Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Umsetzbarkeit der OH-SzA des BSI mittels Open Source Lösungen

Fassung zur Veröffentlichung

Eingereicht am: 27. August 2024
von: Lukas Petrič
Kontakt: lukas@petric-53c.de

Aufgabenstellung

Englischer Titel: Feasibility of Implementing the BSI's OH-SzA Using Open Source Solutions

Die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OH-SzA) des BSI ist durch Betreiber Kritischer Infrastrukturen seit dem 01.05.2023 verpflichtend umzusetzen. Durch das Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit (NIS2UmsuCG) können künftig viele weitere Unternehmen, darunter KMU, zum Betrieb von Systemen zur Angriffserkennung verpflichtet werden. Da in KMU oft wenig Ressourcen für IT- und speziell IT-Sicherheitsthemen zur Verfügung stehen, sollen im Rahmen dieser Master-Thesis die Anforderungen des BSI an Angriffserkennungssysteme nach OH-SzA analysiert und dazu passende Open Source Tools identifiziert und evaluiert werden. Im Anschluss an eine theoretische Evaluierung soll für besonders geeignet scheinende Tools eine prototypische Umsetzung in einer Laborumgebung erfolgen. Die Prototypen werden anschließend auf ihren Erfüllungsgrad der Anforderungen der OH-SzA geprüft und entsprechend dem darin enthaltenen Nachweismodell bewertet. Die Herausforderungen und Chancen bei der Umsetzung der OH-SzA mittels Free and Open Source Software (FOSS) sollen aufgezeigt sowie Empfehlungen für die Umsetzung in KMUs abgeleitet werden.

Kurzreferat

In dieser Arbeit soll die Umsetzbarkeit der OH-SzA des BSI mittels FOSS Lösungen evaluiert und praktisch geprüft werden. Um dies zu erreichen, wird nach einer Beschreibung von Grundlagen und einer Anforderungsanalyse der OH-SzA eine Auswahl an FOSS Lösungen theoretisch gegen die Anforderungen geprüft. Die geeignetsten Systeme werden in einem an die Recplast GmbH angelehnten Prototyp implementiert sowie organisatorische Maßnahmen beschrieben. Der Prototyp wird anhand des Umsetzungsgradmodells der OH-SzA geprüft und erreicht den Umsetzungsgrad 4. Zum Vergleich mit kommerziellen SzA wird ein Interview mit Splunk geführt und auf dessen Basis sowie den gewonnenen Erkenntnissen aus dem Prototyp Empfehlungen für die Umsetzung der OH-SzA in realen KMU gegeben. Dabei sollte nicht nur die Entscheidung zwischen kommerziellen und FOSS SzA, sondern auch für Betriebsmodelle der Systeme und deren Nutzung auf Basis von Vollkostenbetrachtung und unter Berücksichtigung von Strategie und Motivation des Unternehmens erfolgen.

Abstract

This document seeks to evaluate and practically test the feasibility of implementing the German BSI‘s OH-SzA using FOSS. To achieve this, a selection of FOSS tools is first evaluated theoretically against the requirements after a description of related basics and requirements analysis of the OH-SzA. The most fitting systems are implemented in a prototype based on the Recplast GmbH and organizational measures are described. The prototype is evaluated using the implementation level model of the OH-SzA, achieving an level of 4. For comparison with commercial attack detection systems, an interview is conducted with Splunk and recommendations for the implementation of the OH-SzA in real small and medium sized companies are made on the basis of this interview and the knowledge gained from the prototype. The decision should not only be made between commercial and FOSS attack detection systems, but also for operating models of the systems and their use on the basis of full cost consideration, taking into account the strategy and motivation of the company.

Inhalt

1 Einleitung

Mit dem Inkrafttreten des IT-Sicherheitsgesetz 2.0 wurden, neben anderen Inhalten, Kritische Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse zu bestimmten IT-Sicherheitsmaßnahmen verpflichtet [1].

Gemäß §8a Abs. 1a BSIG umfassen diese IT-Sicherheitsmaßnahmen für Kritische Infrastrukturen „ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung“ [2]. Die Erfüllung dieser Anforderung ist gemäß §8a Abs. 3 BSIG dem Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) spätestens ab dem 1. Mai 2024 erstmalig und anschließend alle zwei Jahre nachzuweisen [2].

Diese Systeme zur Angriffserkennung (kurz: SzA) werden neben anderen IT-Sicherheitsmaßnahmen ebenfalls im Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit (kurz: NIS2UmsuCG) §31 (2) für Betreiber kritischer Anlagen gefordert [3, S. 42], welches zum 22.07.2024 als Entwurf vorliegt. Die Formulierung zu SzA entspricht darin der des §8a Abs. 1a BSIG. Darüber hinaus definiert es in §28 je nach Sektor unter anderem ab einer Unternehmensgröße von 50 Mitarbeitern oder 10 Millionen Euro Umsatz besonders wichtige und wichtige Einrichtungen [3, S. 37 f.], die auch zu speziellen Risikomanagementmaßnahmen gemäß §30 verpflichtet sind [3, S. 40].

Um die recht allgemein gehaltene Formulierung zu SzA zu präzisieren und Nachweise gegenüber dem BSI zu ermöglichen, hat das BSI die „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (kurz: OH-SzA) veröffentlicht, die neben den Anforderungen an SzA ein Umsetzungsgradmodell und die Nachweiserbringung beinhaltet [4, S. 4].

1.1 Motivation und Zielsetzung

Zwar sind die SzA bislang nur für Betreiber kritischer Infrastrukturen gefordert, die Gesetzesentwicklung der vergangenen Jahre zeigt jedoch, dass IT-Sicherheit immer weiter in den Fokus des Gesetzgebers rückt. So besteht auch die Möglichkeit, dass Unternehmen abseits von Betreibern kritischer Infrastrukturen künftig zum Einsatz von SzA verpflichtet sein können. Auf Basis der Schwellwerte des NIS2UmsuCG kann dies auch kleine und mittlere Unternehmen (kurz: KMU) treffen, falls eine solche Pflicht auf wichtige Einrichtungen angewendet wird. Üblicherweise ist in KMU die IT-Ausstattung kostenoptimiert, was viele kostenintensivere kommerzielle SzA unattraktiv für diese macht.

Aufgrund dessen wird im Rahmen dieser Arbeit untersucht, ob sich die aktuell gültigen Anforderungen der OH-SzA mittels kostenloser Open Source Anwendungen (Free and Open Source Software, kurz: FOSS) umsetzen lassen, wobei der Fokus auf die technischen Anforderungen gelegt wird. Die SzA werden auf theoretische Erfüllung der OH-SzA bewertet und die vielversprechendsten Anwendungen werden in einem Prototyp geprüft, um Empfehlungen für die Umsetzung von SzA in KMU abzuleiten.

1.2 Aktueller Forschungsstand

Zur OH-SzA existiert aufgrund ihres geringen Alters und bislang engen Geltungsbereichs wenig wissenschaftliche Literatur.

Speziell für den Gesundheitssektor beschreibt der Artikel „Angrifserkennung beim Betrieb von KRITIS gemäß IT-Sicherheitsgesetz 2.0“ von Pilgermann et al. branchenspezifische Möglichkeiten zur Umsetzung der gesetzlichen Anforderungen zum Einsatz von SzA, worin vor allem die Notwendigkeit der Einrichtung eines Security Operations Centers (siehe Kapitel 2.1.1) mit einem SIEM (siehe Kapitel 2.2) betont wird [5, S. 735 f.]. Über die reinen Systeme zur Angriffserkennung weist der Artikel darauf hin, dass für einen ausreichenden Schutz weitere Maßnahmen organisatorischer und technischer Art erforderlich

sind, die aus einem Informationssicherheits-Managementsystem heraus gesteuert werden [5, S. 736 f.]. Der Fokus des Artikels liegt stark auf dem Gesundheitssektor und spezieller der Krankenhaus-IT und behandelt nicht explizit die OH-SzA, insbesondere nicht branchenübergreifend.

Der Artikel „Verpflichtung zur intelligenten Angriffserkennung?“ von Kohpeiß untersucht die OH-SzA vor der konkreten Fragestellung, inwiefern eingesetzte SzA KI-gestützt sein müssen, oder nicht. Dabei ist die Definition des Stands der Technik in Bezug auf SzA der entscheidende Aspekt mit der Schlussfolgerung, dass KI-SzA zwar als Stand der Technik regelbasierten vorgezogen werden sollten, jedoch keine Verpflichtung dazu besteht und ihr Einsatz im Verhältnis zu den Implementierungskosten stehen sollte [6, S. 224].

Die OH-SzA beziehungsweise §8a BSIG wurden unter konkreten Fragestellungen zu ihrer Bedeutung und branchenspezifischen Analysen bereits wissenschaftlich untersucht.

Zum spezifischen Thema, die OH-SzA mittels FOSS oder in KMU umzusetzen, gibt es keine auffindbare Literatur oder aktuelle Forschung.

1.3 Struktur der Arbeit

In Kapitel 1 werden die Motivation, der aktuelle Forschungsstand und die Struktur der Arbeit beschrieben.

In Kapitel 3 werden die Anforderungen der OH-SzA analysiert, indem die Orientierungshilfe strukturell und die Nachweiserbringung beschrieben werden. Die Anforderungen zu den Themen Protokollierung, Detektion und Reaktion werden einzeln betrachtet und besonders relevante Anforderungen diskutiert.

In Kapitel 4 werden Open Source Tools ausgewählt, die wahrscheinlich zur Umsetzung der OH-SzA geeignet sind. Hierzu werden auf Basis der Anforderungen erforderliche Systemtypen herausgearbeitet, für die jeweils womöglich geeignete Tools recherchiert und anhand ihrer Dokumentation

bewertet werden.

In Kapitel 5 wird ein fiktives KMU beschrieben, in dem grob eine theoretische Umsetzung der organisatorischen Anforderungen der OH-SzA beschrieben wird. Die technische Umsetzung der Anforderungen erfolgt prototypisch in einer virtuellen Testumgebung, in der die vielversprechendsten Open Source SzA installiert werden.

In Kapitel 6 werden die eingerichteten SzA anhand der Anforderungen der OH-SzA bewertet, wobei erfüllte Anforderungen herausgearbeitet und nicht erfüllte Anforderungen und Herausforderungen bei der Umsetzung identifiziert werden. Die Ergebnisse der Bewertung werden auf die Nachweiserbringungs-Methode der OH-SzA übertragen.

In Kapitel 7 werden die Ergebnisse der Bewertung für einen Vergleich mit kommerziellen SzA herangezogen, wozu ein Interview mit einem Vertreter eines Herstellers kommerzieller SzA verwendet wird.

Auf Basis der gewonnenen Erkenntnisse werden in Kapitel 8 Empfehlungen für die Umsetzung in realen KMU getroffen.

Die Arbeit endet in Kapitel 9 mit einer Zusammenfassung der gewonnenen Erkenntnisse und einem Fazit.

2 Grundlagen und Begrifflichkeiten

In dieser Arbeit werden einige Fachbegriffe aus dem Bereich der IT-Sicherheit verwendet, die in diesem Kapitel für ein besseres Verständnis der Arbeit einleitend beschrieben werden.

2.1 Systeme zur Angriffserkennung

Systeme zur Angriffserkennung im Sinne der OH-SzA sind „Prozesse, die durch technische Werkzeuge und organisatorische Einbindung unterstützt werden“ [4, S. 6]. Somit bestehen SzA nicht ausschließlich aus technischen Komponenten, sondern umfassen darüber hinaus die Prozesse zu deren Nutzung und Einbindung in die Abläufe des nutzenden Unternehmens. Bezüglich ihrer Funktionalität nimmt die OH-SzA Bezug auf das BSIG, welches fordert, dass die SzA automatisch und fortlaufend Daten aus dem laufenden Betrieb erfassen und auswerten müssen, worauf sie Bedrohungen fortwährend erkennen, vermeiden und geeignete Beseitigungsmaßnahmen vorsehen müssen [2, Abs. 1a]. Entsprechend dieser Definition sind SzA technische und organisatorische Systeme, die sich in den IT-Betrieb einfügen, dessen Daten fortlaufend analysieren, Bedrohungen darin erkennen und Gegenmaßnahmen treffen.

Beispiele für SzA sind somit im bekanntesten Fall Virenscanner, die fortlaufend Dateisignaturen auf Bedrohungen untersuchen und bei erkannten Bedrohungen die betroffenen Dateien löschen oder in Quarantäne verschieben.

2.1.1 Security Operations Center

SzA können gemäß dieser Definition organisatorisch und technologisch beliebig komplex werden – ein komplexeres Beispiel ist ein Security Operations Center (kurz: SOC), das ein Team aus IT-Sicherheitsexperten darstellt und für die Erkennung von Sicherheitsvorfällen, deren Analyse und Reaktion auf sie zuständig ist [7]. So bündelt ein SOC die Systeme zur Angriffserkennung sowohl

in der technologischen als auch der prozessualen Sicht, indem es vom Betrieb der Sicherheitswerkzeuge, deren Nutzung zur Angriffserkennung und Reaktion auf die erkannten Sicherheitsvorfälle die gesamte Kette bündelt.

2.2 Security Information and Event Management

Aus technologischer Perspektive ist häufig ein Security Information and Event Management (kurz: SIEM) das zentrale Werkzeug eines SOC. Ein SIEM korreliert und analysiert Protokolldaten anderer Systeme, um anhand maschinellen Lernens oder definierter Regeln Anomalien im Verhalten von IT-Systemen zu erkennen, die auf einen Sicherheitsvorfall hindeuten [8]. Durch diese Funktionsweise ist SIEM in der Lage, auch die Protokolldaten anderer SzA zentral zu sammeln und auszuwerten, wodurch eine gesamtheitliche Sicht auf alle sicherheitsrelevanten Ereignisse der IT-Umgebung entsteht.

2.2.1 Intrusion Detection Systeme

Intrusion Detection Systeme (kurz: IDS) sind Werkzeuge, die IT-Systeme auf verdächtiges Verhalten hin überwachen und bei Treffern alarmieren.

Grundsätzlich wird zwischen zwei verbreiteten Arten von IDS unterschieden.

Hostbasierte IDS (kurz: HIDS) werden auf den zu überwachenden IT-Systemen, typischerweise Endpunkte wie Server und Clients, direkt installiert und überwachen alle darauf laufenden Aktivitäten [9]. Durch direkten Zugriff auf das zu überwachende System kann ein HIDS Netzwerkverhalten, Dateien und Prozesse des Systems genau überwachen und verdächtige Aktivitäten erkennen.

Netzbasierte IDS (kurz: NIDS) werden im Netzwerk an zentralen Stellen wie Firewalls platziert und überwachen den dort sichtbaren Datenverkehr auf verdächtige Aktivitäten. Hierzu erhalten sie üblicherweise von anderen Netzwerkkomponenten Kopien der durchgehenden Datenpakete und analysieren diese, um den eigentlichen Datenverkehr nicht zu behindern [9].

IDS arbeiten typischerweise signatur- beziehungsweise regelbasiert oder anomaliebasiert. Signaturbasierte IDS prüfen anhand definierter Regeln auf verdächtiges Verhalten, wie zum Beispiel Kommunikation mit bekannt schadhaften IP-Adressen oder bekannte Virensignaturen. Anomaliebasierte IDS lernen über einen bestimmten Zeitraum das Verhalten von IT-Systemen und Netzwerkteilnehmern mittels Machine Learning an (sogenanntes Baselining), woraufhin sie von der Baseline abweichendes Verhalten erkennen können [9].

IDS sind oft nicht nur in der Lage, verdächtiges Verhalten zu erkennen, sondern auch Reaktionsmaßnahmen zu ergreifen. Solche IDS werden auch als „Intrusion Prevention Systeme“, kurz: IPS, bezeichnet. Im Falle von netzbasierten IPS müssen diese anders als reine Detektionssysteme nicht mit gespiegeltem Datenverkehr arbeiten, sondern direkt in die Datenwege zwischengeschaltet werden, um schadhafte Kommunikation verhindern zu können [9].

2.2.2 Endpoint Detection and Response

Endpoint Detection and Response (kurz: EDR) Systeme sind eine spezielle Art von HIDS. EDR überwachen Netzwerkkommunikation, Prozesse, Dateien und weitere relevante Datenpunkte auf Endpunkten wie Servern und Clients auf Bedrohungen. Dabei kommen anders als in klassischen Antivirensystemen nicht nur Signaturen, sondern meist auch maschinelles Lernen zum Einsatz, um Bedrohungen in Echtzeit zu erkennen. Analog zu Antivirensystemen werden EDR-Systeme hochfrequent mit Updates der Detektionsmechanismen versorgt, um die aktuellen Angriffsmuster erkennen zu können. In der Regel aggregieren EDR-Systeme ihre Daten in einem zentralen Verwaltungssystem, das die Ereignisse auf den Endpunkten zentral analysierbar macht [10].

EDR detektieren, wie der Name schon suggeriert, nicht nur Bedrohungen, sondern ermöglichen auch die Reaktion auf diese. EDR-Systeme bieten die Möglichkeit, automatisch auf Bedrohungen zu reagieren, indem zum Beispiel schadhafte Prozesse gestoppt oder an der Ausführung gehindert, Dateien gelöscht oder angegriffene Endpunkte vom Netzwerk isoliert werden, um die

Ausbreitung von Angriffen zu stoppen [10].

2.2.3 Extended Detection and Response

Extended Detection and Response (kurz: XDR) ist ambivalent definiert und meint einerseits eine offene Architektur, die eine Integration verschiedener IT-Sicherheitswerkzeuge miteinander und so ein übergreifendes Zusammenwirken derer ermöglichen soll, wird in der Praxis andererseits aber oft als Begriff für ein „erweitertes“ EDR verwendet, das neben Endpunkt-Agenten noch Funktionen anderer Sicherheitsebenen wie NIDS oder SIEM-artige Funktionen wie zentrale Protokolldatenauswertung übernimmt [11]. Durch die zentrale Bündelung von Detektions- und Reaktionsmöglichkeiten in XDR-Systemen soll eine effizientere und schnellere Analyse und Eindämmung von Bedrohungen über Sicherheitsebenen wie Endpunkte, Netzwerk, Cloudsysteme und weitere ermöglicht werden.

2.2.4 Security Orchestration, Automation and Response

Security Orchestration, Automation and Response (kurz: SOAR) bezeichnet Softwareplattformen, die diverse Sicherheitswerkzeuge integrieren und automatisierte Arbeitsabläufe über diese hinweg ausführen können. So können immer ähnlich ablaufende Arbeitsschritte oder klar definierbare Abläufe zentral automatisiert werden, wodurch IT-Sicherheitspersonal entlastet und die Arbeitsgeschwindigkeit erhöht wird [12].

SOAR können so einerseits in der Analyse von Alarmen unterstützen, indem beispielsweise verdächtige Dateien automatisiert in eine Sandbox kopiert, dort ausgeführt und die Ergebnisse Analysten zur Verfügung gestellt werden, andererseits aber auch bei der Reaktion auf Vorfälle unterstützen, indem beispielsweise automatisiert Firewallregeln erstellt werden, die von Angriffen betroffene Systeme isolieren.

2.3 Protokollierung, Detektion und Reaktion

Auf Basis der Definition von SzA (siehe Kapitel 2.1) trennt das BSI in der OH-SzA drei Aufgabenbereiche der SzA voneinander ab. Die Sammlung der Datengrundlage für die Angriffserkennung bezeichnet es als „Protokollierung“, die Erkennung sicherheitsrelevanter Ereignisse darin als „Detektion“ und die Verhinderung der Auswirkungen von Angriffen als „Reaktion“ [4, S. 7].

Jeder Aufgabenbereich hängt somit von seinem vorherigen ab – ohne gesammelte Daten in der Protokollierung kann keine Detektion, also Analyse der Daten, erfolgen. Ebenso kann ohne ein erkanntes sicherheitsrelevantes Ereignis aus der Detektion keine Reaktion darauf erfolgen.

Die Aufgabenbereiche werden in der OH-SzA als Gliederung der Anforderungen verwendet, sodass ein eindeutiger Bezug von Anforderungen zum jeweiligen Schritt in der oben genannten Ablaufskette zwischen den Bereichen gegeben ist.

2.3.1 „Protokollierung“ und „Logging“

Der Bereich „Protokollierung“ bezieht sich wie oben genannt auf die Sammlung einer Datengrundlage für die Angriffserkennung. Das BSI beschreibt im IT-Grundschutzbaustein OPS.1.1.5 „Protokollierung“, auf den es auch aus der OH-SzA verweist, den Begriff „Protokollierung“ als die automatische Speicherung und Bereitstellung für die Auswertung von allen oder ausgewählten betriebs- oder sicherheitsrelevanten Ereignissen [13, S. 1].

Neben dem deutschen Begriff „Protokollierung“ wird auch häufig der englische Begriff „Logging“ synonym verwendet. Gespeicherte Ereignisse werden im Deutschen meist als „Protokollereignis“, „Protokollmeldung“ oder „Protokollierungsdaten“ bezeichnet [13, S. 2, 5], im Englischen wird hierfür meist der Begriff „Log“ verwendet.

Die Begriffe „Protokollierung“ und „Logging“ werden im Rahmen dieser Arbeit synonym verwendet.

2.4 Weitere Regularien

Neben der OH-SzA beziehungsweise dem BSIG gibt es weitere branchenübergreifende Regularien zur Informationssicherheit, die freiwillig oder zur Erreichung von Zertifizierungen umgesetzt werden können oder müssen. Diese Regularien beinhalten häufig wie die OH-SzA die Pflicht oder Empfehlung zum Einsatz von SzA und werden in den folgenden Unterkapiteln kurz beschrieben.

2.4.1 ISO 27001 / ISO 27002

Die Norm ISO/IEC 27001 definiert einen Rahmen für Informationssicherheits-Managementsysteme (kurz: ISMS) in Einführung, Betrieb und kontinuierlicher Verbesserung. Die Norm ist für Unternehmen aller Größen und Sektoren universell konzipiert und bietet eine Grundlage für eine Zertifizierung nach ISO 27001, um das Vorhandensein eines Risikomanagements bezüglich der Informationssicherheit nach internationalen Standards nachzuweisen [14].

Die Norm ISO/IEC 27002 konkretisiert die ISO/IEC 27001, welche einen Rahmen für ISMS beschreibt, um konkrete Best Practices und spezifische Anforderungen, die in Bereiche wie Zugangssteuerung, Kryptographie und weitere gruppiert sind. So müssen Organisationen sich keine eigenen Maßnahmen zur Erfüllung von ISO/IEC 27001 überlegen, sondern können sich an einem vordefinierten Maßnahmenkatalog ausrichten. Neben vielen weiteren Aspekten der Informationssicherheit beinhaltet die ISO/IEC 27002 ähnlich wie die OH-SzA Vorgaben zur Protokollierung, Überwachung von Aktivitäten (im Sinne der Detektion) und Reaktion auf Sicherheitsvorfälle [15].

2.4.2 BSI IT-Grundschutz

Das BSI veröffentlicht mit dem IT-Grundschutz eine Methode und Anleitung zur Absicherung von Informationen und Systemen von Organisationen. Der IT-Grundschutz ist gestaffelt in die Absicherungsstufen Basis-, Standard- und Kern-

Absicherung, die um jeweils aufeinander aufbauende Anforderungen erweitern. Der IT-Grundschutz ist an der ISO/IEC 27001 ausgerichtet, wodurch eine Zertifizierung nach ISO/IEC 27001 auf Basis des IT-Grundschutzes möglich ist [16].

Inhaltlich besteht der Grundschutz aus zwei groben Komponenten: Den BSI-Standards und dem IT-Grundschutz-Kompendium. Die BSI-Standards beschreiben Methoden und Prozesse zu verschiedenen Informationssicherheitsaspekten, wobei der Standard 200-1 allgemeine Anforderungen an ISMS analog zu ISO/IEC 27001 beschreibt und auch kompatibel zu dieser Norm ist. Der Standard 200-2 beschreibt die IT-Grundschutz-Methodik, also das Vorgehen zu Aufbau und Betrieb eines ISMS. Der Standard 200-3 beschreibt die Vorgehensweise zu Aufbau und Betrieb eines Risikomanagements, welches in der Umsetzung des IT-Grundschutzes wichtig ist. Der letzte Standard, 200-4, bietet eine Anleitung für den Aufbau eines Business Continuity Managements in einer Organisation [17]. Insbesondere die Standards 200-1 und 200-2 können also wie die ISO/IEC 27001 und ISO/IEC 27002 als Vorlage für die Einführung und Betrieb eines ISMS verwendet werden.

Das IT-Grundschutz-Kompendium besteht aus diversen IT-Grundschutz-Bausteinen, die themenbezogen Anforderungen zur Informationssicherheit gruppieren. Die Anforderungen sind dabei je Baustein nochmals getrennt in Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Zum Grundschutz-Kompendium stellt das BSI eine Zuordnungstabelle bereit, die eine Abbildung der ISO/IEC 27001 auf die Anforderungen des Grundschutz-Kompendiums und die Standards ermöglicht [18].

Das BSI verweist aus OH-SzA auf die Grundschutz-Bausteine OPS.1.1.5 „Protokollierung“ [4, S. 9], DER.1 „Detektion von sicherheitsrelevanten Ereignissen“ [4, S. 11] und DER.2.1 „Behandlung von Sicherheitsvorfällen“ [4, S. 14] als Anforderungsbasis. Somit ist eine Umsetzung der OH-SzA zwangsläufig zumindest mit einer Teilumsetzung des Grundschutz-Kompendiums verbunden.

2.4.3 NIST Cybersecurity Framework

Das Cybersecurity Framework (kurz: CSF) des US-amerikanischen National Institute of Standards and Technology bietet einen Leitfaden für das Management von Cybersicherheitsrisiken für beliebige Organisationen unabhängig von ihrer Größe oder ihres Sektors [19, S. iv].

Das CSF teilt sich in drei Komponenten. Die Komponente „CSF Core“ beschreibt abstrakt Cybersecurity-Resultate in einer immer detaillierter werdenden Hierarchie von Funktionen, Kategorien und Unterkategorien. Die Komponente „CSF Organizational Profiles“ beschreibt den Cybersecurity-Stand einer Organisation entlang der CSF Core Resultate. Die „CSF Tiers“ können auf CSF Organizational Profiles angewendet werden, um den Reifegrad einer Organisation hinsichtlich ihres Cybersecurity-Risikomanagements zu beschreiben [19, S. 1].

Das CSF Core teilt sich in verschiedene Funktionen auf, die den Lebenszyklus des Cybersecurity-Risikomanagements widerspiegeln sollen. Die übergreifende Funktion des CSF Core ist „Govern“, worin Strategien und Richtlinien zur Umsetzung und Überwachung der anderen Funktionen definiert werden. Die weiteren Funktionen sind „Identify“, worin Cybersecurity-Risiken für die Organisation erkannt werden, „Protect“, worin präventive Maßnahmen gegen Cybersecurity-Risiken etabliert werden, „Detect“, worin Angriffe erkannt werden, „Respond“, worin auf diese Angriffe reagiert wird, und „Recover“, worin die Auswirkungen von Angriffen beseitigt werden [19, S. 3 f.].

Die Funktionen „Detect“ und „Respond“ des NIST CSF definieren die Inhalte der Bereiche „Detektion“ und „Reaktion“ der OH-SzA also als integrale Bestandteile des Informationssicherheits-Risikomanagements, denen neben präventiven und Management-Funktionen eine große Bedeutung zukommt.

3 Anforderungsanalyse der OH-SzA

In diesem Kapitel werden die Anforderungen, die die OH-SzA an den Einsatz von Angriffserkennungssystemen stellt, analysiert. Dazu werden zunächst die Struktur der OH-SzA sowie die für die Anforderungsanalyse relevante Systematik zur Nachweiserbringung beschrieben. Anschließend werden jeweils die Anforderungen zu Protokollierung, Detektion und Reaktion identifiziert und analysiert, um eine Basis für die spätere Bewertung der Open Source Tools zu haben. Dabei soll eine genauere Betrachtung der für den Betrachtungsaspekt „Umsetzbarkeit mittels FOSS“ relevanten technischen Anforderungen stattfinden, eher eine grobe Betrachtung organisatorisch/prozessualer Anforderungen.

3.1 Struktur der OH-SzA

Die OH-SzA beginnt mit einem Überblick-Kapitel, das den Aufbau der Orientierungshilfe, die Zielsetzung und Adressatenkreis sowie weiterführende Informationen beinhaltet [4, S. 4 f.]. In Kapitel 2 werden Grundlagen für die Einordnung und das Verständnis der OH-SzA beschrieben, darunter der gesetzliche Hintergrund, der zur Entstehung der OH-SzA geführt hat [4, S. 3] sowie eine Beschreibung anhand des BSIG, was Systeme zur Angriffserkennung leisten müssen und welche Systeme durch sie abgedeckt werden müssen [4, S. 6 f.].

In Kapitel 3 beschreibt die OH-SzA ihre Anforderungen an Systeme zur Angriffserkennung, wobei eine Trennung der Bereiche Protokollierung, Detektion und Reaktion in jeweils einen eigenen Abschnitt erfolgt [4, S. 8]. Die Abschnitte Protokollierung und Detektion trennen sich jeweils in Unterabschnitte zur Planung und Umsetzung [4, S. 9] und [4, S. 11].

In Kapitel 4 wird beschrieben, die das Umsetzungsgradmodell der OH-SzA funktioniert und wie die Nachweiserbringung gegenüber dem BSI zu erfolgen hat [4, S. 15 f.].

3.2 Nachweiserbringung

Die OH-SzA beinhaltet ein Umsetzungsgradmodell, das zur Beurteilung der technischen und organisatorischen Maßnahmen in der geprüften Kritischen Infrastruktur dienen soll [4, S. 15]. Dabei wird zwischen sechs Umsetzungsgraden entschieden, die von Umsetzungsgrad 0, in dem keine Anforderungen erfüllt und auch keine entsprechenden Maßnahmen geplant sind, zu Umsetzungsgrad 5 reichen, in dem alle Anforderungen erfüllt oder nachvollziehbar begründet ausgeschlossen sind, zusätzliche Maßnahmen umgesetzt und ein kontinuierlicher Verbesserungsprozess etabliert ist [4, S. 15].

Die Umsetzungsgrade werden für die Nachweiserbringung als Zieldefinition verwendet, wozu die OH-SzA definiert: „Grundsätzlich sollte ein Umsetzungsgrad der Stufe 4 erreicht werden, um die Anforderungen […] zu erfüllen“ [4, S. 16]. Das BSI berücksichtigt dabei, dass die Umsetzung der Anforderungen eine längere Zeit in Anspruch nehmen kann, weshalb im ersten Nachweiszyklus am 1. Mai 2023 ein Umsetzungsgrad der Stufe 3 als ausreichend akzeptiert wurde. Abweichungen nach unten sind im ersten und den folgenden zweijährigen Nachweiszyklen nur unter der Angabe von Gründen zulässig [4, S. 16].

3.3 Allgemeine Anforderungen

Die OH-SzA unterscheidet grundsätzlich zwischen den Anforderungsbereichen Protokollierung, Detektion und Reaktion.

Die Anforderungen darin werden anhand der Modalverben MUSS, SOLLTE und KANN formuliert, was einen Abgleich mit dem Umsetzungsgradmodell ermöglicht, in dem Anforderungen gruppiert anhand ihrer Modalverben für bestimmte Umsetzungsgrade erfüllt sein müssen. Dabei ist die Erfüllung aller MUSS-Anforderungen die Voraussetzung für die Erfüllung des Umsetzungsgrads 3. Alle SOLLTE-Anforderungen müssen für Umsetzungsgrad 4 umgesetzt oder stichhaltig begründet ausgeschlossen werden. Selbiges gilt für alle KANN-Anforderungen bezüglich Umsetzungsgrad 5 [4, S. 8].

Zur Erfüllung der Anforderungen empfiehlt das BSI, aber fordert nicht, die Etablierung eines ISMS [4, S. 8].

Über die konkreten Anforderungsbereiche hinaus stellt das BSI übergreifende Anforderungen für alle Bereiche und Prozesse zur Angriffserkennung. Die übergreifenden Anforderungen werden in Anlage 1 aufgeführt. Als „Anforderung“ wird jeder Satz der OH-SzA und referenzierter Anforderungsdokumente behandelt, der entsprechend der Definition der OH-SzA „mit den in Versalien geschriebenen Modalverben MUSS, SOLLTE und KANN sowie den zugehörigen Verneinungen formuliert“ ist [4, S. 8]. Wenn an einzelnen Stellen die definierten Modalverben nicht in Versalien geschrieben sind, wird der entsprechende Satz nicht als eigene Anforderung betrachtet, sondern der kontextual passenden Anforderung angefügt. Jene Anforderungen, die nicht direkt aus der OH-SzA, sondern von ihr geforderten Grundschutz-Bausteinen stammen, erben das Modalverb der OH-SzA, mit dem der Grundschutz-Baustein gefordert wird. Abweichende Modalverben des jeweiligen Grundschutz-Bausteins werden somit mit dem übergreifenden Modalverb der OH-SzA für diesen Baustein überschrieben.

Die Anlage 1 dient der tabellarischen Darstellung der übergreifenden Anforderungen der OH-SzA und Vorprüfung der Anforderungen dahingehend, ob sie durch die SzA zu erfüllen bzw. erfüllbar und somit in der Prüfung der FOSS-Tools anwendbar sind, oder durch Systeme außerhalb der SzA, die Organisation oder deren Prozesse erfüllt werden müssen und somit in der Prüfung der FOSS-Tools nicht anwendbar sind. Solche Anforderungen, die nicht durch die SzA zu erfüllen bzw. erfüllbar sind, werden auf theoretischer Ebene in Kapitel 5.2 betrachtet. Für jede Anforderung wird die Erfüllbarkeit oder Nichterfüllbarkeit durch die SzA begründet.

Um im weiteren Verlauf dieses Dokuments eine genaue Referenzierung der einzelnen Anforderungen zu ermöglichen, werden die Anforderungen aller Bereiche in den Anlagen eindeutig nummeriert.

Aus der Prüfung der Anforderungen in Anlage 1 wird ersichtlich, dass von fünf übergreifenden Anforderungen nur Anforderung Nummer 4 auf die SzA selbst anwendbar ist.

3.4 Anforderungen zur Protokollierung

Die Anforderungen zur Protokollierung werden in Anlage 2 genauer aufgelistet.

Die Anforderungen zur Protokollierung teilen sich in die Phasen Planung und Umsetzung.

Neben den Anforderungen der OH-SzA selbst wird die Erfüllung aller Basisanforderungen des IT-Grundschutz-Bausteins OPS.1.1.5 als MUSS-Anforderung gefordert [4, S. 9].

Der Anforderungsbereich Protokollierung verlangt die Erhebung und zentrale Speicherung aller sicherheitsrelevanten Ereignisse. Darüber hinaus werden Anforderungen an die Reihenfolge der Anbindung der Quellsysteme auf Netz- und Systemebene, organisatorische Rahmenbedingungen und die sichere Speicherung und Verarbeitung der Protokolldaten gestellt.

3.5 Anforderungen zur Detektion

Die Anforderungen zur Detektion werden in Anlage 3 genauer aufgelistet.

Analog zu den Anforderungen zur Protokollierung, teilen sich die Anforderungen an die Detektion in die Phasen Planung und Umsetzung.

Neben den Anforderungen der OH-SzA selbst wird die Erfüllung aller Basisanforderungen des IT-Grundschutz-Bausteins DER.1 als MUSS-Anforderung gefordert [4, S. 11].

Der Anforderungsbereich Detektion verlangt die kontinuierliche Auswertung der zuvor erhobenen Protokolldaten zur Erkennung von Sicherheitsvorfällen sowie

den Einsatz weiterer Detektionssysteme wie NIDS und Schadcodescannern. Dazu werden Anforderungen an prozessuale Abläufe und organisatorische Rahmenbedingungen wie das Vorhandensein speziell geschulten, dedizierten Personals, gestellt.

3.6 Anforderungen zur Reaktion

Die Anforderungen zur Reaktion werden in Anlage 4 genauer aufgelistet.

Neben den Anforderungen der OH-SzA selbst wird die Erfüllung aller Basisanforderungen des IT-Grundschutz-Bausteins DER.2.1 als MUSS-Anforderung, die Standardanforderungen des selben Bausteins als SOLL-Anforderung gefordert [4, S. 14].

Der Anforderungsbereich Reaktion stellt vor allem prozessuale und organisatorische Anforderungen an die Behandlung von Sicherheitsvorfällen. Darüber hinaus wird auf technischer Ebene die automatische Reaktion auf erkannte Sicherheitsvorfälle durch gefordert, indem automatisiert Maßnahmen zur Vermeidung und Beseitigung von Störungen ergriffen werden, wo dadurch keine relevante Beeinträchtigung der kritischen Dienstleistung des Betreibers entstehen kann.

4 Auswahl von Open Source Tools

In diesem Kapitel werden zur Erfüllung der Anforderungen in Abhängigkeit der Anforderungsanalyse in Kapitel 5 notwendige Systemtypen identifiziert. Je Systemtyp werden zwei bis drei FOSS-Tools als Bewertungskandidaten bestimmt. Anhand der existierenden Dokumentation und ggf. Drittquellen werden die Tools theoretisch auf ihren möglichen Erfüllungsgrad der OH-SzA untersucht.

4.1 Identifikation erforderlicher Systemtypen

Für eine möglichst effiziente Abdeckung der Anforderungen der OH-SzA aus den Bereichen Protokollierung, Detektion und Reaktion sollten die zur Anforderungserfüllung verwendeten Systemtypen mindestens einen der Bereiche möglichst umfassend abdecken.

Die Protokollierung von IT-Systemen ist zunächst nicht spezifisch eine Funktion für die Angriffserkennung, sondern dient neben der Angriffserkennung auch der allgemeinen Dokumentation relevanter Informationen über Aktivitäten in IT-Systemen. Zur möglichst einfachen und übergreifenden Auswertung von Protokolldaten werden diese üblicherweise zentral gesammelt und ausgewertet. Zu diesen Zwecken werden üblicherweise sogenannte Logmanagement-Systeme eingesetzt, die Protokolldaten von IT-Systemen erheben, sammeln, zentralisieren, gegebenenfalls transformieren und für die Auswertung verfügbar machen [20]. Zur Erfüllung der Anforderungen an die Protokollierung wird im Folgenden demnach nach einem geeigneten Logmanagement-System gesucht.

Für die Detektion im Sinne der Angriffserkennung geht aus der OH-SzA hervor, dass diese vorrangig auf Basis von Protokolldaten erfolgen soll. Zur Angriffserkennung auf Basis von Protokolldaten wird üblicherweise ein SIEM (siehe Kapitel 2.1) eingesetzt.

Über SIEM hinaus stellt die OH-SzA die explizite Forderung nach dem Einsatz

von netzwerkbasierten Intrusion Detection Systemen (kurz: NIDS, siehe Anforderung 95 in Anlage 3), die den Datenverkehr im Netzwerk auf verdächtigen Datenverkehr hin überwachen [9].

Zur Reaktion fordert die OH-SzA aus technischer Perspektive die Möglichkeit, automatisiert auf erkannte Sicherheitsvorfälle reagieren zu können. Diese Anforderung ist breit interpretierbar: Genügt schon die übliche Funktion verbreiteter Antivirenprogramme, erkannte schadhafte Dateien in Quarantäne zu versetzen, als automatische Reaktion? Zwar handelt es sich dabei um eine Form automatisierter Reaktion (Verschiebung in Quarantäne) auf einen erkannten Sicherheitsvorfall (Vorhandensein eines Schadprogramms), jedoch gibt es viele Arten von Sicherheitsvorfällen, auf die in dieser Weise nicht reagiert werden kann (z.B. Brute-Force-Angriff auf einen Benutzeraccount). Aus diesem Grund soll, um den Anforderungen umfassend zu entsprechen, eine Lösung eingesetzt werden, die automatisierte Reaktionsmaßnahmen auf eine möglichst breite Variation vn Sicherheitsvorfällen ermöglicht. Hierzu kommt üblicherweise ein Security Orchestration, Automation and Response (kurz: SOAR) System zum Einsatz, welches verschiedene Systeme und Technologien integriert und automatisierte Arbeitsabläufe auf diesen ermöglicht. Hierdurch kann eine systemübergreifende, automatisierte Reaktion auf Sicherheitsvorfälle eingerichtet werden [21].

4.2 Auswahl zu bewertender FOSS-Tools

In diesem Unterkapitel wird eine Auswahl an möglichen Lösungskandidaten identifiziert und anhand verfügbarer Dokumentation gegen die Anforderungen der OH-SzA geprüft. Pro Systemtyp werden die einzelnen Kandidaten miteinander verglichen und der Kandidat mit dem höchsten Abdeckungsgrad der Anforderungen in die prototypische Umsetzung übergeben. Geht aus der Dokumentation nicht klar hervor, ob die Anforderung erfüllt werden kann, wird die Anforderung als nicht erfüllt angenommen, da auch bei praktischer Möglichkeit, eine Anforderung umzusetzen, dies durch mangelnde Dokumentation erschwert wird.

Um die Auswahl möglicher Kandidaten einzugrenzen, werden folgende Anforderungen an die FOSS-Eigenschaft aller Systeme gestellt:

Der Quellcode des Systems muss öffentlich einsehbar sein. Das System muss aktiv entwickelt werden, die letzte Änderung am Quellcode also maximal sechs Monate zurückliegen. Die Lizenz des Systems muss eine kommerzielle Nutzung gestatten, um eine Erfüllung der OH-SzA in Unternehmen möglich zu machen. Werden verschiedene Bezahlmodelle für die Nutzung des Systems angeboten, wird ausschließlich der kostenfreie Funktionsumfang in der Prüfung berücksichtigt. Darüber hinaus angebotene Dienstleistungen oder Funktionen werden nicht betrachtet. Das kostenfreie Preismodell darf keinen Beschränkungen bezüglich Zeit oder Volumen unterliegen sowie nicht an einen anzufordernden Lizenzschlüssel gebunden sein.

Da je nach Systemtyp auch mit dieser Eingrenzung eine Vielzahl möglicher Kandidaten verfügbar sein kann, werden pro Systemtyp maximal drei Vergleichskandidaten betrachtet.

Als Bewertungsgrundlage für die FOSS-Tools wird die aus Anlage 1 bis Anlage 4 abgeleitete Anlage 5 verwendet. Sie ist auf die anwendbaren Anforderungen gefiltert sowie Zeilen zur Festlegung, ob die Anforderung erfüllt ist, eine Begründung hierzu sowie einen Verweis auf eine entsprechende Quelle für die theoretische Prüfung in diesem Kapitel.

4.2.1 Logmanagement

Die Logmanagement-Systeme dienen vorrangig der Erfüllung der Anforderungen des Bereichs „Protokollierung“ (siehe Kapitel 3.4).

Primär sollen sie für eine Sammlung und Weiterleitung der Protokolldaten der relevanten Systeme sorgen, um sie den Systemen zur Detektion zur Auswertung bereitzustellen.

Als Grundlage für die Logmanagement-Systeme wird davon ausgegangen, dass die für die Angriffserkennung relevanten Protokolldaten von Syslog-fähigen

Systemen wie Linux-Endpunkten und üblichen Netzwerkkomponenten sowie Windows-Systemen erzeugt werden.

Logstash

Logstash ist eine von Elastic entwickelte Open Source Datenerfassungslösung, die Daten sowohl aggregieren als auch normalisieren und für nachgelagerte Auswertungen bereitstellen kann. Logstash hat seine Ursprünge in der Sammlung von Protokolldaten [22].

Logstash ist Teil des Elastic Stack, der aus verschiedenen separaten Komponenten besteht, die gemeinsam eine Ende-zu-Ende-Lösung zur Erhebung, Weiterleitung, Aggregation, Speicherung, Analyse und Visualisierung von Daten bietet [23]. Dabei dient Winlogbeat zur Übertragung von Windows Event Protokolldaten an Logstash [24], während Filebeat zur Übertragung von dateibasierten Protokolldaten zum Beispiel auf Linux-Systemen dient [25].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Logstash am 22. Mai 2024 statt [26], von Winlogbeat und Filebeat am 23. bzw. 28. Mai 2024 [27]. Somit werden die drei Systeme alle aktiv entwickelt.

Logstash hat in der kostenlosen und offenen Basisversion einige Funktionseinschränkungen [28], ist jedoch nicht an einen Lizenzschlüssel oder Einschränkungen hinsichtlich Zeit oder Volumen gebunden. Winlogbeat und Filebeat unterliegen keinen Preismodellen und sind nicht an Lizenzschlüssel oder sonstige Einschränkungen gebunden [29].

Logstash, Winlogbeat und Filebeat sind mit der Elastic License lizensiert, welche innerhalb eines Unternehmens keine Einschränkungen der kommerziellen Nutzung vornimmt [30].

Die Anforderungsanalyse von Logstash anhand dessen Dokumentation [22] wird in 0 detailliert durchgeführt.

Als Logmanagementsystem ist Logstash kein Detektions- oder Reaktionssystem, weshalb die entsprechenden Anforderungen für Logstash nicht geprüft werden.

Von den 11 anwendbaren Anforderungen zur Protokollierung erfüllt Logstash 8.

Logstash zeigt Stärken vor allem in der Integration mit Winlogbeat und Filebeat, die eine einfachere und zentral verwaltbare Integration von Endpunkten in das Logmanagement ermöglichen, als auf den Endpunkten native Protokollierungsfunktionen wie Windows Event Forwarding oder rsyslog zu konfigurieren. Eine Schwäche von Logstash ist die funktionale Einschränkung der Basisversion, wodurch nicht der volle Leistungsumfang ohne Lizenzkosten nutzbar ist.

Graylog Open

Graylog Open ist eine von Graylog als Open Source Projekt erstellte, zentralisierte Logmanagement-Lösung für Protokolldatenaggregation, -analyse und -verwaltung [31].

Graylog benötigt eine Datenbank, wobei zwischen Elasticsearch (Versionen vor 7.11) und Opensearch (siehe Kapitel 6.2.2) gewählt werden kann [32]. Graylog ist wie Logstash auf externe Dateneingaben angewiesen und empfiehlt hierzu ebenfalls die Verwendung von Winlogbeat [33] und Filebeat [34].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Graylog am 31. Mai 2024 statt [35]. Somit wird das System aktiv entwickelt.

Graylog hat in der kostenfreien Variante „Open“ einige Funktionseinschränkungen, ist jedoch nicht an einen Lizenzschlüssel oder Einschränkungen hinsichtlich Zeit oder Volumen gebunden [36].

Graylog ist unter der Server Side Public License Version 1 lizensiert, die eine kommerzielle Verwendung der unmodifizierten Software bei rein internem Gebrauch gestattet [37].

Die Anforderungsanalyse von Graylog Open anhand dessen Dokumentation [38] wird in Anlage 7 detailliert durchgeführt.

Graylog Open beinhaltet die durch separate Lizenzen zu erwerbenden

Funktionen zur Korrelation von Protokolldaten [39] oder Anomalieerkennung und Sicherheitsüberwachung [40] nicht, weshalb die Anforderungen zu Detektion und Reaktion für Graylog Open nicht geprüft werden. Von den 11 anwendbaren Anforderungen zur Protokollierung erfüllt Graylog Open 6.

Graylog zeigt seine Stärken in der Interoperabilität mit anderen Systemen, da es unter anderem Winlogbeat und Filebeat als Datenquellen integrieren sowie Logstash als Speicherziel für Protokolldaten nutzen kann. Graylog kann somit als vollständiger Ersatz für Logstash verwendet werden.

Eine große Schwäche von Graylog sind die fehlenden Funktionen in der Variante „Open“, wodurch Korrelations- und Aggregationsfunktionen fehlen. Diese sind nur mit der kostenpflichtigen Variante „Enterprise“ verfügbar.

Fluentd

Fluentd ist ein vom Fluentd Project entwickelter Open Source Datensammler für eine einheitliche Protokollierungsschicht, der über eine Vielzahl an Plugins eine möglichst breite Varianz an Datenquellen und Outputs bedient [41].

Fluentd ist in einer Kombination aus C und Ruby geschrieben und ist in eine Plugin-basierte Architektur strukturiert, deren Kern die Fluentd Engine bildet und diverse Input-, Output- und Puffer-Plugin-Kombinationen unterstützt [42].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Fluentd am 29. Mai 2024 statt [43]. Somit wird das System aktiv entwickelt.

Fluentd ist vollständig kostenfrei, die Webseite verweist nur auf eine Menge an Drittunternehmen, die Enterprise Services zu Fluentd anbieten [44].

Fluentd ist unter der Apache License Version 2 lizensiert, die keine Einschränkungen in der Verwendung der Software, einschließlich kommerzieller Verwendung, vornimmt [45].

Die Anforderungsanalyse von Fluentd anhand dessen Dokumentation [46] wird in Anlage 8 detailliert durchgeführt.

Als Logmanagementsystem ist Fluentd kein Detektions- oder Reaktionssystem, weshalb die entsprechenden Anforderungen für Fluentd nicht geprüft werden. Von den 11 anwendbaren Anforderungen zur Protokollierung erfüllt Fluentd 7.

Eine Schwäche von Fluentd ist die fehlende integrierte Speichermöglichkeit für Protokolldaten abgesehen von lokalen Puffern.

Die große Stärke von Fluentd liegt einerseits in dessen hohen Grad an Flexibilität durch die Plugin-basierte Architektur, die Integrationen mit einer Vielzahl an Eingabe- und Zielsystemen ermöglicht, andererseits auch in der vollständigen Kostenfreiheit mit gleichzeitiger Verwendung der Apache License.

4.2.2 Security Information and Event Management

Die Security Information and Event Management (kurz: SIEM) Systeme dienen vorrangig der Erfüllung der Anforderungen des Bereichs „Detektion“ (siehe Kapitel 3.5).

Die SIEM-Systeme sollen eine Detektion sicherheitsrelevanter Ereignisse auf Basis von Protokolldaten ermöglichen, die entweder von einem Logmanagement-System oder systemeigenen Komponenten erhoben werden. Manche SIEM-Systeme bieten eigene Funktionen zur Protokollierung oder gar zur Reaktion. Die Systeme werden abhängig von ihrem beworbenen Funktionsumfang in den jeweils relevanten Bereichen geprüft.

Wazuh

Wazuh ist eine von Wazuh Inc. entwickelte Open Source Security Plattform, die SIEM- und XDR-Funktionen für Endpunkte und Cloud bietet, darunter Echtzeit-Korrelationen, Angriffserkennung und -alarmierung sowie aktive Reaktionsmöglichkeiten. Dabei stehen öffentliche Clouds, private Clouds und Rechenzentren on-premise im Fokus [47].

Wazuh besteht aus einem zentralen Server, der zur Verarbeitung von Protokolldaten über Syslog, API oder weitere Empfangsmöglichkeiten dient. Der

Server verarbeitet die Daten und legt sie in einem Wazuh Indexer ab, der sie wiederum speichert und zur Auswertung bereitstellt. Der Wazuh Server prüft die Protokolldaten gegen definierte Detektionsregeln. Darüber hinaus bietet Wazuh einen Agenten, der Protokolldaten auf seinem Hostsystem erhebt und an den Wazuh Server weiterleitet [48]. Die Möglichkeit zur Protokollierung ist somit in Wazuh für agentenfähige Systeme mit integriert.

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Wazuh am 03. Juni 2024 statt [49]. Somit wird das System aktiv entwickelt.

Wazuh ist vollständig kostenfrei, es gibt keine Angaben über kostenpflichtige Varianten oder Dienstleistungen auf der Webseite [48].

Wazuh ist unter der GNU General Public License Version 2 lizensiert, die keine Einschränkungen der kommerziellen Nutzung der Software vornimmt [50].

Die Anforderungsanalyse von Wazuh anhand dessen Dokumentation [51] wird in Anlage 9 detailliert durchgeführt.

Wazuh wirbt mit Funktionen in den Bereichen Protokollierung, Detektion und Reaktion und wird daher in allen Bereichen geprüft. Von der 1 anwendbaren übergreifenden Anforderung erfüllt Wazuh 1, von den 11 anwendbaren Anforderungen zur Protokollierung erfüllt Wazuh 9, von den 21 anwendbaren Anforderungen zur Detektion 19 und von den 4 anwendbaren Anforderungen zur Reaktion 4.

Wazuh zeigt Schwächen in der Ausführung von Suchen auf bereits analysierten Protokolldaten, wozu keine einfache Möglichkeit in der Dokumentation ersichtlich ist.

Die große Stärke von Wazuh liegt in der übergreifenden Behandlung aller Anforderungsbereiche, indem die Erhebung von Protokolldaten sowie automatisierte Reaktionen über den Wazuh Agenten ermöglicht sowie zentrale Detektion im Wazuh Server ausgeführt wird. Wazuh bietet so das Potenzial, als einzelnes System alle Anforderungsbereiche zu erfüllen. Die Kostenfreiheit in

Verbindung mit der GNU General Public License Version 2 ermöglicht die volle Ausschöpfung des Potenzials der Software ohne Lizenzkosten.

OpenSearch

OpenSearch ist eine flexible Open-Source Lösung zur Erkundung, Anreicherung und Visualisierung von Daten mit Integrationen für maschinelles Lernen, Datenverarbeitung und mehr. OpenSearch wirbt mit Security Analytics Funktionen, die die Erkennung von Bedrohungen in Echtzeit ermöglichen sollen [52]. OpenSearch ging als Open-Source Fork aus Elasticsearch und Kibana hervor und bietet eine sichere, hochwertige Such- und Analyseplattform, die von ihrer Community und einem Partnernetzwerk weiterentwickelt wird [53].

OpenSearch besteht aus einer Datenhaltungs- und -analyseplattform namens OpenSearch, einem Visualisierungs- und Benutzerinterface namens OpenSearch Dashboards und einem serverseitigen Datensammler namens Data Prepper [53].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von OpenSearch am 10. Juni 2024 statt [54]. Somit wird das System aktiv entwickelt.

OpenSearch ist vollständig kostenfrei, es gibt keine Angaben über kostenpflichtige Varianten oder Dienstleistungen auf der Webseite [52].

OpenSearch ist unter der Apache License Version 2 lizensiert, die keine Einschränkungen in der Verwendung der Software, einschließlich kommerzieller Verwendung, vornimmt [53].

Die Anforderungsanalyse von OpenSearch anhand dessen Dokumentation [55] wird in Anlage 10 detailliert durchgeführt.

Als Datenauswertungssystem ist Logstash kein Protokollierungs- oder Reaktionssystem, weshalb die entsprechenden Anforderungen durch dieses System nicht erfüllt werden können. Von der 1 anwendbaren übergreifenden Anforderung erfüllt Wazuh 1, von den 21 anwendbaren Anforderungen zur Detektion 17.

OpenSearch zeigt Schwächen in der fehlenden Möglichkeit zur Erkennung von Schadcode.

Die große Stärke von OpenSearch besteht in dessen vollständiger Kostenfreiheit und gleichzeitiger Verwendung der Apache License Version 2, wodurch die kommerzielle Verwendung vollumfänglich möglich ist.

Security Onion

Security Onion ist eine von Security Onion Solutions, LLC entwickelte freie Open-Source Plattform für Threat Hunting, Netzwerksicherheitsüberwachung und Protokolldatenverwaltung. Security Onion bündelt diverse andere FOOS-Tools [56].

Security Onion bietet Netzwerk- und Hostüberwachungsfunktionen, Honeypots, Protokolldatenverwaltung und Case Management Funktionen auf Basis von Tools wie Suricata, Zeek und ElasticSearch (siehe OpenSearch).

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Security Onion am 29. Mai 2024 statt [57]. Somit wird das System aktiv entwickelt.

Security Onion ist vollständig kostenfrei, auf der Webseite werden über die Software hinaus fertig konfigurierte Hardware-Pakete sowie Training, Premium Support und Zertifizierungen angeboten [56].

Security Onion ist unter der Elastic License 2.0 lizensiert, die kommerzielle Nutzung gestattet, aber die Nutzung einschränkt. So darf die Anwendung nicht als gehosteter oder gemanagter Service bereitgestellt werden, wenn Anwender Zugang zu einem bedeutenden Anteil der Softwarefunktionen erhalten. Enthaltene Lizenzschlüsselfunktionen dürfen nicht verändert oder anderweitig umgangen werden, ebenso darf die Lizensierung und das Urheberrecht in der Software nicht verschleiert, entfernt oder verborgen werden [58]. So kann Security Onion innerhalb eines Unternehmens verwendet werden, es muss allerdings beachtet werden, dass die Software nicht als Service für externe Kunden bereitgestellt wird.

Die Anforderungsanalyse von Security Onion anhand dessen Dokumentation [59] wird in Anlage 11 detailliert durchgeführt.

Security Onion wirbt mit Funktionen in den Bereichen Protokollierung und Detektion und wird daher in diesen Bereichen geprüft. Von den 11 anwendbaren Anforderungen zur Protokollierung erfüllt Security Onion 11 und von den 21 anwendbaren Anforderungen zur Detektion 18.

Security Onion zeigt Schwächen in dem Fehlen von Möglichkeiten zur Erkennung von Schadcode.

Der große Vorteil von Security Onion liegt im großen Funktionsumfang, was Detektions- und Analysewerkzeuge betrifft, bei gleichzeitiger Kostenfreiheit.

4.2.3 NIDS

Die NIDS dienen der Erfüllung der Anforderung Nummer 95, welche diese Systeme explizit fordert [4, S. 11], siehe Anlage 3) Darüber hinaus können NIDS als Mittel zur Erfüllung der Anforderungen Nummer 9 und 13 dienen, welche für Systeme, die nicht in der Lage sind ausreichend selbst zu protokollieren oder dies im Interesse der Verfügbarkeit der kritischen Dienstleistung nicht sollten, adäquaten Ersatz durch Detektion von sicherheitsrelevanten Ereignissen auf Netzwerkebene bieten [4, S. 9], siehe Anlage 2).

Snort

Snort ist ein Intrusion Prevention System, das anhand eines Regelwerks Netzwerkpakete prüft und im Falle eines Treffers Alerts erzeugt. Über eine Alarmierung hinaus kann Snort auch in eine Netzwerkverbindung zwischengeschaltet werden, um Pakete anhand von Regeltreffern zu verwerfen und so schadhaftes Verhalten zu unterbinden.

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Snort am 06. Juni 2024 statt [60]. Somit wird das System aktiv entwickelt.

Snort ist kostenfrei, es werden jedoch unterschiedliche vordefinierte Regelwerke für alle Anwender (Community), registrierte Anwender (Registered) und zahlende Anwender (Subscription) angeboten [61].

Snort lizensiert die Snort Engine und die Community Snort Rules unter der GNU General Public License Version 2, die keine Einschränkungen der kommerziellen Nutzung der Software vornimmt [62]. Die proprietären Snort Rules (Community und Registered) wiederum sind unter der „Non-Commercial Use License for the Proprietary Snort Rules“ Lizenz verfügbar. Diese erlaubt zwar die Kopie, Modifizierung und Verteilung des Quellcodes der proprietären Snort Rules, allerdings nicht zum Zweck einer kommerziellen Gewinnerzielung [62].

Als NIDS wird Snort nicht dediziert für einen der Anforderungsbereiche der OH-SzA gefordert und wird daher nicht gegen deren Anforderungen geprüft. Die oben genannten Anforderungen, die zur Verwendung des Systemtyps NIDS führen, sind allein durch eine Basisfunktionalität des NIDS gegeben.

Suricata

Suricata ist eine von der Open Information Security Foundation entwickelte, weit verbreitete Open Source Netzwerkanalyse- und Bedrohungsdetektionssoftware [63]. Suricata bietet neben IDS/IPS Funktionen auch eine Protokollierung von Netzwerkereignissen eine einfache Integration mit Logmanagement-Systemen [64].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Suricata am 25. Juni 2024 statt [65]. Somit wird das System aktiv entwickelt.

Suricata ist als Software vollständig kostenfrei, auf der Webseite wird nur auf zusätzliche Trainingsangebote im Rahmen einer gebührenpflichtigen Konferenz verwiesen [66].

Suricata ist unter der GNU General Public License Version 2 lizensiert, die keine Einschränkungen der kommerziellen Nutzung der Software vornimmt. Für die Integration von Suricata in eigens vertriebene Produkte bietet Suricata über die

Open Information Security Foundation die Möglichkeit, andere Lizenzen zu beziehen [67].

Als NIDS wird Suricata nicht dediziert für einen der Anforderungsbereiche der OH-SzA gefordert und wird daher nicht gegen deren Anforderungen geprüft. Die oben genannten Anforderungen, die zur Verwendung des Systemtyps NIDS führen, sind allein durch eine Basisfunktionalität des NIDS gegeben.

Zeek

Zeek ist ein Open Source Plattform für Netzwerksicherheitsüberwachung, das vor 2018 „Bro“ genannt wurde. Zeek beobachtet und interpretiert Netzwerkverkehr in Protokolldaten, Dateien oder anderweitige Ausgaben, um sie zur Verarbeitung bereitzustellen [68].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von Zeek am 26. Juni 2024 statt [69]. Somit wird das System aktiv entwickelt.

Zeek ist vollständig kostenfrei es wird keine zahlungspflichtige Komponente oder Dienstleistung auf der Webseite genannt [68].

Zeek ist unter der BSD Lizenz lizensiert, die keine Einschränkung der kommerziellen Verwendung der Software inklusive der Verwendung in eigenen Produkten vornimmt. [70].

Als NIDS wird Zeek nicht dediziert für einen der Anforderungsbereiche der OH-SzA gefordert und wird daher nicht gegen deren Anforderungen geprüft. Die oben genannten Anforderungen, die zur Verwendung des Systemtyps NIDS führen, sind allein durch eine Basisfunktionalität des NIDS gegeben.

4.2.4 Security Orchestration, Automation and Response

Die SOAR Tools dienen vorrangig der Erfüllung der Anforderungen des Bereichs „Reaktion“ (siehe Kapitel 3.6).

Die SOAR-Systeme sollen eine automatisierte Reaktion auf von den Systemen

zur Detektion erkannte Sicherheitsvorfälle ermöglichen.

n8n.io

n8n ist eine Workflow-Automatisierungsplattform für technische Teams, die die Erstellung automatisierter Arbeitsabläufe mit Code oder grafischem Editor ermöglicht. n8n ist für diverse Anwendungsfälle flexibel einsetzbar, wirbt aber explizit mit dem Anwendungsfall SecOps (Security Operations) [71].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von n8n am 21. Juni 2024 statt [72]. Somit wird das System aktiv entwickelt.

n8n ist in einer kostenfreien, eingeschränkten Community Edition verfügbar und mit den Editionen Starter, Pro und Enterprise in verschiedenen Funktionsumfängen und Volumen bezüglich Workflow-Ausführungen [73]. Für die Auswertung werden ausschließlich die Funktionen der Community Edition berücksichtigt.

n8n verwendet für die zu bezahlenden Anteile die n8n Enterprise License, die Anteile der Community Edition sind unter der Sustainable Use License lizensiert. Diese erlaubt die Verwendung der Software ausschließlich innerhalb eines Unternehmens oder zu nicht-kommerziellen oder persönlichen Zwecken [74]. Somit ist die interne Verwendung der Community Edition innerhalb eines Unternehmens zulässig.

Die Anforderungsanalyse von n8n anhand dessen Dokumentation [75] wird in Anlage 12 detailliert durchgeführt.

n8n wirbt mit Funktionen zur Workflow-Automatisierung und wird daher nur im Bereich der Reaktion geprüft. Von der 1 anwendbaren übergreifenden Anforderung erfüllt n8n 1 und von den 4 anwendbaren Anforderungen zur Reaktion 4.

Die Stärke von n8n.io liegt in dessen Flexibilität, die Anwendungsfälle über SOAR hinaus ermöglicht, womit auch explizit geworben wird.

Die Schwäche von n8n.io liegt insbesondere in den Funktions- und Volumeneinschränkungen der verschiedenen Editionen, die den Nutzen der Community Edition in der produktiven Nutzung stark einschränken.

Shuffle

Shuffle ist eine Automatisierungslösung für die Erstellung und das Teilen von Security-Workflows, die mittels grafischer Editoren oder Code eine Automatisierung der Prozesse ermöglicht. Shuffle liefert Vorlagen für die Erstellung von Automatisierungen mit und bietet über 2000 Apps bzw. Integrationen, wobei eigene mit einem No-Code App Ersteller geschaffen werden können [76].

Zum Zeitpunkt des Zugriffs fand die letzte Änderung am Quellcode von n8n am 20. Juni 2024 statt [77]. Somit wird das System aktiv entwickelt.

Shuffle unterscheidet grundsätzlich zwischen Cloud-Deployments und selbst gehosteten Installationen. In der Cloud wird ein auf 10000 App-Ausführungen beschränkter, kostenfreier Service namens „Build“, sowie „Grow“ mit zusätzlichen Ausführungen, Multimandantenfähigkeit und verbessertem Support angeboten. Für die selbst gehostete Installation wird zwischen „Build“ ohne Nutzungseinschränkungen oder „Speed & Scale“ mit Hochverfügbarkeits-Optionen und einem Preis abhängig von der Anzahl eingesetzter CPU-Kerne angeboten. Da es kostenfrei und unbegrenzt sowie die aktuell vorhandenen fachlichen Features alle beinhaltet sind, wird hier die Edition „Build“ zur selbst gehosteten Installation geprüft [76].

Shuffle ist unter der GNU Affero General Public License Version 3 lizensiert. Diese schränkt die Verwendung zu kommerziellen Zwecken nicht ein, erfordert jedoch bei Zugänglichmachung des Systems auch über das Netzwerk eine Veröffentlichung des Quellcodes [78]. Somit ist die interne Verwendung der „Build“ Version zu kommerziellen Zwecken vollständig zulässig, wobei die Veröffentlichung und Verfügbarmachung des Quellcodes erfolgen muss.

Die Anforderungsanalyse von Shuffle anhand dessen Dokumentation [76] wird in

0 detailliert durchgeführt.

Shuffle wirbt mit Funktionen zur Security Workflow Automatisierung und wird daher nur im Bereich der Reaktion geprüft. Von der 1 anwendbaren übergreifenden Anforderung erfüllt Shuffle 1 und von den 4 anwendbaren Anforderungen zur Reaktion 4.

Shuffles Stärke liegt im vollständigen Funktionsumfang der Build-Edition bei eigener Installation sowie der bestehenden Integrationen mit einer Vielzahl anderer IT-Sicherheitswerkzeuge.

Die Schwäche von Shuffle liegt in den nichtfunktionalen Einschränkungen der Build-Edition bezüglich Hochverfügbarkeit und Leistung, wobei die Build-Edition für kleinere Anwendungsszenarien ohne Hochverfügbarkeits-Anforderungen ausreichend scheint.

4.2.5 Übersicht und Auswahl

Tabelle 1 listet die bewerteten FOSS-Tools nach Systemtyp und im jeweiligen Bereich erfüllten Anforderungen auf. Die fett geschriebenen Systeme werden für den entsprechenden Bereich im Prototyp exemplarisch umgesetzt und detaillierter geprüft. Die Auswahl einzelner Systeme gegenüber ihren Alternativen wird im Folgenden begründet.

Tabelle 1 - Übersicht und Auswahl von Open Source Tools

System	Systemtyp	Bereich	Anforderungen	Erfüllt
Logstash	Logmanagement	Protokollierung	11	8
Graylog Open	Logmanagement	Protokollierung	11	6
Fluentd	Logmanagement	Protokollierung	11	7
Wazuh	SIEM	Protokollierung	11	9

Wazuh	SIEM	Detektion	21	19
Wazuh	SIEM	Reaktion	4	4
OpenSearch	SIEM	Detektion	21	17
Security Onion	SIEM	Protokollierung	11	11
Security Onion	SIEM	Detektion	21	18
Snort	NIDS	-	-	-
Suricata	NIDS	-	-	-
Zeek	NIDS	-	-	-
n8n.io	SOAR	Reaktion	4	4
Shuffle	SOAR	Reaktion	4	4

Wazuh bietet Funktionen sowohl im Bereich der Protokollierung als auch der Detektion und hat in der theoretischen Bewertung der Anforderungen in beiden Bereichen einen höheren Erfüllungsgrad als Konkurrenzlösungen. Durch die höhere Bewertung und die Möglichkeit, beide Bereiche abzudecken, wird Wazuh sowohl für die Protokollierung als auch die Detektion verwendet. Darüber hinaus sind mit Wazuh alle vorhandenen Funktionen vollständig kostenfrei verfügbar. Zwar erfüllt Wazuh auch die Anforderungen an Reaktion, allerdings ist die Reaktions-Funktion nur über den Wazuh Agenten gegeben, was die Reaktionsmöglichkeiten auf kompatible Endpunkte, also vorrangig Windows- und übliche Linux-Systeme, einschränkt.

Um eine möglichst umfassende Kompatibilität mit in Reaktionen relevanten Systemen zu erreichen, wird Shuffle verwendet. Zwar erfüllen sowohl n8n.io als

auch Shuffle die Anforderungen zur Reaktion gleichermaßen, allerdings ist für Shuffle eine fertige Integration für Wazuh [79] vorhanden. Darüber hinaus ist die kostenfreie selbst gehostete Variante von Shuffle anders als n8n.io nicht in Volumen oder Funktionen eingeschränkt.

Gleichermaßen könnten alle aufgeführten NIDS für die Anforderungserfüllung zum Einsatz kommen. Um die Prototypisierung möglichst zu vereinfachen, wird als NIDS Suricata eingesetzt, da Wazuh selbst eine Proof of Concept Anleitung für die Integration von Suricata als Datenquelle bietet [80].

Im Prototypen kommen zur Anforderungserfüllung also Wazuh, Shuffle und Suricata zum Einsatz.

5 Prototypische Umsetzung der OH-SzA mittels Open Source Tools

In diesem Kapitel wird zuerst ein exemplarisches, fiktives KMU orientiert an der „Recplast GmbH“ des BSI als Grundlage für eine Prototypisierung beschrieben. Dabei werden Anpassungen an der Recplast GmbH vorgenommen, um wo möglich die Komplexität des Prototyps zu reduzieren, ohne der Vergleichbarkeit der Ergebnisse zu schaden.

Anschließend werden erforderliche organisatorische Maßnahmen im exemplarischen KMU anhand der Anforderungen der OH-SzA beschrieben. Dabei wird keine exemplarische Umsetzung der Anforderungen beispielsweise anhand von detaillierten Prozessdefinitionen getroffen, sondern eine theoretische Beschreibung der erforderlichen Maßnahmen gegeben, da im Betrachtungsmittelpunkt dieser Arbeit die technische Umsetzbarkeit der OH-SzA mittels FOSS steht.

Danach erfolgt die technische Umsetzung des Prototypen in einer virtuellen Umgebung. Hierbei wird zunächst die Einrichtung der virtuellen Testumgebung beschrieben, woraufhin in jeweils einem eigenen Unterkapitel für jeden Systemtyp das FOSS Tool installiert und konfiguriert wird, das in Kapitel 4.2.5 ausgewählt wurde.

5.1 Fiktives KMU als Prototyp

Das BSI beschreibt zur exemplarischen Darstellung der IT-Grundschutz-Methodik ein fiktives Beispielunternehmen namens „RECPLAST GmbH“. Für dieses Unternehmen werden neben der Beschreibung Referenzdokumente bereitgestellt, die die für eine Absicherung des Unternehmens nach IT-Grundschutz-Methodik [81] relevant sind.

Durch die umfassende Beschreibung des Unternehmens sowie dessen Informationsverbundes und Richtlinien ist die RECPLAST GmbH als Vorlage für

die Umsetzung der Anforderungen der OH-SzA gut geeignet und wird sowohl auf Basis ihrer Richtlinien und Strukturanalyse bzw. technischen Beschreibung als Grundlage für den Prototypen verwendet.

Die RECPLAST GmbH „produziert und vertreibt […] unterschiedliche, aus Recyclingmaterialien gefertigte Kunststoffprodukte […], teils in größeren Serien für Endkunden, teils spezifisch für einzelne Geschäftskunden“ [82, S. 6], mit einem Gesamtumsatz von ca. 50 Millionen und einem Gewinn von ca. einer Million Euro [82, S. 6]. Das Unternehmen teilt sich in die Abteilungen Verwaltung, Einkauf, Produktion, Marketing und Vertrieb sowie Lager und Logistik. Die Abteilungen sind der Geschäftsführung unterstellt, der wiederum als Stabsstelle ein Datenschutzbeauftragter, Informationssicherheitsbeauftragter und ICS-Informationssicherheitsbeauftragter unterstellt sind [82, S. 7].

Das Netz der RECPLAST GmbH teilt sich zwei Standorte auf, die über eine Standleitung verbunden sind. Dieses Netz ist wird in Bild 1 [82, S. 8] grafisch dargestellt. Der Standort Bonn Bad-Godesberg beinhaltet eine DMZ, zu der aus dem Internet mittels VPN eine Verbindung von den Vertriebsstandorten in Berlin, München und Paderborn möglich ist. Innerhalb der Standorte Bonn Bad-Godesberg und Bonn Beuel sind Clients für Anwender, Server und TK-Anlagen neben Netzwerkinfrastruktur wie Switchen, Routern, einer Firewall, Cloudservern und ReCoBS (Remote-Controlled Browsers System, vgl. [83] platziert.

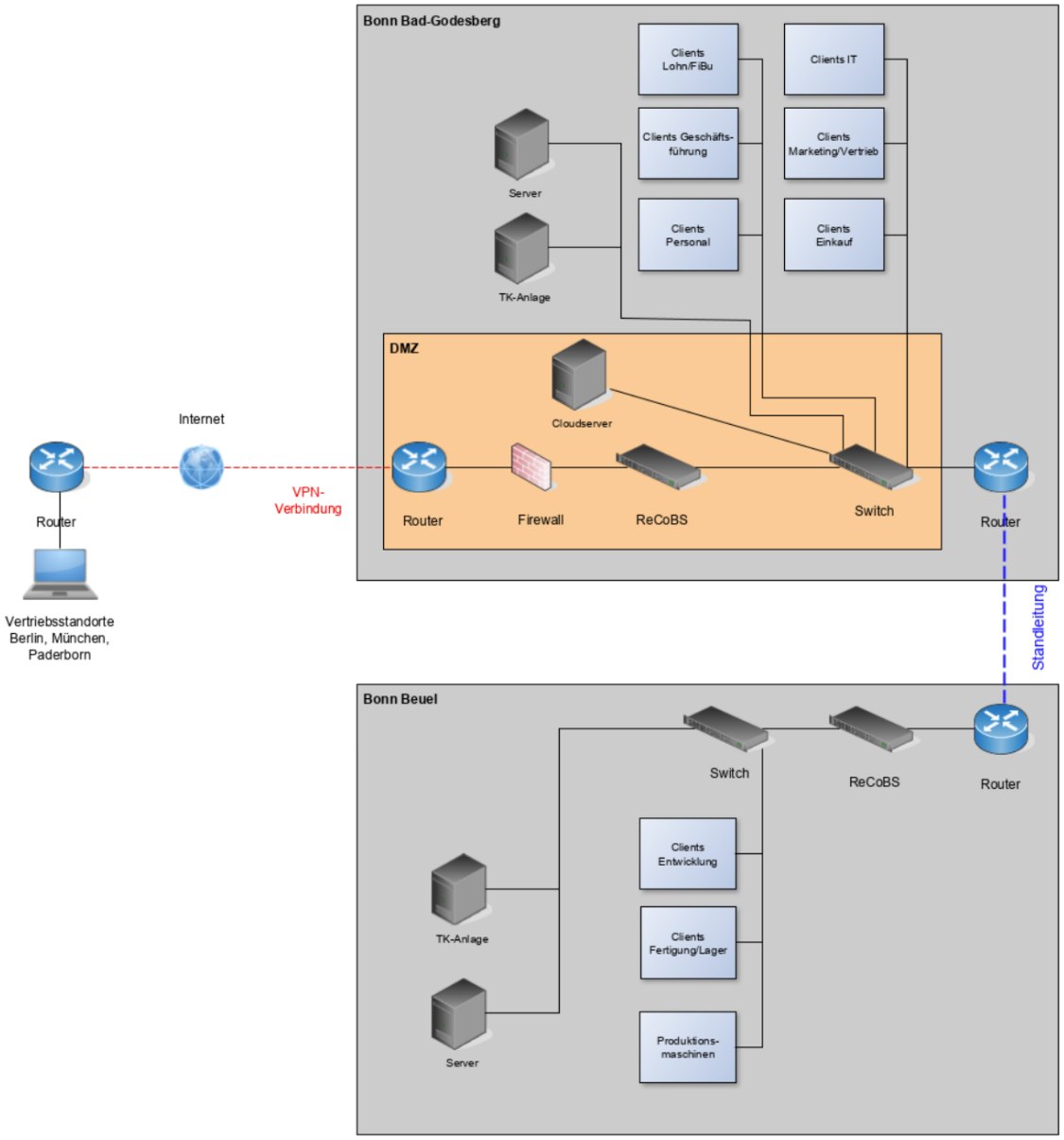

Bild 1 - Netzplan der RECPLAST GmbH [82, S. 8]

Die Clients sind mit Windows 10 als Betriebssystem ausgestattet, die Server sind unterschiedlich als Windows- und Linux-Systeme ausgestaltet [82, S. 9].

5.2 Theoretische Umsetzung organisatorischer Anforderungen

Neben den durch die Systeme zur Angriffserkennung selbst umsetzbaren Anforderungen, definiert die OH-SzA eine Reihe an Anforderungen, die nicht technisch zu lösen sind, sondern prozessualer oder organisatorischer Art sind

oder andere Systeme betreffen. Für diese Anforderungen wird in diesem Unterkapitel eine theoretische Umsetzung anhand der Organisationsbeschreibungen des BSI über die RECPLAST GmbH vorgenommen, indem Maßnahmen definiert, beschrieben und Anforderungen zugeordnet werden. Dabei wird auf Details der Umsetzung wie die konkrete Ausgestaltung von Prozessen verzichtet.

Hier werden all jene Anforderungen betrachtet, die in Anlage 1 bis Anlage 4 als nicht anwendbar markiert sind. Die Anforderungen werden, wo sinnvoll, gruppiert behandelt, wobei auch Anforderungen unterschiedlicher Bereiche gruppiert werden können. Zur besseren Darstellung der zugrunde liegenden Anforderungen wird zu jeder Maßnahmenbeschreibung die entsprechende Anforderung mit der in den genannten Anlagen vergebenen Nummer referenziert.

5.2.1 Übergreifend

Maßnahme	Etablierung eines kontinuierlichen Verbesserungsprozesses
Anforderungen	Das Umsetzungsgradmodell der OH-SzA fordert die Etablierung eines kontinuierlichen Verbesserungsprozesses [4, S. 15]. Eine explizite Anforderung dazu existiert außerhalb des Umsetzungsgradmodells nicht.
Beschreibung	Für die Bereiche Protokollierung, Detektion und Reaktion wird ein Prozess etabliert, der eine kontinuierliche Verbesserung der Bereiche in der RECPLAST GmbH erzeugt. Hierfür werden die Technologien, Prozesse und Organisationsstrukturen der Bereiche jährlich auf Verbesserungsmöglichkeiten geprüft und diese eingeplant, sowie innerhalb der Bereiche regelmäßig „Lessons

	Learned“ Besprechungen durchgeführt. Dabei werden beispielsweise in der Detektion nach jedem erkannten Sicherheitsvorfall die zugehörigen Detektionsmechanismen dahingehend geprüft, ob Bedarf zur Erweiterung oder Tuning besteht, um künftige Vorfälle zuverlässiger zu erkennen. Im Falle einer Erweiterung kann sich dies in Form eines Bedarfs nach weiteren Protokolldaten auf die Protokollierung auswirken. Der kontinuierliche Verbesserungsprozess zur Reaktion wird in Kapitel 5.2.4 beschrieben.

Tabelle 2 - Maßnahme "Etablierung eines kontinuierlichen Verbesserungsprozesses"

Maßnahme	Aufnahme der SzA in den IT-Betrieb
Anforderungen	3
Beschreibung	Die im Rahmen der anderen Bereiche eingeführten oder bestehende Hard- und Software, die für die Angriffserkennung erforderlich sind, werden innerhalb des GP007 „IT-Betrieb“ [84] in die laufende Pflege aufgenommen, sodass sie immer auf dem aktuellen Stand gehalten werden.

Tabelle 3 - Maßnahme "Aufnahme der SzA in den IT-Betrieb"

5.2.2 Protokollierung

Maßnahme	Erstellung einer Richtlinie zur Protokollierung
Anforderungen	1, 21-34, 38-41, 46
Beschreibung	Ausgehend von der Leitlinie zur Informationssicherheit [85] der RECPLAST GmbH wird eine spezifische Richtlinie zur

	Protokollierung erstellt (Anforderung 21). Diese Richtlinie definiert, wie Protokollierung aufzubauen, zu planen und zu betreiben ist (Anforderung 22). Die Richtlinie gibt vor, dass die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen für ihre Umsetzung geschaffen werden müssen (Anforderung 1) sowie die für die Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden muss (Anforderung 2). In der Richtlinie wird definiert, wie welches System was protokollieren soll (Anforderung 23). Im speziellen wird für diesen Prototypen festgelegt, dass mit dem Wazuh Agenten kompatible Systeme diesen installiert haben müssen und andere Systeme mittels Syslog direkt an den Wazuh Server senden müssen. Bezüglich der Protokollierungsinhalte wird sich am Schutzbedarf der Informationen orientiert (Anforderung 24). Dies bedeutet, dass die Richtlinie zwischen den für die RECPLAST GmbH definierten Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ [86, S. 5] differenzieren und entsprechend die Relevanz von Anwendungen und IT-Systeme für die Protokollierung und deren Protokollierungsumfang festlegt. Die Richtlinie wird vom ISB der RECPLAST GmbH gemeinsam mit den Fachverantwortlichen erstellt und allen für die Protokollierung zuständigen Mitarbeitern, also dem IT-Personal, bekannt gemacht (Anforderungen 25 und 26). In der Richtlinie wird festgelegt, dass Änderungen an ihr oder bei Abweichungen eine Abstimmung mit dem ISB und eine Dokumentation erfolgen muss (Anforderung 27). Der Umfang und die Dokumentation der internen ISMS-Auditierung [87, S. 5 f.] wird um eine Prüfung der korrekten

	Umsetzung der Richtlinie zur Protokollierung erweitert (Anforderung 28 und 29). Die Richtlinie gibt vor, dass alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen, die in der Richtlinie als relevant definiert sind, unter Beachtung der Vorgaben des Herstellers protokolliert werden müssen (Anforderung 30 bis 32). Die Richtlinie definiert Prüfintervalle, in denen stichpunktartig geprüft wird, ob die Protokollierung noch korrekt funktioniert (Anforderung 33 und 34). Für die RECPLAST GmbH wird alle zwei Wochen in einem rollierenden Verfahren eine Teilmenge aller im SIEM eingehender Protokolldatenquellen auf Vorhandensein und korrektes Format und Umfang der Protokolle geprüft. Die Richtlinie wird mit dem Datenschutzbeauftragten abgestimmt, um die Einhaltung von Datenschutzgesetzen sicherzustellen (Anforderung 38). Zur Wahrung der Persönlichkeitsrechte der Mitarbeiter und Mitbestimmungsrechte der Mitarbeitendenvertretung wird die Richtlinie auch mit dem nach Beschreibung der RECPLAST GmbH vorhandenen Betriebsrat [82, S. 11] abgestimmt (Anforderung 39). Zur Beachtung anderweitiger gesetzlicher Vorgaben wird sie auch mit der nach Beschreibung der RECPLAST GmbH vorhandenen Rechtsabteilung [82, S. 11] abgestimmt (Anforderung 40). Die Richtlinie legt einen verbindlichen Prozess zur Löschung von Protokollierungsdaten fest, der ein regelmäßiges Löschen von Protokollen mit einem höheren Alter als acht Wochen vorschreibt, um exzessive Speicherbedarfe zu vermeiden (Anforderung 41). Der

	Prozess berücksichtigt darüber hinaus die situative Löschung spezifischer Datensätze, um eventuelle Löschanfragen personenbezogener Datensätze bearbeiten zu können. Die Richtlinie legt fest, dass die notwendigen technischen, finanziellen und personelle Ressourcen für die definierte Protokollierung durch das Unternehmen bereitgestellt werden (Anforderung 46).

Tabelle 4 - Maßnahme "Erstellung einer Richtlinie zur Protokollierung"

Maßnahme	Synchronisation der Systemzeit der Protokolldatenquellen
Anforderungen	36, 96
Beschreibung	Die Systemzeit aller protokollierenden Systeme wird synchronisiert, indem eine gemeinsame Zeitquelle für alle IT-Systeme und Anwendungen der RECPLAST GmbH festgelegt wird (Anforderung 36). Hierfür wird ein NTP-Server aufgebaut, der allen protokollierenden Systemen als Zeitquelle dient. Dies ermöglicht eine chronologische Ordnung der Protokolldaten und den Nachvollzug zeitlicher Abläufe [88, S. 1]. Mit der Systemzeit werden auch die Zeitstempel der Protokolldaten zeitlich synchronisiert (Anforderung 96).

Tabelle 5 - Maßnahme "Synchronisation der Systemzeit der Protokolldatenquellen"

Maßnahme	Einführungsprojekt zur Protokollierung

Anforderungen	6-7, 10, 12, 14-18, 50-54
Beschreibung	Es wird ein Projekt gestartet, um die Einführung der Protokollierung umzusetzen. Das Projekt gliedert sich wie der Bereich Protokollierung der OH-SzA in eine Planungs- und Umsetzungsphase. Vor Projektstart wird auf über die OH-SzA hinausgehende branchenspezifische Anforderungen an die Protokollierung geprüft und diese in das Projekt aufgenommen (Anforderung 54). In der Planungsphase wird eine schrittweise Umsetzung der Protokollierung angedacht (Anforderung 6) und so aufgeteilt, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird (Anforderung 7). In der Planung werden alle Systeme identifiziert, die für die Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind (Anforderung 12). Im Falle der RECPLAST GmbH wird keine kritische Dienstleistung erbracht, allerdings sind die in der Strukturanalyse als Kerngeschäfts-Prozesse erkannten Prozesse und deren unterstützende Systeme für das Unternehmen kritisch. Die zur Speicherung notwendigen Systeme, also das SIEM, und deren IT-Sicherheitsvorkehrungen sind Teil der Planung (Anforderung 10). Für alle gemäß der Richtlinie zur Protokollierung anzubindenden Systemgruppen wird das Protokolldatenvolumen anhand eines repräsentativen Systems bestimmt (Anforderung 14). Die Planung wird dokumentiert, wobei alle Netzbereiche,

	deren Protokolldatenquellen, deren Beziehungen und der Datenfluss der Protokolldaten enthalten ist (Anforderung 15 und 16). Die Systeme werden dabei nach Typ und Verwendungszweck gruppiert, um die Bewertung des Einsatzes von SzA zu vereinfachen (Anforderung 17). Auch wird für jede Systemgruppe dokumentiert, welche Ereignisse diese protokolliert sowie das bestimmte anfallende Volumen (Anforderung 18). In der Umsetzung geht das Projekt auf Netzebene von außen nach innen vor (Anforderung 50), auf der Systemebene ausgehend von den zuvor identifizierten kritischen Systemen (Anforderung 51). Die Priorisierung der Protokolldatenquellen wird dabei von ihrem Schutzbedarf gemäß der Strukturanalyse abgeleitet (Anforderung 52). Nach Umsetzung des Projektes wird geprüft, ob die Umsetzung aller Protokolldatenquellen gemäß Planung erfolgt ist (Anforderung 53).

Tabelle 6 - Maßnahme "Einführungsprojekt zur Protokollierung"

Maßnahme	Anpassung der IT-Betriebsprozesse
Anforderungen	19
Beschreibung	Der Prozess IT-Betrieb (GP007, vgl. [84] und seine Unterprozesse werden dahingehend erweitert, dass bei Veränderungen der IT die Protokollierung entsprechend angepasst wird – also neue Systeme aufgenommen werden oder bei Updates, die die Protokollierung beeinflussen, eine entsprechende Anpassung im SIEM stattfindet.

Tabelle 7 - Maßnahme "Anpassung der IT-Betriebsprozesse"

Maßnahme	Festlegung der Protokollierungsinfrastruktur
Anforderungen	44-45
Beschreibung	Für die Speicherung der Protokolldaten wird das SIEM als zentrale Stelle definiert, sodass alle erfassten Protokolldaten dort gebündelt zugreifbar sind (Anforderung 44). Das SIEM wird dabei ausreichend dimensioniert, um die im Einführungsprojekt zur Protokollierung bestimmten Protokolldatenvolumen speichern und auswerten zu können (Anforderung 45).

Tabelle 8 - Maßnahme "Festlegung der Protokollierungsinfrastruktur"

5.2.3 Detektion

Maßnahme	Erstellung einer Richtlinie zur Detektion
Anforderungen	1, 60-68, 125
Beschreibung	Ausgehend von der Leitlinie zur Informationssicherheit [85] der RECPLAST GmbH wird eine spezifische Richtlinie zur Detektion von sicherheitsrelevanten Ereignissen erstellt (Anforderung 60). Die Richtlinie gibt vor, dass die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen für ihre Umsetzung geschaffen werden müssen (Anforderung 1) sowie die für die Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden muss (Anforderung 2).

	Diese Richtlinie definiert, wie die Detektion sicherheitsrelevanter Ereignisse aufzubauen, zu planen und zu betreiben ist (Anforderung 61). Die Richtlinie wird allen für die Detektion zuständigen Mitarbeitern bekannt gemacht (Anforderung 62). In der Richtlinie wird festgelegt, dass Änderungen an ihr oder bei Abweichungen eine Abstimmung mit dem ISB und eine Dokumentation erfolgen muss (Anforderung 63). Der Umfang und die Dokumentation der internen ISMS-Auditierung [87, S. 5 f.] wird um eine Prüfung der korrekten Umsetzung der Richtlinie zur Detektion von sicherheitsrelevanten Ereignissen erweitert (Anforderungen 64 und 65). Die Richtlinie wird mit dem Datenschutzbeauftragten abgestimmt, um die Einhaltung von Datenschutzgesetzen sicherzustellen (Anforderung 66). Zur Wahrung der Persönlichkeitsrechte der Mitarbeiter und Mitbestimmungsrechte der Mitarbeitendenvertretung wird die Richtlinie auch mit dem nach Beschreibung der RECPLAST GmbH vorhandenen Betriebsrat [82, S. 11] abgestimmt (Anforderung 67). Zur Beachtung anderweitiger gesetzlicher Vorgaben wird sie auch mit der nach Beschreibung der RECPLAST GmbH vorhandenen Rechtsabteilung [82, S. 11] abgestimmt (Anforderung 68). Branchenspezifische weitergehende gesetzliche oder regulatorische Anforderungen werden in die Richtlinie mit aufgenommen (Anforderung 125).

Tabelle 9 - Maßnahme "Erstellung einer Richtlinie zur Detektion"

Maßnahme	Etablierung eines Melde- und Alarmierungsprozesses

Anforderungen	69-75
Beschreibung	Es wird ein Melde- und Alarmierungsprozess etabliert, der ausführliche Schritte beinhaltet (Anforderung 74). In diesem Prozess werden geeignete Melde- und Alarmierungswege festgelegt und dokumentiert (Anforderung 69) sowie bestimmt, welche Stellen wann zu informieren sind (Anforderung 70) und wie die jeweiligen Personen erreicht werden können (Anforderung 71). Abhängig von der Dringlichkeit werden verschiedene Kommunikationswege genutzt (Anforderung 72), wie direkte Anrufe für kritische Ereignisse und E-Mails für nicht kritische. Alle für die Meldung relevanten Personen werden über ihre Aufgaben gemäß des Prozesses informiert (Anforderung 73). Die eingerichteten Melde- und Alarmierungswege werdem regelmäßig geprüft, erprobt und aktualisiert (Anforderung 75).

Tabelle 10 - Maßnahme "Etablierung eines Melde- und Alarmierungsprozesses"

Maßnahme	Schulung der Mitarbeitenden
Anforderungen	76-78, 100
Beschreibung	Alle IT-Benutzenden werden dahingehend geschult, dass sie Ereignismeldungen ihrer Clients nicht einfach ignorieren oder schließen (Anforderung 76), sondern entsprechend der Alarmierungswege an das verantwortliche Incident

	Management weitergeben (Anforderung 77) sowie einen von ihnen erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden (Anforderung 78). Mitarbeitende werden außerdem darin geschult, Meldungen über sicherheitsrelevante Ereignisse als solche zu erkennen und an die richtige Stelle weiterzuleiten (Anforderung 100).

Tabelle 11 - Maßnahme "Schulung der Mitarbeitenden"

Maßnahme	Konfiguration der Detektion auf eingesetzten IT-Systemen
Anforderungen	5, 79
Beschreibung	Die auf eingesetzten IT-Systemen vorhandenen Funktionen zur Detektion sicherheitsrelevanter Ereignisse werden aktiviert (Anforderung 79), zum Beispiel der Windows Defender. Alle relevanten Systeme werden so konfiguriert, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen (Anforderung 5). Dies erfolgt typischerweise über die Installation des Wazuh Agenten oder die Aktivierung entsprechender Protokolldaten.

Tabelle 12 - Maßnahme "Konfiguration der Detektion auf eingesetzten IT-Systemen"

Maßnahme	Etablierung eines Security Operations Centers
Anforderungen	80-82, 86, 89-92, 104-107, 113, 122-124
Beschreibung	Es wird ein Personenkreis aus internen und/oder externen

	Mitarbeitern benannt, die für die Auswertung und Untersuchung von Ereignismeldungen und Protokolldaten zuständig sind (Anforderung 90 und 107). Dieser Personenkreis wird in der Praxis oft als „Security Operations Center“ bezeichnet. Für das SOC werden genügend personelle Ressourcen bereitgestellt (Anforderung 92). Das SOC ist speziell damit beauftragt, alle Protokolldaten auszuwerten (Anforderung 104), wobei dies die höchst priorisierte Aufgabe der SOC-Mitarbeiter ist (Anforderung 105). Hierfür erhalten die SOC-Mitarbeiter spezialisierte Schulungen (Anforderungen 106). Das SOC wertet bei einem sicherheitsrelevanten Vorfall die Meldungen der betroffenen und anderer IT-Systeme aus (Anforderungen 80 und 81). Es wertet alle eingehenden Meldungen aus und untersucht sie (Anforderung 86) innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne (Anforderung 89). Die Einleitung einer dem Bedarf entsprechenden Reaktion bei einem Alarm stellt das SOC ebenfalls sicher (Anforderung 113). Das SOC stellt durch seine manuellen und automatisierten Analysen sicher, dass nur qualifizierte SRE den Prozess der Reaktion auslösen (Anforderung 122 und 123). Auf Basis der während der Analysen gewonnenen Erkenntnisse passt das SOC die Detektionsmechanismen, darunter die Regeln im SIEM, an (Anforderung 124), um beispielsweise falsch positive Meldungen zu verringern. Darüber hinaus kontrolliert das SOC die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig (Anforderung 82). Für die aktive Suche nach

	sicherheitsrelevanten Ereignissen definiert das SOC Verfahrensanleitungen (Anforderung 91).

Tabelle 13 - Maßnahme "Etablierung eines Security Operations Centers"

Maßnahme	Einholen und Auswerten von Threat Intelligence
Anforderungen	2, 99, 101-103
Beschreibung	Es werden externe Quellen für die Gewinnung neuer Erkenntnisse über SRE für den eigenen Informationsverbund herangezogen (Anforderung 99). Hierfür bieten sich sogenannte „Threat Intelligence“ Quellen bereit, die dediziert Informationen über SRE und Bedrohungsakteure sammeln. Die Informationen zuverlässiger Quellen werden grundsätzlich ausgewertet (Anforderung 101). Hierzu eignen sich beispielsweise die Cyber-Sicherheitswarnungen des BSI [89]. In diesen und anderen Threat Intelligence Quellen sind in der Regel Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten beinhaltet, weshalb diese für die bei der RECPLAST GmbH eingesetzten Systeme über diese Quellen eingeholt werden (Anforderung 2). Alle eingelieferten Informationen werden auf Relevanz für die RECPLAST GmbH bewertet (Anforderung 102) und im entsprechenden Fall entsprechend dem Melde- und Alarmierungsprozess eskaliert (Anforderung 103). Es bietet sich an, für die Verkürzung von Meldewegen und zur Bündelung von IT-Sicherheitskompetenzen diese Aufgaben dem SOC zuzuweisen.

Tabelle 14 - Maßnahme "Einholen und Auswerten von Threat Intelligence"

Maßnahme	Etablierung eines Schwachstellenmanagements
Anforderungen	117
Beschreibung	Es wird ein Schwachstellenmanagementprozess geschaffen, indem fortlaufend Meldungen relevanter Stellen geprüft werden und in das Schwachstellenmanagement einfließen (Anforderung 117). In diesem Prozess wird eine Bewertung der Schwachstellen durchgeführt und abhängig von der Kritikalität sofort gepatcht bzw. mitigierende Maßnahmen ergriffen, im Rahmen des regulären Updatezyklus gepatcht oder das Risiko getragen.

Tabelle 15 - Maßnahme "Etablierung eines Schwachstellenmanagements"

Maßnahme	Einsatz zusätzlicher Detektionssysteme
Anforderungen	83, 94
Beschreibung	Es wird geprüft, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen (Anforderung 83). Dies ist vor allem dann empfehlenswert, wenn die IT-Systeme keine eigenen Schadcodescanner beinhalten (wie den Windows Defender). Auf Netzebene wird anhand des Netzplans festgelegt, welche Netzsegmente durch zusätzliche Detektionssysteme (wie NIDS) geschützt werden müssen (Anforderung 94). Empfehlenswert ist dies vor allem an Netzübergängen, auch internen.

Tabelle 16 - Maßnahme "Einsatz zusätzlicher Detektionssysteme“

Maßnahme	Kalibrierung der Detektionsmechanismen
Anforderungen	118-120
Beschreibung	Im Rahmen der Umsetzung von Detektionsmechanismen wie SIEM-Regeln wird initial eine Kalibrierung durchgeführt, um die im Normalzustand auftretenden SRE festzustellen (Anforderung 118). Dabei wird bewertet, ob die Anzahl falsch positiver Meldungen zu hoch ist und Änderungen erforderlich sind, oder hingenommen werden kann (Anforderung 119). Bei Änderungen der Systeme oder der Bedrohungslage wird erneut kalibriert (Anforderung 120).

Tabelle 17 - Maßnahme "Kalibrierung der Detektionsmechanismen"

Maßnahme	Bedrohungs- und Risikoanalyse
Anforderungen	55-56, 58
Beschreibung	Als Grundlage für die Auswahl von Detektionsmaßnahmen dient die Bedrohungslandschaft der RECPLAST GmbH, die möglichst umfassend und effizient abgedeckt werden muss (Anforderung 55). Hierzu werden Ergebnisse der Risikoanalyse und Strukturanalyse mit einbezogen (Anforderung 56). Nach Anforderung 58 kann in Abhängigkeit der Unternehmensgröße und Bedrohungslandschaft eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein, für die RECPLAST

	GmbH ist dies jedoch aufgrund der geringen Größe der OT-Umgebung nicht sinnvoll.

Tabelle 18 - Maßnahme "Bedrohungs- und Risikoanalyse"

5.2.4 Reaktion

Maßnahme	Erstellung einer Richtlinie zur Reaktion
Anforderungen	1, 128-145
Beschreibung	Ausgehend von der Leitlinie zur Informationssicherheit [85] der RECPLAST GmbH wird eine spezifische Richtlinie zur Behandlung von Sicherheitsvorfällen erstellt (Anforderung 132). Die Richtlinie gibt vor, dass die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen für ihre Umsetzung geschaffen werden müssen (Anforderung 1). Diese Richtlinie definiert ihren Zweck, ihr Ziel und regelt alle Aspekte der Behandlung von Sicherheitsvorfällen (Anforderung 133). Sie definiert klar, was ein Sicherheitsvorfall ist (Anforderung 128) und grenzt diesen so weit wie möglich von Störungen im Tagesbetrieb ab (Anforderung 129). Die Definition und Eintrittsschwellen eines Sicherheitsvorfalls richten sich dabei nach dem Schutzbedarf der betroffenen Geschäftsprozesse, Anwendungen und IT-Systeme (Anforderung 131). Sie definiert Verhaltensregeln für verschiedene Arten von

	Sicherheitsvorfällen (Anforderung 134) und gibt für alle Mitarbeitenden zielgruppenorientierte und praktische Handlungsanweisungen (Anforderung 135). Dabei berücksichtigt sie die Schnittstellen zu anderen Managementbereichen wie dem Notfallmanagement (Anforderung 136). Die Richtlinie wird mit dem IT-Betrieb abgestimmt und von der Geschäftsführung verabschiedet (Anforderung 138) sowie allen Mitarbeitenden bekannt gemacht (Anforderung 137). Somit ist die Definition eines Sicherheitsvorfalls allen an der Behandlung beteiligten Mitarbeitenden bekannt (Anforderung 130). Die Richtlinie wird regelmäßig überprüft und aktualisiert (Anforderung 139). Inhaltlich regelt die Richtlinie, wer bei Sicherheitsvorfällen wofür verantwortlich ist (Anforderung 140) und legt die Aufgaben und Kompetenzen aller Mitarbeitenden bei Sicherheitsvorfällen fest (Anforderung 141). Mitarbeiter, die Sicherheitsvorfälle bearbeiten sollen, werden gezielt über diese Aufgaben und Kompetenzen informiert (Anforderung 142). Zu forensischen Untersuchungen definiert die Richtlinie, wer eine Entscheidung zu ihnen trifft sowie nach welchen Kriterien und wann eine solche Entscheidung erfolgen soll (Anforderung 143). Die Ansprechpartner und Ansprechpartnerinnen für alle Arten von Sicherheitsvorfällen sowie deren Kontaktinformationen werden in dieser Richtlinie aufgeführt und sind somit allen Mitarbeitenden bekannt und zugänglich

	(Anforderung 144 und 145).

Tabelle 19 - Maßnahme "Erstellung einer Richtlinie zur Reaktion"

Maßnahme	Definition eines Prozesses zur Reaktion
Anforderungen	150-153, 156-170, 176-178, 183-193, 202, 204-219
Beschreibung	Es wird ein Prozess zur Behandlung von Sicherheitsvorfällen definiert (Anforderung 166), der die Abläufe für die verschiedenen Sicherheitsvorfälle eindeutig regelt und dokumentiert wird (Anforderung 167). Der Prozess wird von der Geschäftsführung in Kraft gesetzt und allen an der Behandlung beteiligten Mitarbeitenden zugänglich gemacht (Anforderung 168). Der Umfang und die Dokumentation der internen ISMS-Auditierung [87, S. 5 f.] wird um eine Prüfung der Aktualität und Wirksamkeit des Prozesses zur Reaktion erweitert (Anforderung 169), wobei der Prozess bei Bedarf angepasst wird (Anforderung 170). In diesem Prozess werden alle festgestellten Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen behandelt (Anforderung 228). Es wird eine zentrale Meldestelle für Störungen und Sicherheitsvorfällen eingerichtet und an alle Mitarbeitenden kommuniziert (Anforderung 176 und 178). Somit ist sichergestellt, dass Mitarbeitende Sicherheitsvorfälle schnell und einfach über einen verlässlichen Kanal melden können (Anforderung 177). Hierzu bietet sich ein Service Desk an. Dem Service Desk werden geeignete Hilfsmittel

	zur Erkennung von Sicherheitsvorfällen wie beispielsweise Checklisten und Inventarlisten zur Verfügung gestellt (Anforderung 204). Der Service-Desk wird in der selbstständigen Anwendung der Hilfsmittel geschult (Anforderung 205). Dem Service-Desk werden die Schutzbedarfe aller IT-Systeme zugänglich gemacht (Anforderung 206). Für ausgewählte Sicherheitsvorfallszenarien werden bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt (Anforderung 185) und entsprechende Vorüberlegungen zu geeigneten Maßnahmen durch das Sicherheitsvorfall-Team getroffen. Der Prozess definiert ein einheitliches Verfahren zur Einstufung von Sicherheitsvorfällen und Störungen (Anforderung 186), das zwischen dem Sicherheitsmanagement und dem Incident Management der IT abgestimmt ist (Anforderung 187). Dabei werden die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement analysiert (Anforderung 188) und eventuell gemeinsam benutzbare Ressourcen identifiziert (Anforderung 189). Die Mitarbeitenden der Störungs- und Fehlerbehebung werden für die Behandlung von Sicherheitsvorfällen und das Notfallmanagement sensibilisiert (Anforderung 190). Das Sicherheitsmanagement erhält lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge (Anforderung 191). Die Aktivitäten innerhalb des Prozesses werden mit dem Notfallmanagement und den Zuständigen für Störungs- und

	Fehlerbehebung abgestimmt (Anforderung 192 und 193). Die Checklisten für Störungs- und Fehlerbehebung werden regelmäßig um sicherheitsrelevante Themen ergänzt oder aktualisiert (Anforderung 202). Der Prozess regelt den Ablauf der Behandlung von Sicherheitsvorfällen. Zunächst wird das Problem eingegrenzt und die Ursache gefunden (Anforderung 150). Parallel zur Ursachenanalyse wird entschieden, ob es wichtiger ist, den Schaden einzudämmen oder den Vorfall aufzuklären (Anforderung 183). Für die Einschätzung der Auswirkungen und damit eine informierte Entscheidung über Aufklärung oder Eindämmung müssen ausreichend Informationen vorliegen (Anforderung 184), die Entscheidung kann also nicht bereits zu Beginn der Analyse getroffen werden. Wer die Entscheidung zur Aufklärung und damit forensischen Untersuchung trifft, wird in der Richtlinie zur Reaktion geregelt. Im Anschluss werden die erforderlichen Maßnahmen zur Behebung ausgewählt (Anforderung 151). Die Maßnahmen werden durch die Leitung des IT-Betriebs vor Umsetzung freigegeben (Anforderung 152). Anschließend wird die Ursache beseitigt und ein sicherer Zustand wiederhergestellt (Anforderung 153). Im Zuge dessen werden die betroffenen Komponenten vom Netz genommen (Anforderung 156) und alle erforderlichen Daten gesichert, die Aufschluss über Art und Ursache des Problems geben könnten (Anforderung 157). Hier sind insbesondere Protokolldaten aus dem SIEM zu betrachten. Auf allen betroffenen Komponenten werden Betriebssystem

	und Applikationen auf Veränderungen untersucht (Anforderung 158). Die entsprechenden Originaldaten werden von schreibgeschützten Datenträgern wieder eingespielt (Anforderung 159), wobei alle sicherheitsrelevanten Konfigurationen und Patches mit eingespielt werden (Anforderung 160). Dabei wird sichergestellt, dass die wieder einzuspielenden Datensicherungen nicht selbst vom Vorfall betroffen waren (Anforderung 161). Vor Wiederinbetriebnahme der betroffenen Komponenten werden alle Zugangsdaten auf diesen geändert (Anforderung 162) und sie einem Penetrationstest unterzogen (Anforderung 163). Zusätzlich werden Anwendungsfunktionstests unter Einbezug der Benutzenden durchgeführt (Anforderung 164). Nach Wiederinbetriebnahme werden die Komponenten inklusive der Netzübergänge gezielt überwacht (Anforderung 165), wozu eine Anpassung des Regelwerks im NIDS und SIEM verwendet werden kann. Die Dokumentation der Behebung von Sicherheitsvorfällen wird innerhalb des Prozesses geregelt, wobei ein standardisiertes Verfahren zur Anwendung kommt (Anforderung 207). In der Dokumentation sind alle durchgeführten Aktionen mit Zeitpunkten und die Protokolldaten der betroffenen Komponenten als Auszug aus dem SIEM enthalten (Anforderung 208). Die Berichte werden als vertrauliche Dokumente behandelt und entsprechend verwahrt und archiviert (Anforderung 209). Dabei kann, falls geeignet, das in der Eskalationsstrategie verwendete Ticket-System zum Einsatz kommen (siehe Maßnahme „Definition einer Eskalationsstrategie“). In

	dieses System werden die benötigten Informationen eingepflegt, bevor die Störung als beendet und abgeschlossen markiert wird (Anforderung 210). Die hierfür erforderlichen Anforderungen an die Qualitätssicherung werden mit dem oder der ISB definiert (Anforderung 211). Die Nachbereitung von Sicherheitsvorfällen wird im Prozess standardisiert geregelt (Anforderung 212). Dabei wird untersucht, wie schnell der Vorfall erkannt und behoben wurde (Anforderung 213), ob die Meldewege funktionierten und ausreichend Informationen für die Bewertung vorhanden sowie die Detektionsmaßnahmen wirksam waren (Anforderung 214). Die ergriffenen Maßnahmen und Aktivitäten werden auf Wirksamkeit und Effizienz bewertet (Anforderung 215). Im Rahmen der Nachbereitung werden die Erfahrungen aus den Sicherheitsvorfällen verwendet, um konkrete Handlungsanweisungen für vergleichbare Vorfälle zu erstellen (Anforderung 216). Insbesondere als wirksam und effizient erkannte Maßnahmen werden so als Standardvorgehen für künftige Vorfälle festgelegt. Die Handlungsanweisungen werden den Mitgliedern des SIRT (siehe Maßnahme „Etablierung eines Sicherheitsvorfall-Teams“) bekanntgegeben und regelmäßig aktualisiert (Anforderung 217). Die Geschäftsführung wird jährlich über alle Sicherheitsvorfälle unterrichtet (Anforderung 218). Bei sofortigem Handlungsbedarf wird sie umgehend informiert (Anforderung 219).

Tabelle 20 - Maßnahme "Definition eines Prozesses zur Reaktion"

Maßnahme	Etablierung eines Sicherheitsvorfall-Teams
Anforderungen	154-155, 171-175
Beschreibung	Für den Umgang mit Sicherheitsvorfällen wird als Organisationsstruktur ein Sicherheitsvorfall-Team (auch „Security Incident Response Team“, kurz „SIRT) aufgebaut (Anforderung 171), dessen Mitglieder je nach Art des Vorfalls einberufen werden (Anforderung 172). Die Mitglieder sind im Vorfeld benannt und gemäß Richtlinie zur Reaktion in ihre Aufgaben eingewiesen (Anforderung 173). Das SIRT ist somit für die Umsetzung des Prozesses zur Reaktion verantwortlich und beinhaltet alle daran beteiligten Mitarbeitenden. Es wird eine aktuelle Liste mit internen und externen Sicherheitsfachleuten gepflegt, die für Fragen aus den erforderlichen Themenbereichen hinzugezogen werden können (Anforderung 154). Diese Sicherheitsfachleute werden als Mitglieder im SIRT aufgenommen. Mit allen Mitgliedern des SIRT werden sichere Kommunikationsverfahren etabliert (Anforderung 155), indem zum Beispiel dedizierte Smartphones für diesen Anwendungsfall mit verschlüsselten Kommunikationsanwendungen eingesetzt werden, die von der restlichen IT-Infrastruktur der RECPLAST GmbH getrennt sind. Die Zusammensetzung des SIRT wird regelmäßig auf Angemessenheit geprüft (Anforderung 174) und das Team im Bedarfsfall neu zusammengestellt (Anforderung 175).

Tabelle 21 - Maßnahme "Etablierung eines Sicherheitsvorfall-Teams"

Maßnahme	Definition einer Kommunikations- und Kontaktstrategie
Anforderungen	146-149, 179-182
Beschreibung	Im Rahmen des Prozesses zur Reaktion wird eine Kommunikations- und Kontaktstrategie definiert (Anforderung 179), in der geregelt wird, wer in welcher Reihenfolge in welcher Tiefe informiert wird (Anforderung 180), wer Informationen über Sicherheitsvorfälle an Dritte weitergibt (Anforderung 181) und wie verhindert wird, dass unautorisierte Personen Informationen über den Sicherheitsvorfall weitergeben (Anforderung 182). Alle betroffenen internen und externen Stellen werden zeitnah informiert (Anforderung 146) und über die erforderlichen Maßnahmen in Kenntnis gesetzt (Anforderung 149), wobei geprüft wird, ob der oder die Datenschutzbeauftragte, der Betriebsrat und Mitarbeitende der Rechtsabteilung einbezogen werden müssen (Anforderung 147). Da die RECPLAST GmbH keiner regulierten Branche angehört oder eine Behörde ist, müssen keine entsprechenden Meldepflichten nach Anforderung 148 berücksichtigt werden.

Tabelle 22 - Maßnahme "Definition einer Kommunikations- und Kontaktstrategie"

Maßnahme	Definition einer Eskalationsstrategie

Anforderungen	194-201, 203, 229
Beschreibung	Im Rahmen des Prozesses zur Reaktion wird eine Eskalationsstrategie definiert (Anforderung 194), die zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem ISMS abgestimmt ist (Anforderung 195). Darin sind eindeutige Anweisungen enthalten, wer wie bei welcher Art von Sicherheitsvorfällen wann einzubeziehen ist (Anforderung 196) sowie zu welchen Maßnahmen eine Eskalation führt und wie reagiert werden soll (Anforderung 197). Für die Eskalation werden geeignete Werkzeuge definiert (Anforderung 198), die sich auch zur Verarbeitung vertraulicher Informationen eignen (Anforderung 199) und während eines Sicherheitsvorfalls oder Notfalls verfügbar bleiben (Anforderung 200). Hierzu bietet sich beispielsweise ein Ticket-System in einer von den restlichen Netzbereichen weitestmöglich abgegrenzten und gehärteten Umgebung an. Die Eskalationsstrategie wird im Rahmen der Prozessprüfung mit überprüft und aktualisiert (Anforderung 201). Die definierten Eskalationswege werden in Übungen regelmäßig erprobt (Anforderung 203). Da die RECPLAST GmbH kein Betreiber Kritischer Infrastrukturen ist, ist eine Prüfung der Meldepflicht von Sicherheitsvorfällen an das BSI nach Anforderung 229 nicht erforderlich, könnte allerdings im Rahmen der Eskalationsstrategie stattfinden.

Tabelle 23 - Maßnahme "Definition einer Eskalationsstrategie"

Maßnahme	Einrichtung eines kontinuierlichen

	Verbesserungsprozesses zu Reaktion
Anforderungen	220-223
Beschreibung	Es wird ein kontinuierlicher Verbesserungsprozess zur Reaktion etabliert. In diesem wird nach Analyse eines Sicherheitsvorfalls im Prozess zur Reaktion untersucht, ob der Prozess geändert oder weiterentwickelt werden muss (Anforderung 220). Dabei berichten alle beteiligten SIRT-Mitglieder über ihre Erfahrungen (Anforderung 221). Es wird geprüft, ob neue Entwicklungen im Bereich des Incident Managements oder Forensik in den Prozess zur Reaktion eingebracht werden können (Anforderung 222). Die Checklisten und Hilfsmittel des Service Desk und des SIRT werden auf sinnvolle Erweiterungen geprüft (Anforderung 223).

Tabelle 24 - Maßnahme "Einrichtung eines KVP zur Reaktion"

Maßnahme	Automatisierte Reaktion
Anforderungen	225-228
Beschreibung	Da die RECPLAST GmbH keine kritische Dienstleistung erbringt, wird in allen Netzen die Möglichkeit zum automatischen Eingriff in den Datenstrom geschaffen, um Sicherheitsvorfälle zu unterbinden (Anforderung 225). Hierzu werden geeignete Schnittstellen für die SzA wie das SOAR aktiviert, um beispielsweise Firewalls zu schließen oder Benutzerkonten im Active Directory zu sperren. Wo

	dies nicht möglich ist, wird mittels manueller Prozesse eine Unterbindung des Sicherheitsvorfalls sichergestellt (Anforderung 226), wie durch die Aufnahme von Systemadministratoren in das SIRT. Der Ausschluss von Netzen von einer automatisierten Reaktion muss schlüssig begründet sein (Anforderung 227), ist gemäß Anforderung 225 allerdings nur für solche Netze möglich, in denen die kritische Dienstleistung dadurch gefährdet wird. Für die RECPLAST GmbH ist ein solcher Ausschluss also nicht möglich.

Tabelle 25 - Maßnahme "Automatisierte Reaktion"

5.3 Technische Umsetzung

In diesem Unterkapitel wird die technische Umsetzung des Prototypen, also die Einrichtung der virtuellen Testumgebung entsprechend der Beschreibung in Kap. 5.1 und die Einrichtung der FOSS-Tools beschrieben.

5.3.1 Einrichtung der virtuellen Testumgebung

Für den Prototypen soll das Netz der RECPLAST GmbH (siehe Kapitel 5.1) vereinfacht repräsentiert werden, um die Erfüllbarkeit der Anforderungen der OH-SzA anhand der ausgewählten FOSS-Tools zu prüfen. Eine vollständige Replikation des Netzwerks der RECPLAST GmbH ist hierzu nicht erforderlich, weshalb auf eine vereinfachte Version zurückgegriffen wird.

Da mit dem Windows 10 Client bereits ein Windows-System enthalten ist, wird auf einen zusätzlichen Windows-Server verzichtet und als Server ein Linux-Server angenommen. Um zusätzliche weitere Komponenten wie Router und Produktionsmaschinen zu simulieren, wird eine virtuelle Firewall installiert, die mittels Syslog anstelle des Wazuh Agenten protokolliert. So wird das netzbasierte Protokollierungsverhalten nicht agentenfähiger Systeme simuliert.

Als virtuelle Firewall wird die Open Source Firewall OPNSense eingesetzt, die Protokollierungsfunktionen bietet [90]. OPNSense bietet ein integriertes Intrusion Prevention System auf Basis von Suricata [91], weshalb keine dedizierte Suricata-Instanz installiert, sondern die in OPNSense integrierte Funktionalität genutzt wird.

OPNSense bietet einen vollständigen Appliance-Installer, der das darunterliegende FreeBSD Betriebssystem mit installiert [92].

Wazuh empfiehlt unter anderem Ubuntu 22.04 als Betriebssystem [93], während Shuffle Docker als Installationsweg empfiehlt [94]. Für die Installation von Shuffle und Wazuh werden also als Basis Ubuntu 22.04 Server eingesetzt, wobei für Shuffle Docker mit installiert wird.

Die hieraus resultierende Systemliste der Testumgebung wird in Tabelle 26 aufgeführt.

System	Typ	Anzahl
Windows 10 Client	IT-System	1
OPNSense Firewall	IT-System	1
Ubuntu Server	IT-System	3
Wazuh	Anwendung	1
Shuffle	Anwendung	1

Tabelle 26 - Systemliste der Testumgebung

Die Testumgebung wird in verschiedene Netzzonen getrennt, um näherungsweise dem Aufbau der RECPLAST GmbH zu entsprechen. Die OPNSense Firewall dient als Router zwischen den einzelnen Netzzonen und bildet somit die Funktionen der Firewall und des Switches der RECPLAST GmbH nach. Für den Zugriff auf die Weboberfläche der Firewall wird ein dediziertes Netzwerkinterface verwendet. Der Netzplan der Testumgebung wird in Bild 2

gezeigt.

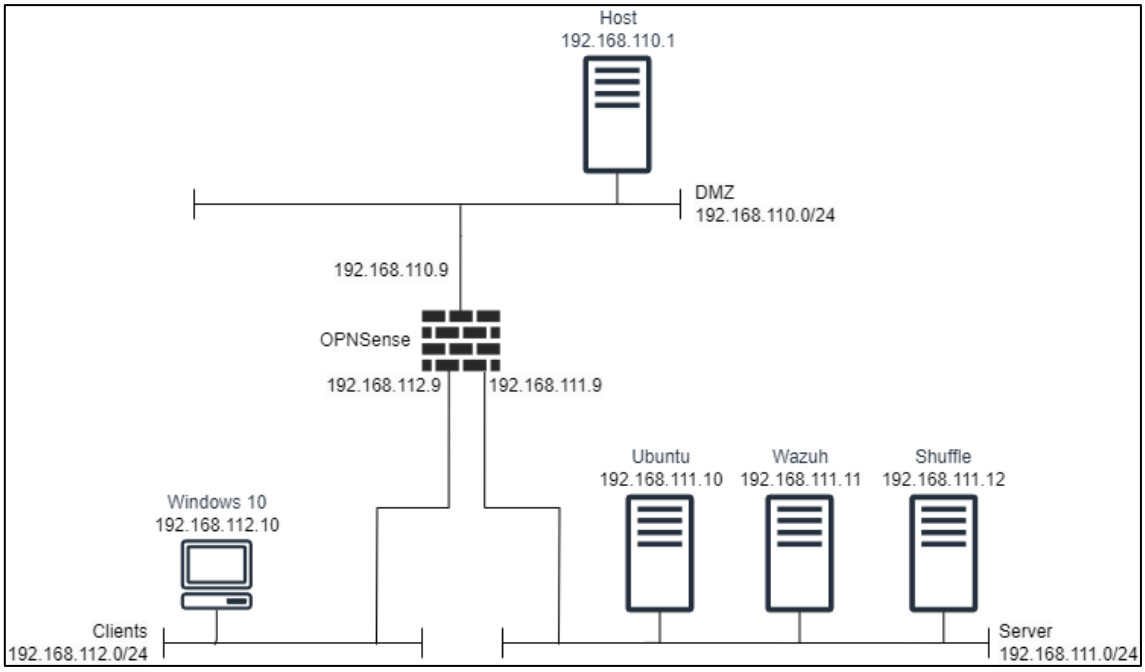

Bild 2 - Netzplan der Testumgebung des Prototyps

Als Host für die virtuelle Testumgebung wird ein Windows 10 System mit VMWare Workstation 17 Pro in der Version 17.5.2 verwendet, wie in Bild 3 ersichtlich.

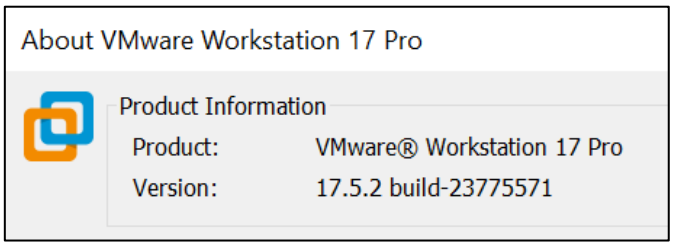

Bild 3 - Version von VMWare Workstation Pro

Die in Bild 2 dargestellten Netzbereiche werden im virtuellen Netzwerkeditor von VMWare Workstation nachgebildet. Dabei wird zur Verbindung der DMZ mit dem Host das Netzwerk als NAT-Netzwerk konfiguriert, das Server- und Clients-Netzwerk bleibt ohne externe Verbindung oder Verbindung zum Host. Die in

VMWare Workstation umgesetzte Netzwerkkonfiguration wird in Bild 4 dargestellt.

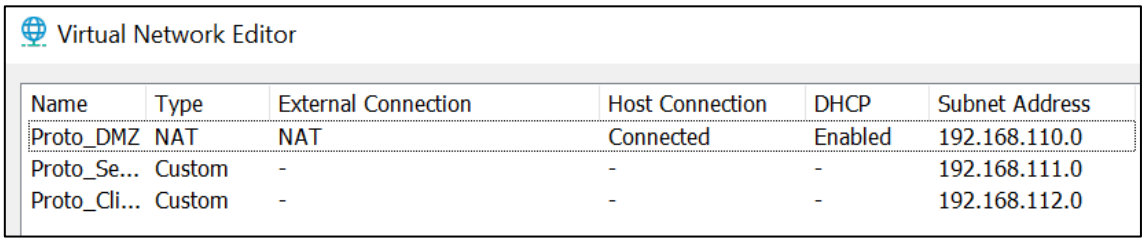

Bild 4 - Netzwerkkonfiguration in VMWare Workstation

Das Gateway der DMZ, die über NAT durch den Host auf externe Netze zugreifen kann, ist standardmäßig 192.168.110.2 (siehe Bild 5).

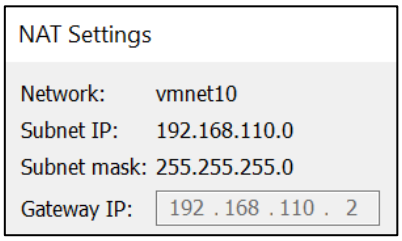

Bild 5 - NAT-Einstellungen des DMZ-Netzwerks

Als Installationsverzeichnis für alle VMs wird auf dem Host der Pfad „D:\VM“ angelegt.

Installation der OPNSense Firewall

Als Grundlage für die weiteren Arbeiten in den einzelnen Netzzonen der Testumgebung wird zuerst die OPNSense Firewall als verbindendes Element der Netzzonen installiert.

Der Installer von OPNSense wird auf der Webseite zum Download angeboten [95]. Dazu wird zur Integritätsprüfung des heruntergeladenen Installers eine SHA256-Prüfsumme angeboten, die wie in Bild 6 dargestellt auf dem Host erfolgreich geprüft wurde.

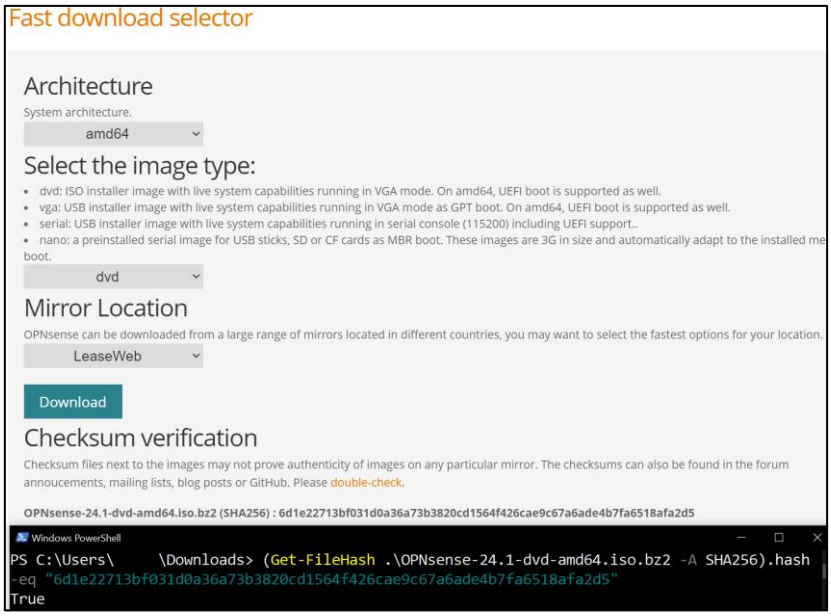

Bild 6 - Prüfsummenverifikation des OPNSense Installers

Die heruntergeladene Version von OPNSense, die in der folgenden Installation verwendet wird, ist OPNSense 24.1.

Die VM für OPNSense wird entsprechend der als „Reasonable“ definierten Hardware-Anforderungen mit zwei CPU-Kernen, 4 GB Arbeitsspeicher und 40 GB Speicher eingerichtet, da in der Minimalausstattung Funktionseinschränkungen von Suricata möglich sind [96].

Für die Anbindung an alle Netzbereiche wird die VM mit insgesamt vier Netzwerkadaptern ausgestattet, davon einer als Anbindung an den Host über die DMZ, einer als Interface für die Weboberfläche ebenfalls über die DMZ und jeweils einer für das Server- und das Client-Netzwerk.

Die heruntergeladene BZ2-Datei wird zu ISO entpackt und in das virtuelle CD-Laufwerk als Installationsmedium eingebunden.

Die vollständige Hardwareausstattung der OPNSense VM wird in Bild 7 gezeigt.

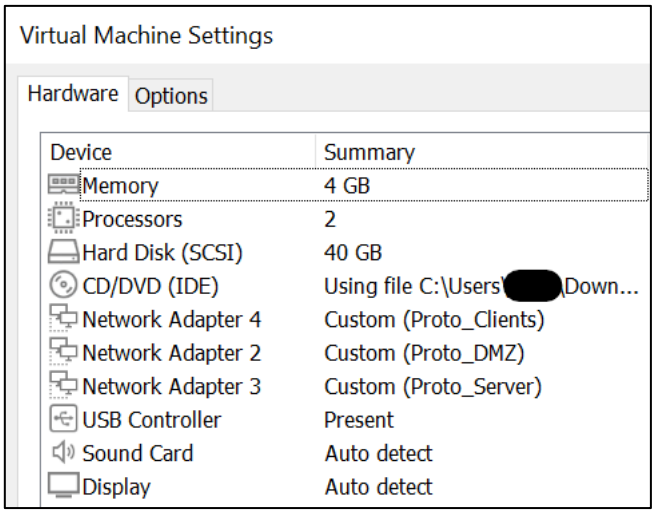

Bild 7 - Hardwareausstattung OPNSense

Die Installation beim ersten Start der VM mit der heruntergeladenen ISO-Datei erfolgt mittels des OPNSense Installers wie in der Installationsanleitung von OPNSense beschrieben [92]. Hierbei wird ZFS als Dateisystem gewählt. Da in dieser Testumgebung keine Redundanz erforderlich ist, wird ohne RAID-Konfiguration installiert.

Nach dem Login werden zunächst die Netzwerkschnittstellen zugewiesen. Im Anschluss werden die in Bild 2 definierten IP-Adressen den entsprechenden Netzwerkschnittstellen zugewiesen (siehe Bild 8).

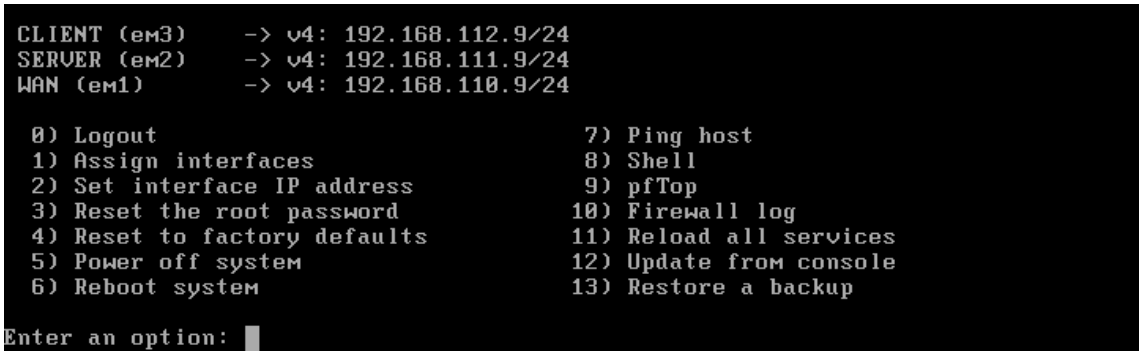

Bild 8 - IP-Adresszuweisung der OPNSense Firewall

Nach der IP-Zuweisung ist das Webinterface von OPNSense unter der Adresse

102.168.111.9 verfügbar und kann für die weitere Einrichtung verwendet werden. Beim ersten Login mittels der Root-Zugangsdaten wird der Setup Wizard gestartet, der durch die Basiseinrichtung von OPNSense führt. Hier werden als Grundkonfiguration der Hostname „opnsense-fw“, die Domain „recplast.lan“ sowie Deutsch als Systemsprache und das automatische VMWare Workstation Gateway als DNS-Server festgelegt, wie in Bild 9 ersichtlich. Die restlichen Einstellungen werden im Standard belassen.

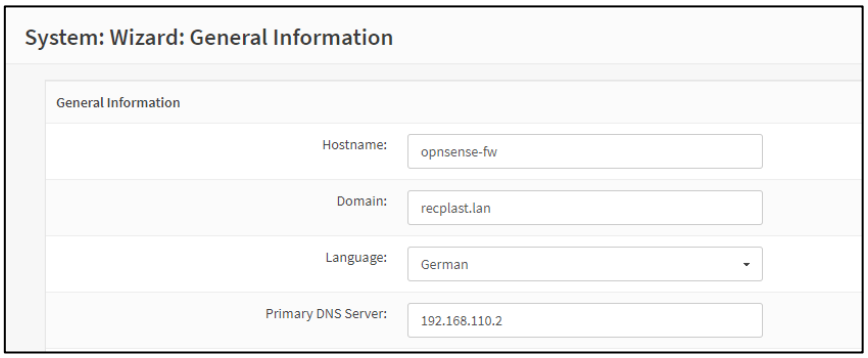

Bild 9 - Grundkonfiguration der OPNSense Firewall

Um die Zeitzone der Systeme anzugleichen, wird Europe/Berlin als Zeitzone für OPNSense festgelegt. Eine Synchronisierung der Systemzeiten erfolgt, indem die Firewall als Zeitquelle für die anderen Systeme im Anschluss an deren Installation festgelegt wird. Dies wird dadurch ermöglicht, dass OPNSense einen integrierten NTPd Server mitliefert [97]. Dieser wird, wie in Bild 10 ersichtlich, so konfiguriert, dass ausschließlich time.windows.com als Zeitquelle dient. Dies sorgt dafür, dass die Standardzeitquelle von Windows als Zeitquelle für alle Systeme verwendet wird.

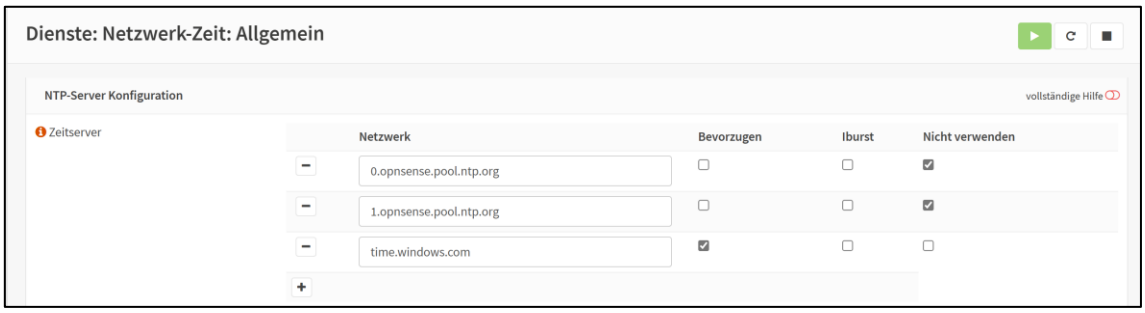

Bild 10 - NTP-Konfiguration in OPNSense

Die Blockierung von RFC1918-Netzwerken wird über die in Bild 11 ersichtliche Einstellung deaktiviert, sodass die internen Netzwerke nicht blockiert werden.

Bild 11 - Deaktivierung von RFC-1918-Netzwerk-Blockierung

Weitere Anpassungen der Standardkonfiguration werden vorerst nicht durchgeführt, die grundlegende Einrichtung von OPNSense ist abgeschlossen.

Installation von Ubuntu

Ubuntu Server 22.04.4 LTS steht auf Canonicals offizieller Webseite zum kostenlosen Download bereit [98]. Der Download der Ubuntu ISO wird auf dem Host mittels PowerShell verifiziert und ist fehlerfrei, wie in Bild 12 dargestellt.

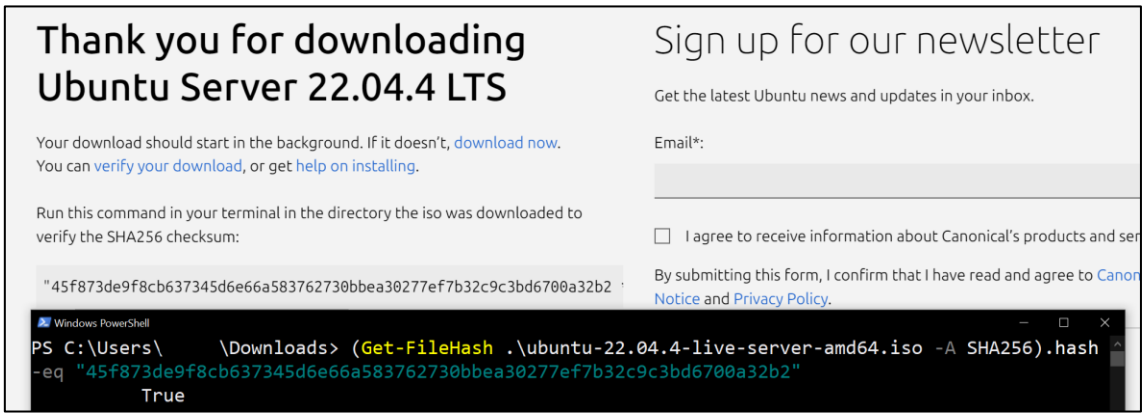

Bild 12 - Verifizierung des Ubuntu Server Downloads

Zu Zwecken dieses Prototyps wird auf allen Ubuntu-Systemen der Benutzer „recplast“ angelegt.

Als Basis für die Wazuh und Shuffle Server wird zunächst der Server für Wazuh installiert. Im Anschluss wird die virtuelle Maschine geklont und die Klone mit den

entsprechenden IP-Adressen und Docker-Installationen für Wazuh und Shuffle vorbereitet.

Die Installation des eigenständigen Ubuntu Servers erfolgt im Anschluss mit einer geringeren Hardwareausstattung, um Ressourcen auf dem Virtualisierungshost zu schonen.

Das Sizing der Server erfolgt anhand der Empfehlungen von Wazuh (4 vCPU, 8 GB RAM, 50 GB Storage, vgl. [93] und den Anforderungen der Shuffle-Komponenten (4vCPU, 8 GB RAM, 100 GB Storage, [76], wobei aufgrund der geringen Größe der Testumgebung die Ausstattung leicht nach unten korrigiert wird. Die Hardwareausstattung der Wazuh- und Shuffle-Server wird in Bild 13 abgebildet.

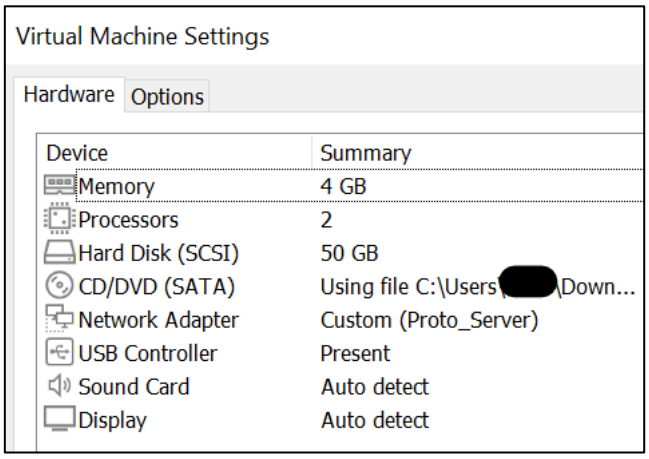

Bild 13 - Hardwareausstattung der Wazuh- und Shuffle-Server

Im Rahmen der Installation wird die Netzwerkkonfiguration für den Wazuh-Server wie in Tabelle 27 beschrieben vorgenommen.

Tabelle 27 - Netzwerkkonfiguration Wazuh Server

Hostname	wazuh
Subnetz	192.168.111.0/24
IP-Adresse	192.168.111.11

Gateway	192.168.111.9
Namensserver	192.168.111.9
Suchdomäne	recplast.lan

Mit diesen Einstellungen kann der Server für den Download der erforderlichen Softwarekomponenten über die OPNSense Firewall auf das Internet zugreifen.

Die virtuelle wird nun heruntergefahren und ein Klon für Shuffle erstellt. Auf diesem erfolgt die Netzwerkkonfiguration wie in Tabelle 28 beschrieben.

Tabelle 28 - Netzwerkkonfiguration Shuffle Server

Hostname	shuffle
Subnetz	192.168.111.0/24
IP-Adresse	192.168.111.12
Gateway	192.168.111.9
Namensserver	192.168.111.9
Suchdomäne	recplast.lan

Zusätzlich wird auf dem Shuffle Server als Vorbereitung für die folgende Installation von Shuffle Docker gemäß der offiziellen Installationsanleitung [99] installiert. Hierzu wird das apt-Repository von Docker entsprechend der Anleitung hinzugefügt und die Pakete docker-ce, docker-ce-cli, containerd.io, docker-buildx-plugin und docker-compose-plugi installiert. Die Installation wird mittels „sudo docker run hello-world“ getestet und ist, wie in Bild 14 gezeigt, funktionsfähig.

```
recplast@shuffle:~$ sudo docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

Bild 14 - Verifikation der Docker-Installation auf dem Shuffle Server

Zuletzt wird der Ubuntu Server installiert, der einen Applikationsserver der RECPLAST GmbH simulieren soll.

Dieser wird zur Schonung der Virtualisierungshost-Ressourcen mit geringerer Systemausstattung konfiguriert. Die Hardwareausstattung des Ubuntu Servers wird in Bild 15 dargestellt.

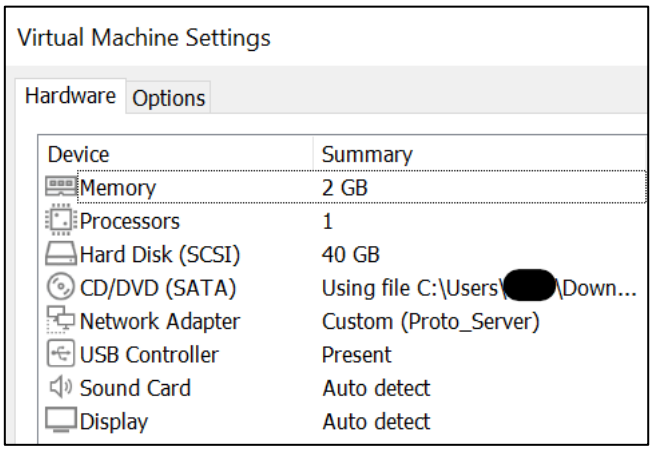

Bild 15 - Hardwareausstattung des Ubuntu Servers

Die Netzwerkkonfiguration des Ubuntu Servers erfolgt wie in Tabelle 29 beschrieben.

Tabelle 29 - Netzwerkkonfiguration Ubuntu Server

Hostname	ubuntu
Subnetz	192.168.111.0/24
IP-Adresse	192.168.111.10
Gateway	192.168.111.9
Namensserver	192.168.111.9
Suchdomäne	recplast.lan

Auf allen Ubuntu-Systemen wird die IP-Adresse 192.168.111.9 als Zeitquelle festgelegt, wodurch OPNSense alle NTP-Anfragen wie konfiguriert an time.windows.com weiterleitet.

Die Ubuntu Systeme sind damit vollständig installiert und für die Installation der FOSS Tools bereit.

Installation von Windows

Zur Installation des Windows 10 Clients wird das Media Creation Tool von Microsoft heruntergeladen [100]. Mit dem Media Creation Tool wird eine ISO-Datei für Windows 10 mit x64-Architektur erstellt.

Der Windows 10 Client wird zur Schonung der Virtualisierungshost-Ressourcen mit geringerer Systemausstattung konfiguriert. Als Client wird das Windows-System mit dem Client-Netzwerk verbunden. Die Hardwareausstattung des Windows Clients wird in Bild 15 dargestellt.

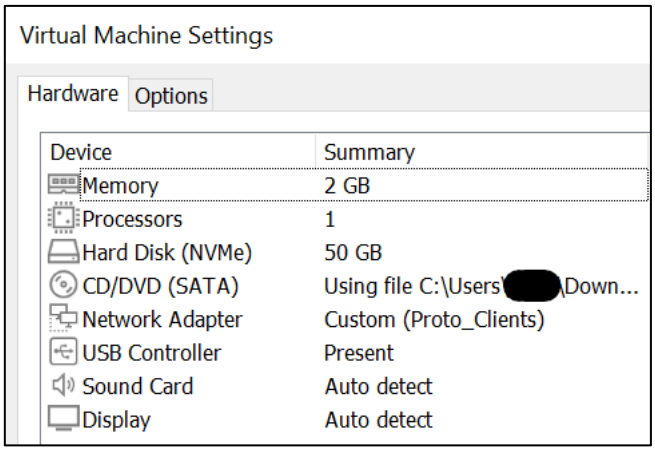

Bild 16 - Hardwareausstattung des Windows Clients

Als Windows-Edition wird Windows 10 Pro gewählt.

Auf dem Windows Client wird der Benutzer „recplast“ angelegt.

Die Netzwerkkonfiguration des Windows Clients erfolgt wie in Tabelle 29 beschrieben.

Tabelle 30 - Netzwerkkonfiguration Windows Client

Subnetz	192.168.112.0/24
IP-Adresse	192.168.112.10
Gateway	192.168.112.9
Namensserver	192.168.112.9
Suchdomäne	recplast.lan

Wie in Bild 17 zu sehen ist, ist time.windows.com die standardmäßig in Windows synchronisierte Zeitquelle. Somit sind alle Systeme der Testumgebung mit derselben Zeitquelle synchronisiert.

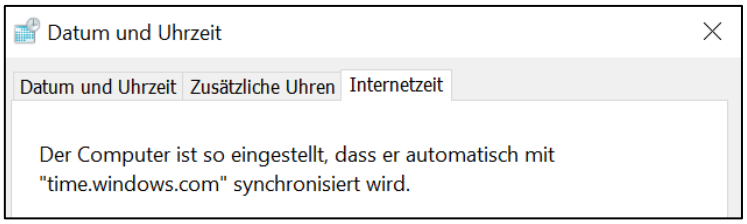

Bild 17 - Standard-Zeitsynchronisierung auf Windows 10

Mit dieser Konfiguration ist die Grundinstallation des Windows 10 Clients abgeschlossen und es kann mit der Installation der FOSS Tools fortgefahren werden.

5.3.2 Einrichtung der FOSS Tools

In diesem Kapitel wird die Einrichtung der FOSS-Tools beschrieben.

Aus Gründen der vereinfachten Integration der Tools miteinander wird zunächst Wazuh installiert, anschließend Suricata installiert und dessen Protokolldaten an Wazuh übertragen und zuletzt Shuffle installiert und mit Wazuh integriert.

Installation von Wazuh

Die Installation von Wazuh erfolgt anhand der offiziellen Quickstart-Installationsanleitung [93]. Hierzu wird der Wazuh Installation Assistant mittels des Befehls „curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh && sudo bash ./wazuh-install.sh -a“ [93] auf dem Wazuh Server ausgeführt.

Wie in Bild 18 und Bild 19 zu sehen ist, installiert der Installation Assistant Wazuh in der Version 4.8.0, genauer die Komponenten Wazuh Indexer, Wazuh Server und Wazuh Dashboard, auf dem System. Wazuh empfiehlt für produktive Installationen eine Installation des Wazuh Servers und der Wazuh Indexer auf getrennten Systemen [48], für die funktionale Bewertung von Wazuh anhand der OH-SzA in diesem Prototyp ist eine gemeinsame Installation jedoch ausreichend, da keine Skalierung über mehrere Wazuh Indexer oder Hochverfügbarkeit benötigt wird.

```
recplast@wazuh:~$ curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh && sudo bash ./wazuh-inst
all.sh -a
[sudo] password for recplast:
12/07/2024 14:40:08 INFO: Starting Wazuh installation assistant. Wazuh version: 4.8.0
12/07/2024 14:40:08 INFO: Verbose logging redirected to /var/log/wazuh-install.log
12/07/2024 14:40:11 INFO: Verifying that your system meets the recommended minimum hardware requirem
ents.
12/07/2024 14:40:18 INFO: Wazuh web interface port will be 443.
12/07/2024 14:40:27 INFO: --- Dependencies ----
12/07/2024 14:40:27 INFO: Installing apt-transport-https.
12/07/2024 14:40:34 INFO: Wazuh repository added.
12/07/2024 14:40:34 INFO: --- Configuration files ---
12/07/2024 14:40:34 INFO: Generating configuration files.
12/07/2024 14:40:34 INFO: Generating the root certificate.
12/07/2024 14:40:35 INFO: Generating Admin certificates.
12/07/2024 14:40:35 INFO: Generating Wazuh indexer certificates.
12/07/2024 14:40:35 INFO: Generating Filebeat certificates.
12/07/2024 14:40:35 INFO: Generating Wazuh dashboard certificates.
12/07/2024 14:40:35 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certif
icates, and passwords necessary for installation.
12/07/2024 14:40:36 INFO: --- Wazuh indexer ---
12/07/2024 14:40:36 INFO: Starting Wazuh indexer installation.
12/07/2024 14:42:19 INFO: Wazuh indexer installation finished.
12/07/2024 14:42:19 INFO: Wazuh indexer post-install configuration finished.
12/07/2024 14:42:19 INFO: Starting service wazuh-indexer.
12/07/2024 14:42:35 INFO: wazuh-indexer service started.
12/07/2024 14:42:35 INFO: Initializing Wazuh indexer cluster security settings.
12/07/2024 14:42:46 INFO: Wazuh indexer cluster security configuration initialized.
12/07/2024 14:42:46 INFO: Wazuh indexer cluster initialized.
```

Bild 18 - Wazuh Installation Assistant (Teil 1)

```
12/07/2024 14:42:46 INFO: --- Wazuh server ---
12/07/2024 14:42:46 INFO: Starting the Wazuh manager installation.
12/07/2024 14:43:59 INFO: Wazuh manager installation finished.
12/07/2024 14:43:59 INFO: Wazuh manager vulnerability detection configuration finished.
12/07/2024 14:43:59 INFO: Starting service wazuh-manager.
12/07/2024 14:44:15 INFO: wazuh-manager service started.
12/07/2024 14:44:15 INFO: Starting Filebeat installation.
12/07/2024 14:44:48 INFO: Filebeat installation finished.
12/07/2024 14:44:56 INFO: Filebeat post-install configuration finished.
12/07/2024 14:44:56 INFO: Starting service filebeat.
12/07/2024 14:45:00 INFO: filebeat service started.
12/07/2024 14:45:00 INFO: --- Wazuh dashboard ---
12/07/2024 14:45:00 INFO: Starting Wazuh dashboard installation.
12/07/2024 14:48:01 INFO: Wazuh dashboard installation finished.
12/07/2024 14:48:01 INFO: Wazuh dashboard post-install configuration finished.
12/07/2024 14:48:01 INFO: Starting service wazuh-dashboard.
12/07/2024 14:48:03 INFO: wazuh-dashboard service started.
12/07/2024 14:48:04 INFO: Updating the internal users.
12/07/2024 14:48:11 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/in
ternalusers-backup folder.
12/07/2024 14:48:29 INFO: There was an error accessing the API. Retrying...
12/07/2024 14:49:22 INFO: Initializing Wazuh dashboard web application.
12/07/2024 14:49:23 INFO: Wazuh dashboard web application initialized.
12/07/2024 14:49:23 INFO: --- Summary ---
12/07/2024 14:49:23 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 1E9pBcEGqDQoxoc?fCNzdE2U5MPTgTCY
12/07/2024 14:49:23 INFO: Installation finished.
recplast@wazuh:~$
```

Bild 19- Wazuh Installation Assistant (Teil 2)

Nach Abschluss der Installation zeigt der Wazuh Installation Assistant wie in Bild 19 die Zugangsdaten und die URL für den Zugriff auf das Wazuh Dashboard an. Der Standardnutzer ist dabei „admin“ mit einem zufällig erzeugten Passwort.

Das Wazuh Dashboard ist nun wie von einem IT-Mitarbeiter der RECPLAST GmbH über den Windows 10 Client erreichbar und zeigt bei Aufruf der Adresse „https://192.168.111.11:443“ die in Bild 20 dargestellte Anmeldemaske.

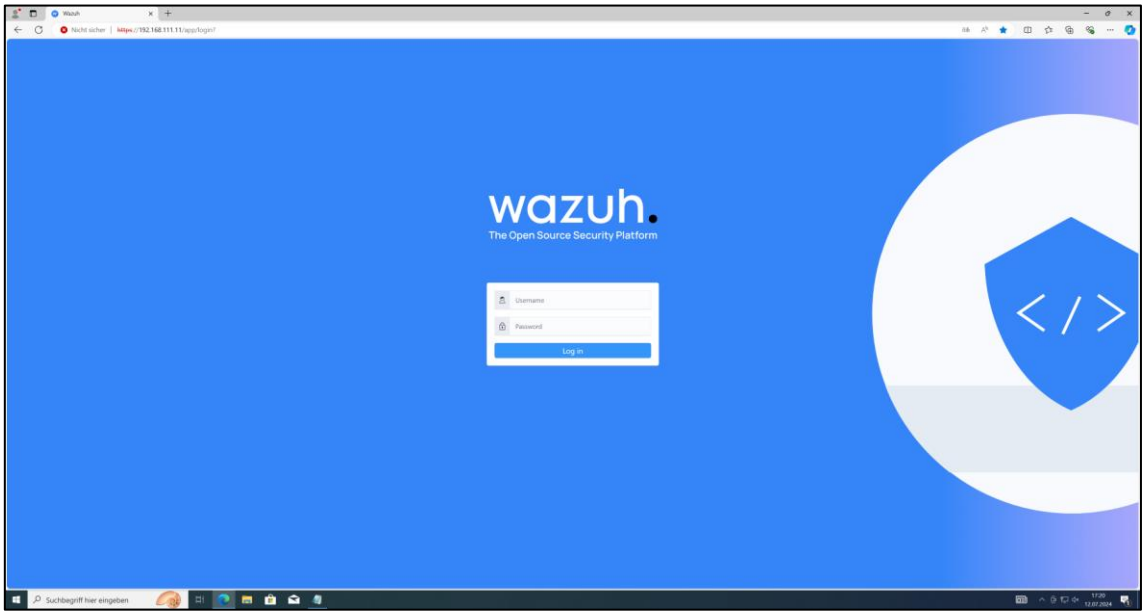

Bild 20 - Anmeldemaske von Wazuh

Das nach Anmeldung erscheinende Wazuh Dashboard bietet einen Überblick über die Funktionalitäten von Wazuh und merkt an, dass keine Agenten dem Manager zugeordnet sind (siehe Bild 21).

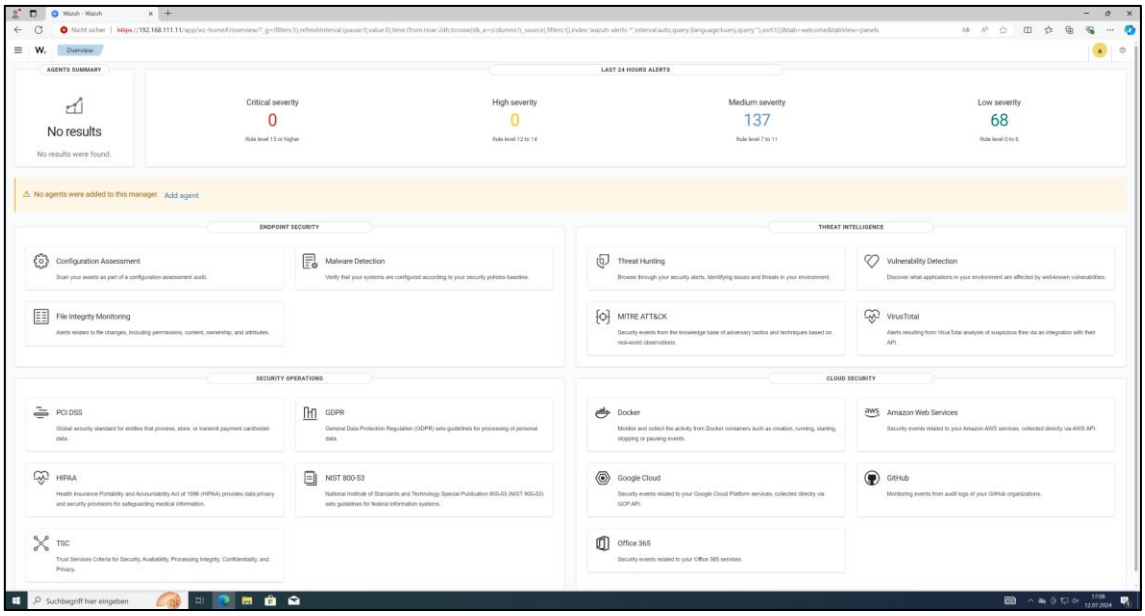

Bild 21 - Initiales Wazuh Dashboard

Die Installation eines Agenten soll auf allen Windows- und Linux-Systemen der Umgebung erfolgen.

Begonnen wird mit der Installation auf dem Windows-Client, wozu auf den Link „Add agent“ in der in Bild 21 sichtbaren Warnmeldung geklickt wird.

Die sich darauffolgend öffnende Maske „Deploy new agent“ bietet Auswahlmöglichkeiten für die Zielplattform, in diesem Fall Windows, die Serveradresse, also die IP-Adresse des Wazuh Servers sowie optional einen Namen und eine Gruppenzuweisung für den Agenten (siehe Bild 22).

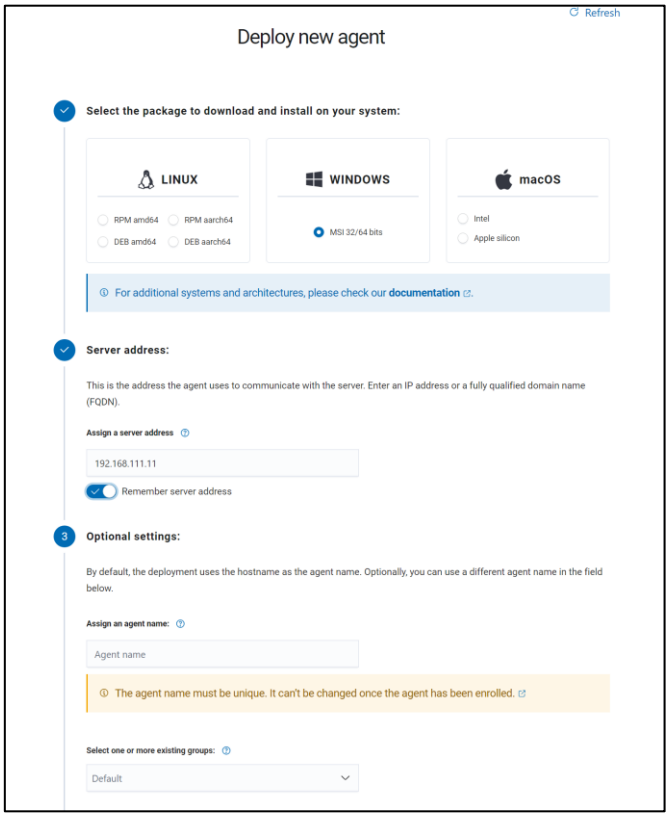

Bild 22 - Deployment-Maske für Wazuh Agenten (Konfiguration)

Aus der Konfiguration wird automatisch ein Powershell-Befehl generiert, der kopiert und zur Installation auf dem Windows Client ausgeführt werden kann (siehe Bild 23). Der generierte Befehl für den Windows Client lautet:

„Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-

agent-4.8.0-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.111.11'“

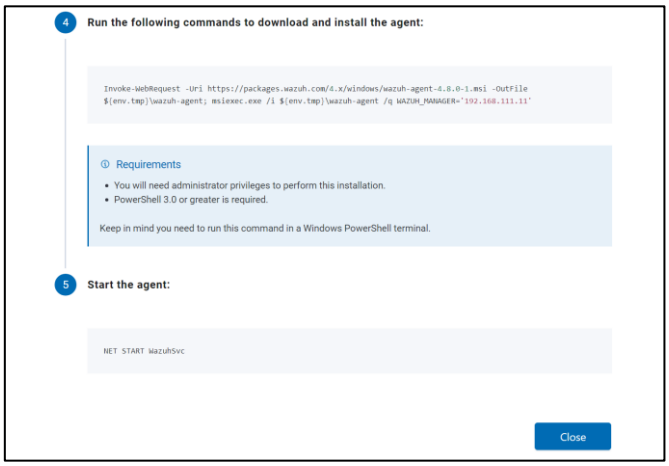

Bild 23 - Deployment-Maske für Wazuh Agenten (Installationsbefehl)

Der Befehl wird auf dem Windows Client in einem mit Administratorrechten gestarteten Powershell-Fenster ausgeführt. Anschließend wird der Agent mit dem Befehl „NET START WazuhSvc“ wie in Bild 23 vorgegeben gestartet. Der Start des Wazuh Agenten wird in Powershell wie in Bild 24 bestätigt.

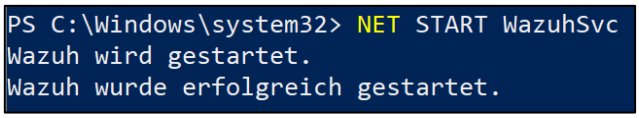

Bild 24 - Bestätigung über Start des Windows Wazuh Agenten

Ein Klick auf „Close“ im Wazuh Dashboard führt auf die „Endpoints“-Seite, wo der installierte Agent sofort sichtbar ist und als Namen den automatisch generierten Windows-Hostnamen erhalten hat (siehe Bild 25).

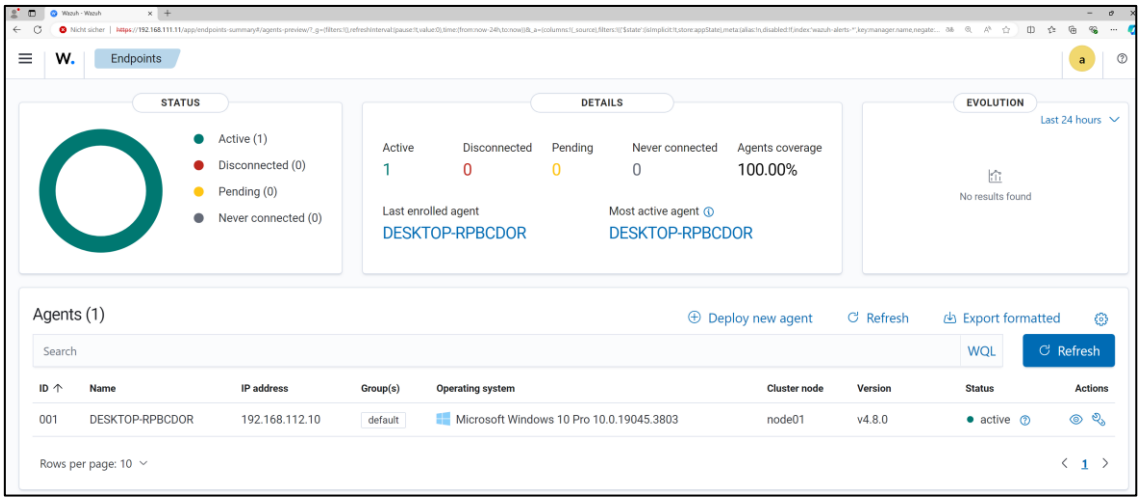

Bild 25 - Erster Wazuh Agent

Analog zum Windows Agenten werden die Linux-Agenten über die „Deploy new agent“ Maske nach einem Klick auf „Deploy new agent“ auf der Endpoints-Übersicht angelegt. Für die Ubuntu-Systeme wird als Plattform „DEB amd64“ gewählt.

Der generierte Befehl zur Installation des Wazuh Agenten auf den Ubuntu-Systemen ist:

„wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.111.11' dpkg -i ./wazuh-agent_4.8.0-1_amd64.deb“

Zum Start der Agenten werden anschließend die folgenden Befehle ausgeführt:

„sudo systemctl daemon-reload

sudo systemctl enable wazuh-agent

sudo systemctl start wazuh-agent“

Nach Ausführung dieser Befehle auf dem Ubuntu-Server und dem Shuffle-Server erscheinen die Agenten auf dem Endpoint Dashboard, wobei der Shuffle-Agent als der zuletzt hinzugefügte hervorgehoben wird (siehe Bild 26).

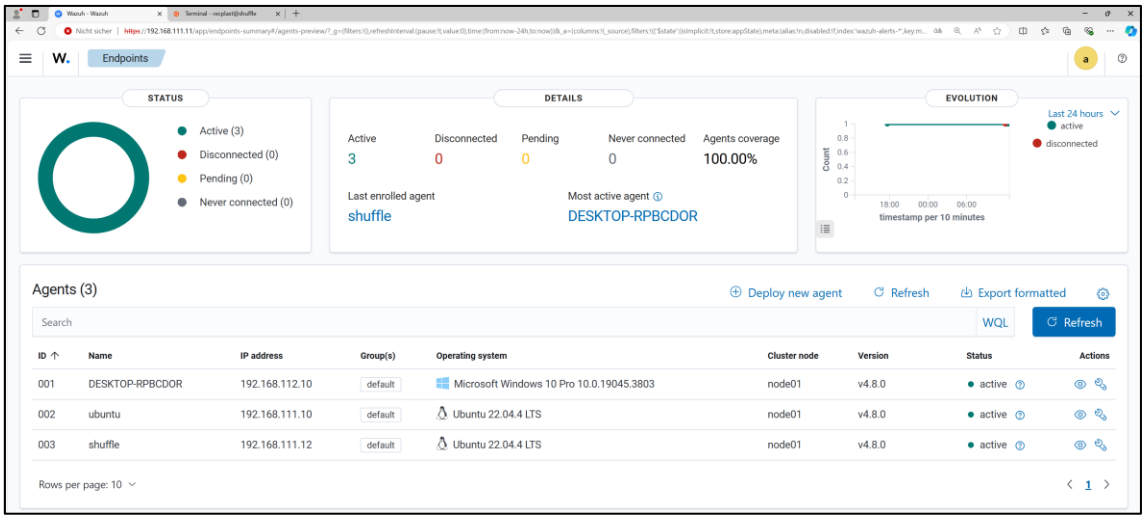

Bild 26 - Gesamtübersicht aller Wazuh Agenten

Zur Aktivierung des Empfangs von Syslog-Nachrichten wird im Menüpunkt „Server Management“ unter „Settings“ die Konfiguration des Wazuh Servers angepasst. Über „Edit Configuration“ kann die Konfiguration im XML-Format direkt bearbeitet werden. Entsprechend der Anleitung von Wazuh [101] wird der Konfiguration der in Bild 27 gezeigte, auf die Prototyp-Umgebung angepasste Eintrag für die Syslog-Verbindung hinzugefügt. Anschließend wird über die Schaltflächen „Save“ und „Restart Manager“ die Konfiguration übernommen.

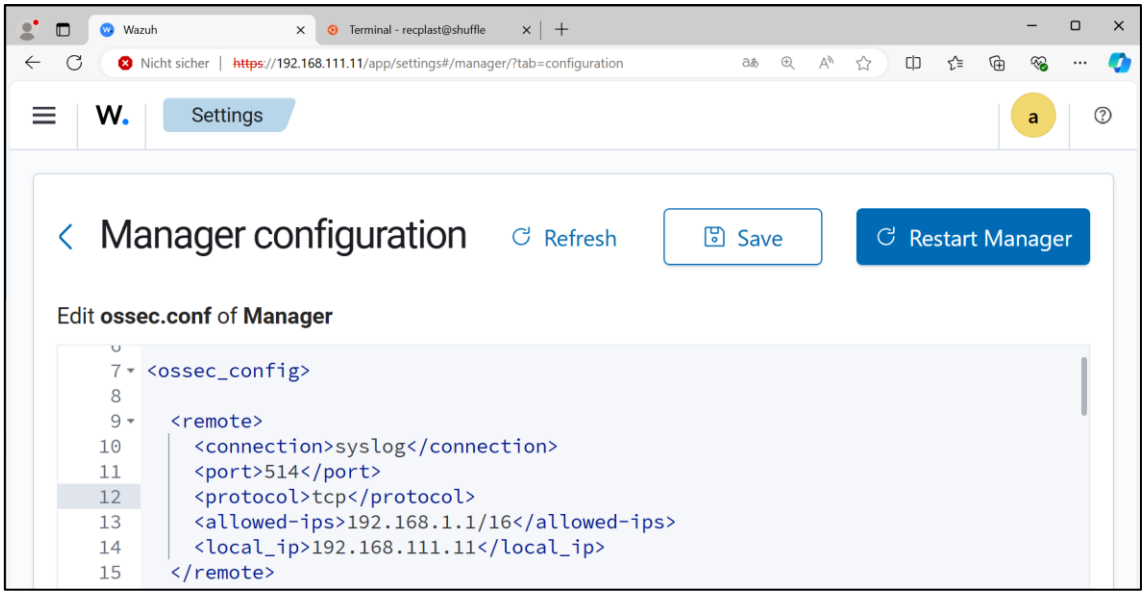

Bild 27 - Syslog-Konfiguration des Wazuh Servers

Darüber hinaus wird der Eintrag „logall_json“ unter „global“ auf „yes“ gesetzt, um alle Protokolldaten zu speichern, unabhängig davon, ob sie einen Alert auslösen [102]. Um die Events im Wazuh Dashboard einsehen zu können, wird in der Filebeat-Konfiguration auf dem Wazuh-Server die Einstellung „archives: enabled“ auf „true“ gesetzt [102]. Als letzter Schritt wird in den Einstellungen unter „Dashboard Management“ im Menüpunkt „App settings“ die Einstellung „Index pattern“ auf „wazuh-*“ gesetzt (siehe Bild 28). Die Dokumentation für Wazuh Version 4.8 sieht dies über den Menüpunkt „Stack management“ vor [102], der allerdings in Wazuh 4.8 nicht existiert.

Bild 28 - Index pattern in Wazuh

Der Wazuh-Server empfängt nun Protokolldaten über die Wazuh Agenten und ist für den Empfang weiterer Protokolldaten über Syslog bereit.

Installation von Suricata

Für die Installation von Suricata wird die in OPNSense integrierte IDS-Funktionalität verwendet. Zur Aktivierung derer wird unter dem Menüpunkt „Dienste“ der Dienst „Einbruchserkennung“ unter „Verwaltung“ aktiviert und auf alle Schnittstellen der Firewall angewendet, wie in Bild 29 zu sehen ist. Dabei wird der IPS-Modus aktiviert, um die Downloads nicht nur alarmieren, sondern auch verhindern zu können. Für eine zusätzliche Protokollierung werden Systemprotokoll-Alarme aktiviert. Die weiteren Einstellungen werden auf dem Standard belassen.

Bild 29 - Aktivierung von Suricata auf OPNSense

Im Reiter „Herunterladen“ wird das Regelwerk „OPNsense-App-detect/test“ aktiviert und heruntergeladen (siehe Bild 30), um die Funktionalität von Suricata zu testen.

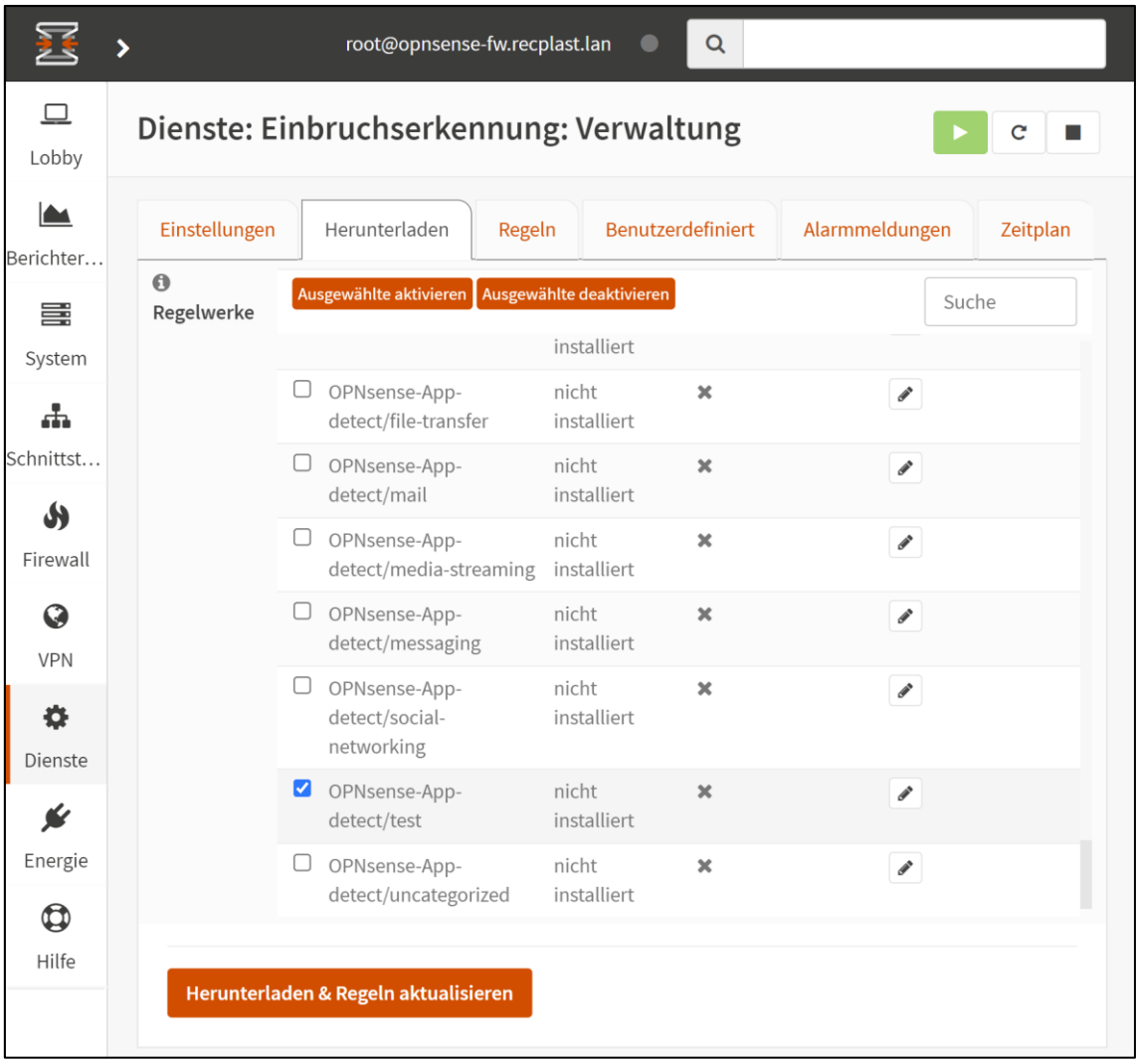

Bild 30 - Aktivierung des Testregelwerks für Suricata

Das Regelwerk ist auf Github verfügbar, worauf aus OPNSense verlinkt wird. Es beinhaltet nur eine Regel, die auf einen Zugriff auf die URL „www.eicar.org/anti_virus_test_file.htm“ mit einem entsprechenden Inhalt prüft [103]. Das EICAR Test File wurde vom European Institute for Computer Antivirus Research und der Computer Antivirus Research Organization zum Testen von Antivirus-Lösungen entwickelt, ohne tatsächliche Schadsoftware verwenden zu müssen [104].

Die aktivierte Regel ist nun im Reiter „Regeln“ sichtbar (siehe Bild 31).

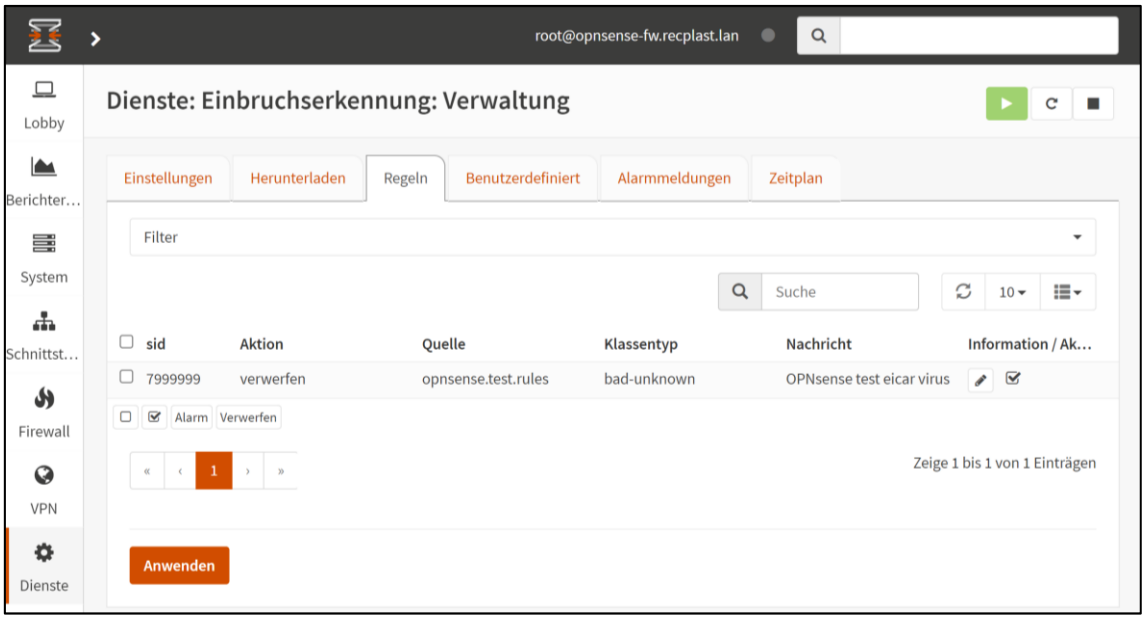

Bild 31 - Aktive Testregel für Suricata

Unter den Menüpunkten „System“, „Einstellungen“, „Protokollierung“ wird nun im Reiter „Remote“ die Weiterleitung der Suricata-Protokolldaten an Wazuh konfiguriert. Hierzu wird ein neuer Eintrag hinzugefügt, in dem die Applikation „suricata“ als Datenquelle und die IP-Adresse von Wazuh als Empfänger gewählt werden. Das Transportprotokoll wird entsprechend der in Wazuh getroffenen Einstellungen auf TCP geändert, die restlichen Einstellungen werden im Standard belassen. Die vollständige Konfiguration ist in Bild 32 zu sehen.

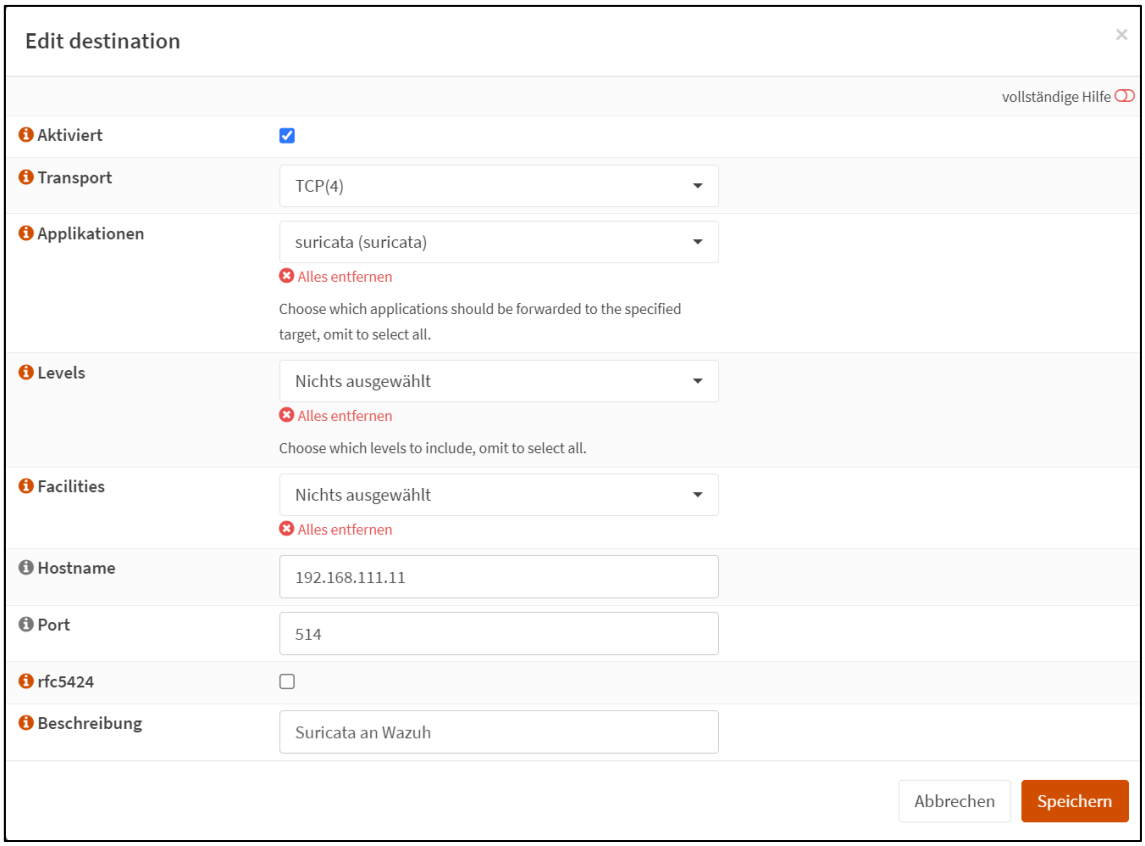

Bild 32 - Weiterleitung der Suricata-Protokolldaten an Wazuh

Die Überwachung des Datenverkehrs mittels der Testregel in Suricata und die Weiterleitung der Ereignisse an Wazuh sind somit eingerichtet.

Installation von Shuffle

Die Installation von Shuffle auf dem Shuffle-Server erfolgt entsprechend der Anleitung auf Github [94]. Nach genauer Befolgung der dort gelisteten Installationsschritte kann die Weboberfläche von Shuffle vom Windows-Client aus über die URL „http://192.168.111.12:3001/“ aufgerufen werden und fordert zur Anlage eines Administrator-Accounts auf (siehe Bild 33).

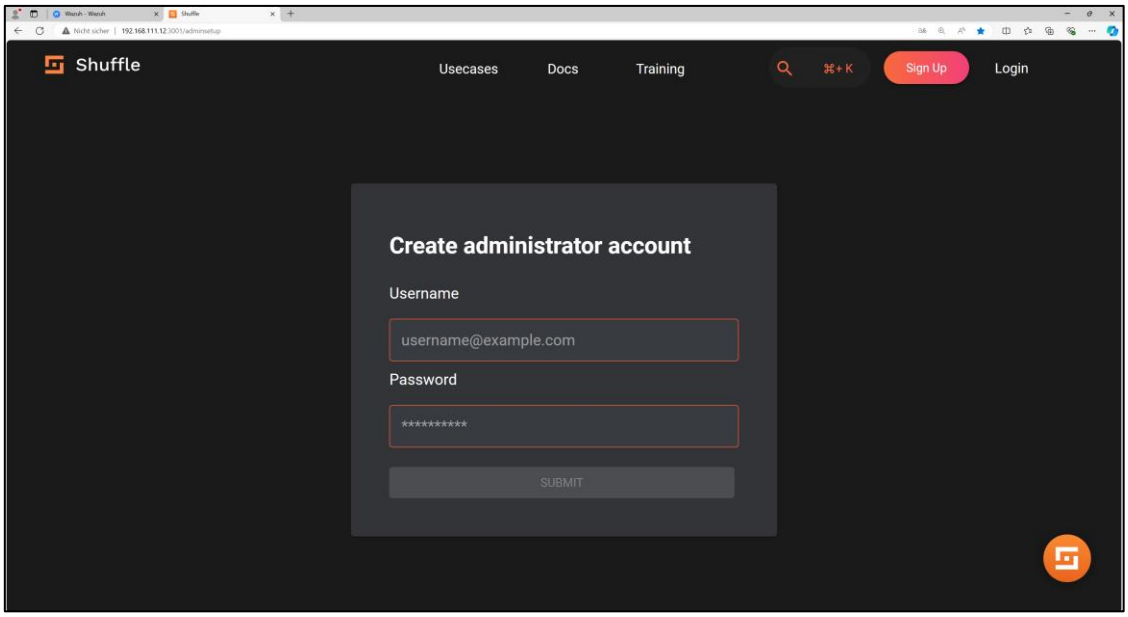

Bild 33 - Erster Aufruf von Shuffle

Nach dem ersten Login öffnet sich ein Einrichtungsassistent, der neuen Nutzern eine einfachere Einrichtung ermöglicht (siehe Bild 34).

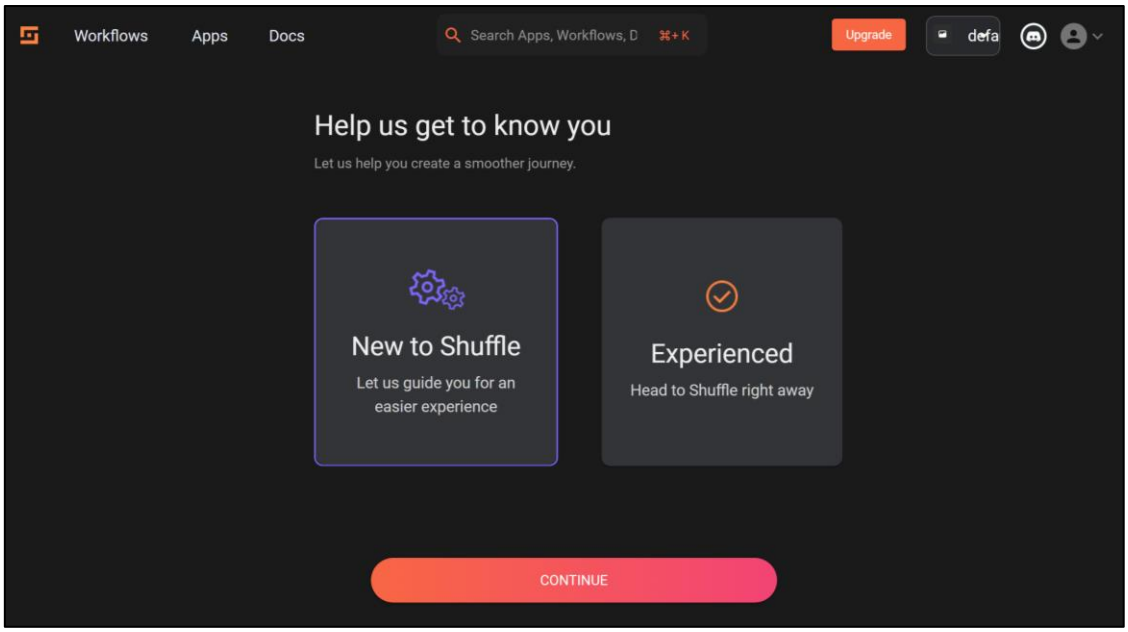

Bild 34 - Shuffle Einrichtungsassistent

Nach einem Klick auf „New to Shuffle“ bietet Shuffle eine Auswahlmöglichkeit für Integrationen typischer Komponenten einer SzA-Systemumgebung an, darunter SIEM (hier wird Wazuh gewählt), Threat Intelligence, EDR, Email und Case-

Management (siehe Bild 35).

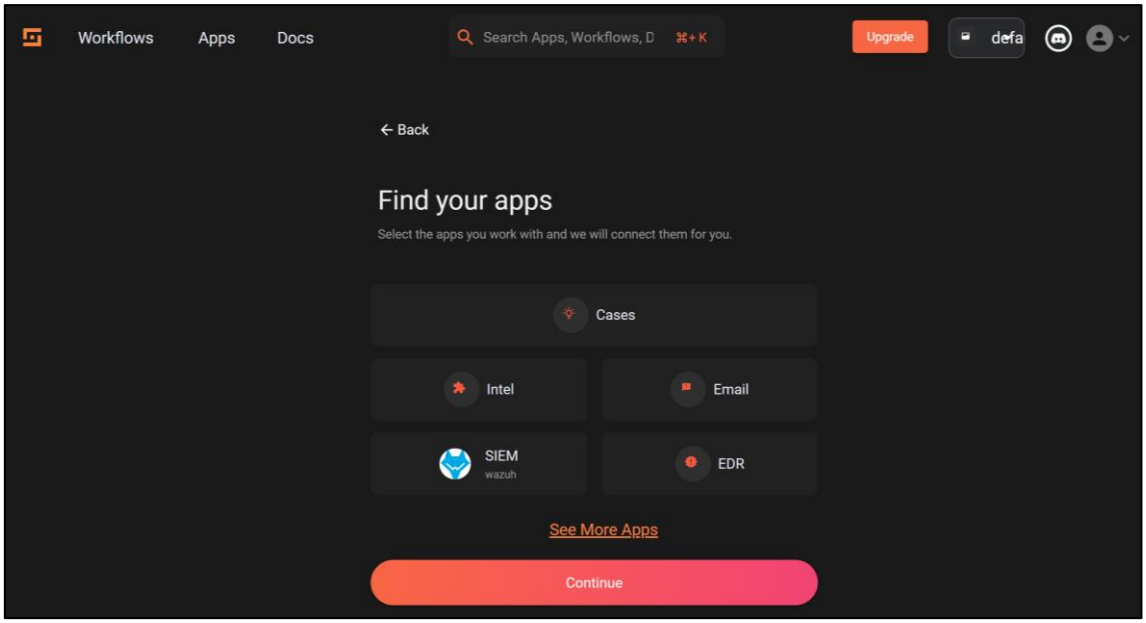

Bild 35 - Shuffle App Auswahlassistent

Im folgenden Schritt schlägt der Einrichtungsassistent auf Basis der ausgewählten Apps passende Workflows vor (siehe Bild 36). Zu Testzwecken wird im Anschluss an die Basiseinrichtung ein eigener Test-Workflow definiert, daher wird mittels „Continue to workflows“ die Einrichtung fertiger Workflows übersprungen.

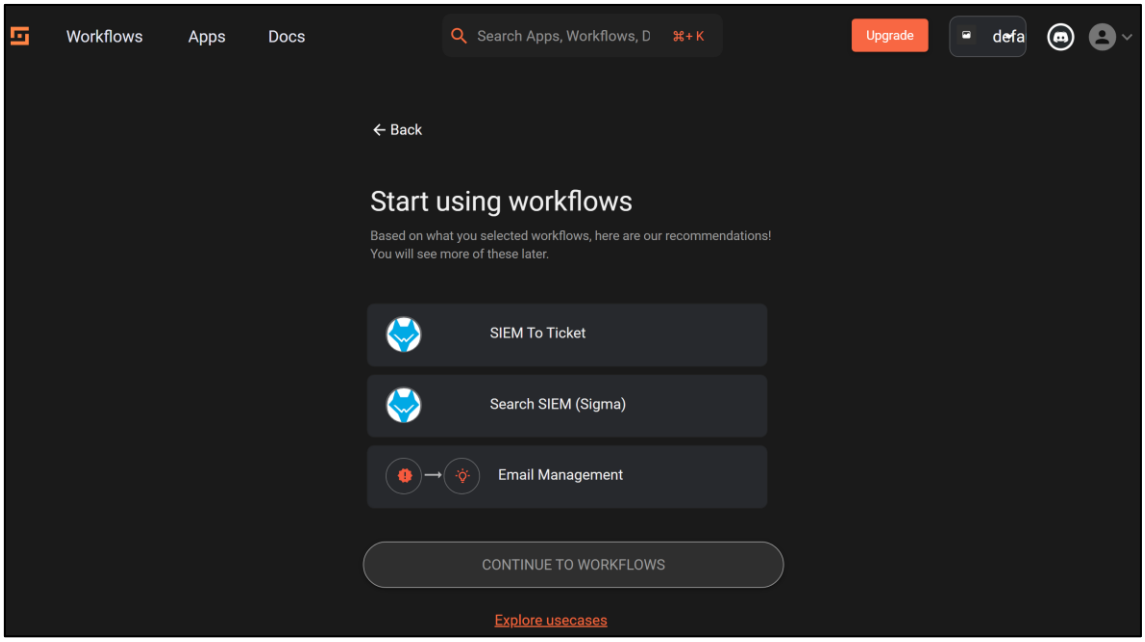

Bild 36 - Vorgeschlagene Shuffle Workflows

Nach der Einrichtung des Workflows leitet Shuffle auf die Übersichtsseite der Workflows weiter, die in Bild 37 zu sehen ist.

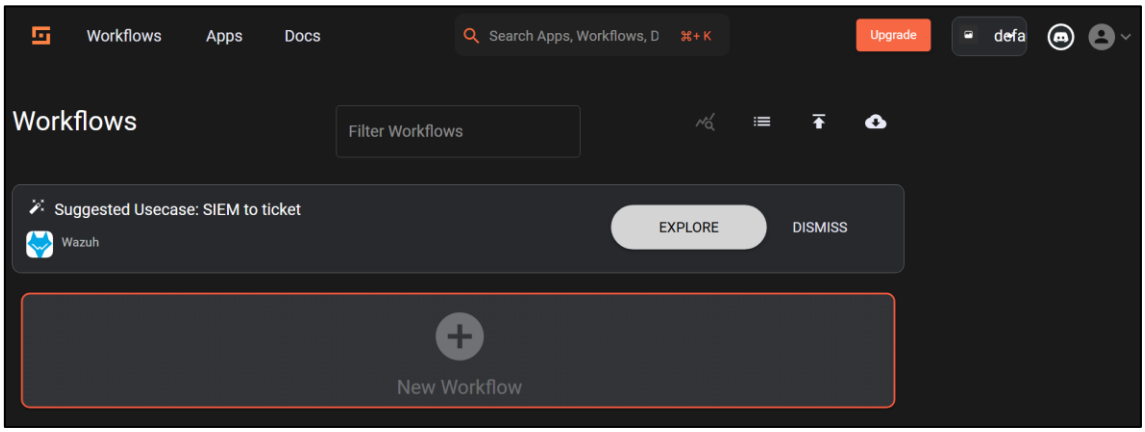

Bild 37 - Workflows-Übersicht in Shuffle

Entsprechend der Anleitung von Wazuh wird nun einem neuen Workflow ein Webhook mit der App Wazuh als Trigger angelegt, um Alerts von Wazuh empfangen zu können [105]. Der Webhook wird zu „Wazuh trigger“ umbenannt und gestartet. Damit wird eine Shuffle Tools Node mit der Aktion „Repeat back to me“ verbunden, die als Parameter die Variable „$exec“, also den durch den Webhook übertragenen Eingangsparameter des Workflows, erhält. Der Test Workflow sieht wie in Bild 38 gezeigt aus.

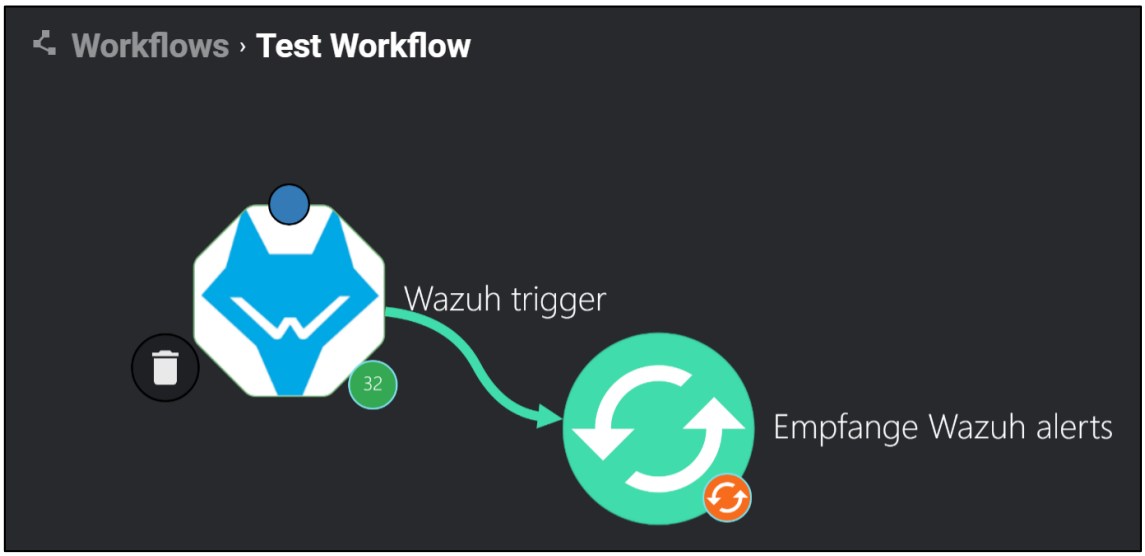

Bild 38 - Shuffle Test Workflow mit Wazuh

Für die Integration auf Seiten Wazuhs wird erneut die Manager-Konfiguration um den in der Integrationsanleitung beschriebenen „integration“-Anteil erweitert, wobei die Hook-URL entsprechend durch die in Shuffle angezeigte URL des Wazuh Webhooks ersetzt wird (siehe Bild 39).

Bild 39 - Konfiguration der Shuffle-Integration in Wazuh

Somit sollte der Workflow nun die empfangenen Wazuh Alerts wiedergeben. Tatsächlich erscheinen in den Workflow-Ausführungen nun Einträge, von denen einer zum erfolgreichen Login auf dem Windows Client in Bild 40 dargestellt wird.

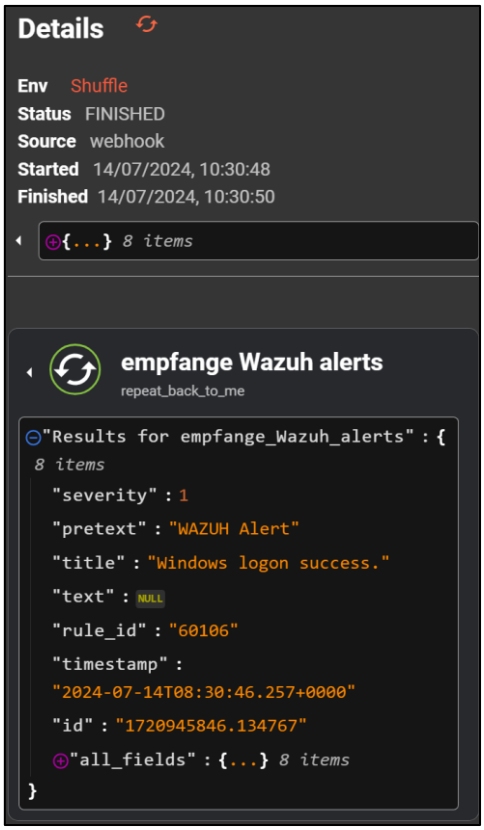

Bild 40 - Shuffle Workflow Ausführung für Windows Login

Die grundlegende Einrichtung von Shuffle ist nun abgeschlossen.

Erstellung eines exemplarischen Workflows

Mit den grundlegend eingerichteten FOSS Tools wird nun ein exemplarischer Workflow abgebildet und dessen Funktionsfähigkeit validiert. Als Anwendungsfall soll eine Alarmierung von Suricata auf einen aus dem Client-Netz erkannten Download der EICAR-Testdatei an Wazuh weitergeleitet werden, dort ein Alert generiert und an Shuffle weitergeleitet werden, wo eine Active Response ausgelöst wird, die auf der OPNsense Firewall eine Isolierung des Client-Netzes vornimmt (siehe Bild 41).

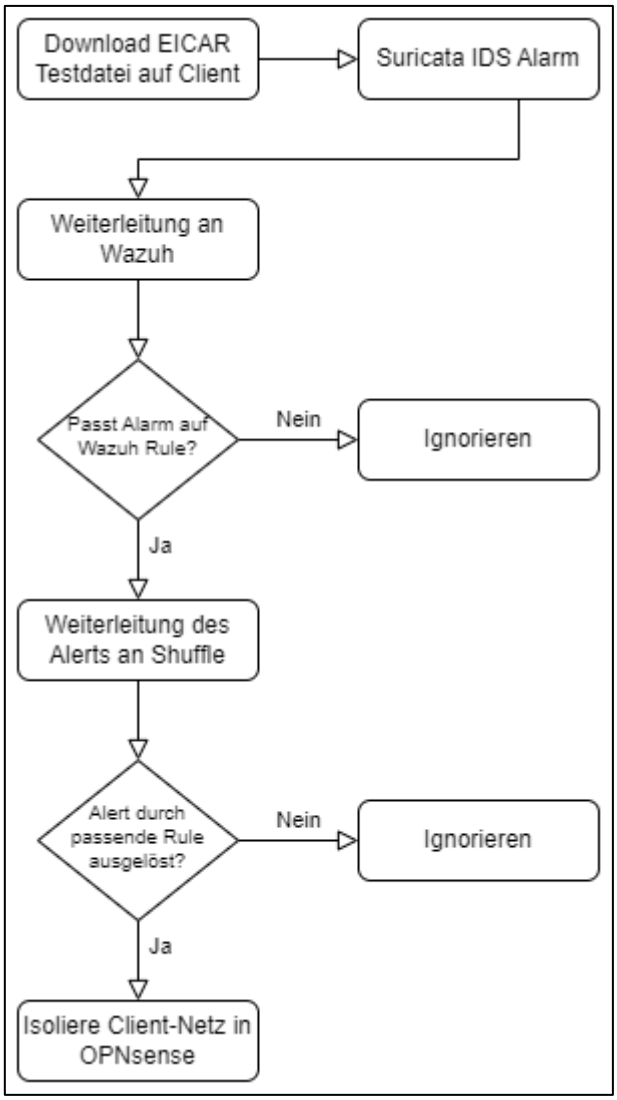

Bild 41 - Ablaufdiagramm des exemplarischen Workflows

Um Format und Inhalt der gesuchten Suricata-Ereignisse zu bestimmen, wird zunächst auf dem Windows Client mittels Powershell der Befehl „Invoke-WebRequest -Uri ‚http://pkg.opnsense.org/test/eicar.com.txt‘ -OutFile notavirus.txt“ ausgeführt, um die bei OPNSense gehostete EICAR-Testdatei herunterzuladen. Hierbei ist die Verwendung von HTTP anstelle von HTTPS sehr wichtig, da Suricata andernfalls den verschlüsselten Datenverkehr nicht untersuchen kann. Wie in Bild 42 zu sehen ist, gelingt der Download in Powershell nicht und in der Protokolldatei von OPNSense erscheint ein Eintrag über das Verwerfen der Pakete.

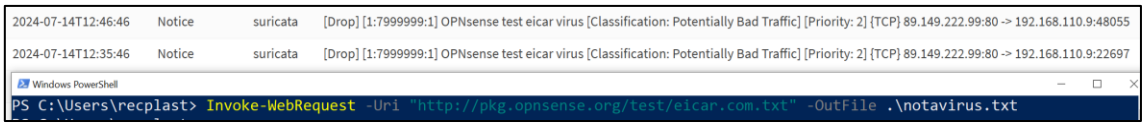

Bild 42 - Blockierter EICAR-Dateidownload durch Suricata

Die protokollierten Ereignisse sind im Wazuh Archive Index sichtbar (siehe Bild 43).

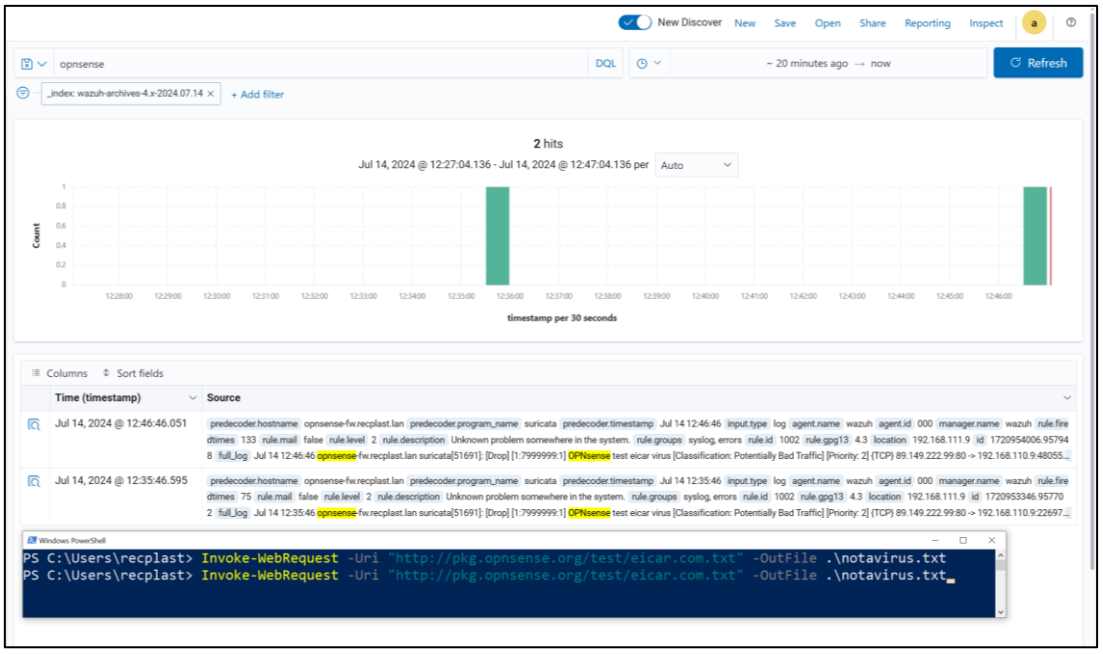

Bild 43 - Suricata Alerts in Wazuh Archive

In den Protokollen fällt auf, dass die IP-Adresse des DMZ-Interfaces der Firewall als Ziel-IP des Downloads angezeigt wird. Um den Download dem tatsächlichen Ziel, dem Windows-Client, zuordnen zu können, wird in der Suricata-Konfiguration die DMZ-Schnittstelle entfernt. Somit wird in folgenden Ereignissen die IP-Adresse des tatsächlich für den Download verantwortlichen Systems angezeigt.

Zur Erstellung einer auf diese Ereignisse maßgeschneiderten Wazuh Rule wird nun das Feld „full_log“ eines dieser Ereignisse kopiert und im Menü unter „Ruleset Test“ genauer getestet. Die Ereignisse werden durch das Pre-Encoding verarbeitet, anschließend wird jedoch kein passender Decoder gefunden (siehe Bild 44).

Bild 44 - Ruleset Test für Suricata Protokolle

Um die Ereignisse zu dekodieren, wird im Menü unter „Server management“ im Menüpunkt „Decoders“ auf „Custom decoders“ gefiltert (Bild 45). Hier wird mittels der Schaltfläche „Add new decoders file“ eine neue Decoder-Datei namens „suricata-custom“ angelegt.

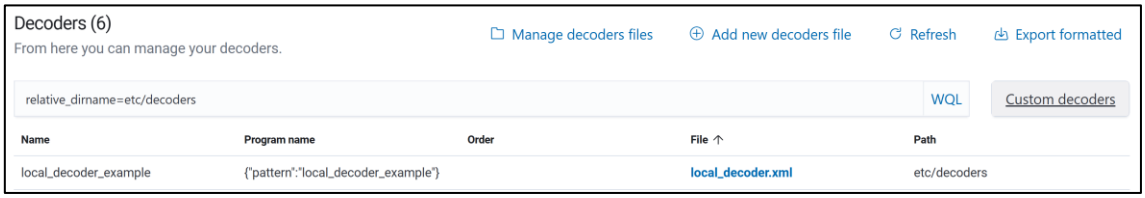

Bild 45 - Custom Decoders in Wazuh

Die neu angelegte Decoder-Datei wird mit auf das Ereignis passenden Decodern nach Vorbild eines Wazuh-Blogposts [106] erstellt. Die definierten Decoder sind in 0 angehängt.

Analog zur neu angelegten Decoder-Datei wird im Menüpunkt „Rules“ auf „Custom rules“ gefiltert und eine neue Rules-Datei namens „suricata-alerts.xml“ angelegt. Die neu angelegte Rules-Datei wird mit einer Rule nach Vorbild eines Wazuh-Blogposts [106] erstellt, die auf alle Ereignisse alarmiert, die durch den zuvor definierten Decoder verarbeitet wurden. Die definierte Rule ist in Anlage 15 angehängt.

Mit dieser Rule sind nun die von Suricata erkannten Ereignisse nach erneutem

Auslösen des Downloads in Wazuh wie in Bild 46 sichtbar.

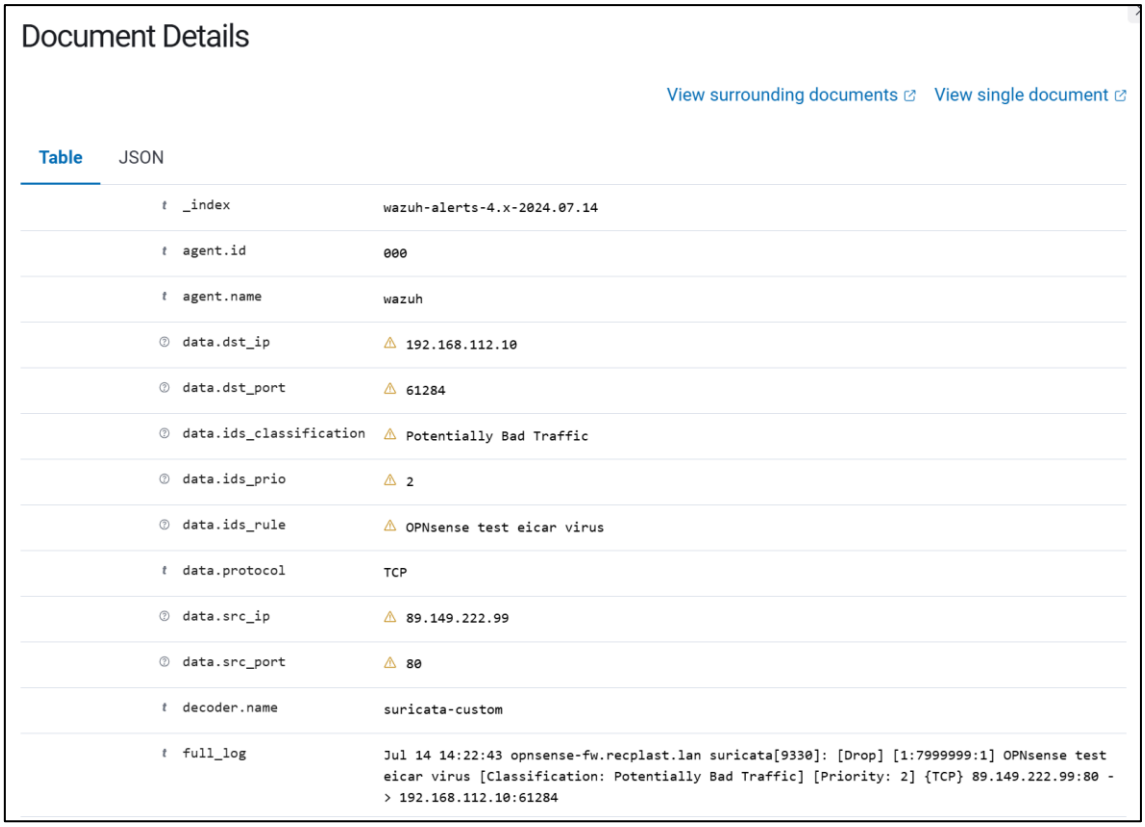

Bild 46 - Suricata-Alerts in Wazuh mit eigenem Decoder

Die ausgelösten Alerts müssen nun in Shuffle zu einer automatisierten Reaktion führen. In dem eingangs eingerichteten Test Workflow werden die Suricata Alerts bereits verarbeitet, wie in Bild 47 zu sehen ist.

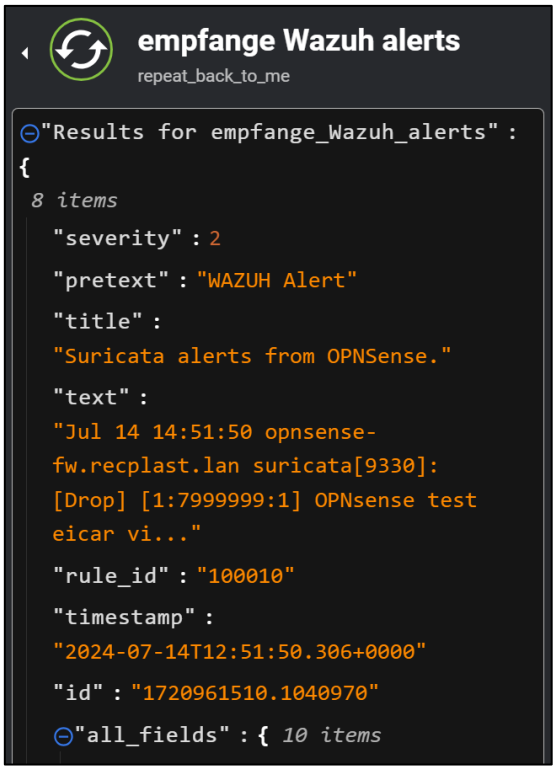

Bild 47 - In Shuffle empfangene Suricata Alerts

Um in künftigen Ausführungen dieses Workflows auf ausschließlich diese Alerts einzuschränken, wird der Branch zwischen dem Wazuh Webhook und der Shuffle Tools Node um die Condition erweitert, dass das Feld „$exec.all_fields.rule_id“ den Wert „100010“, also die ID der in Wazuh definierten Rule, enthält (siehe Bild 48).

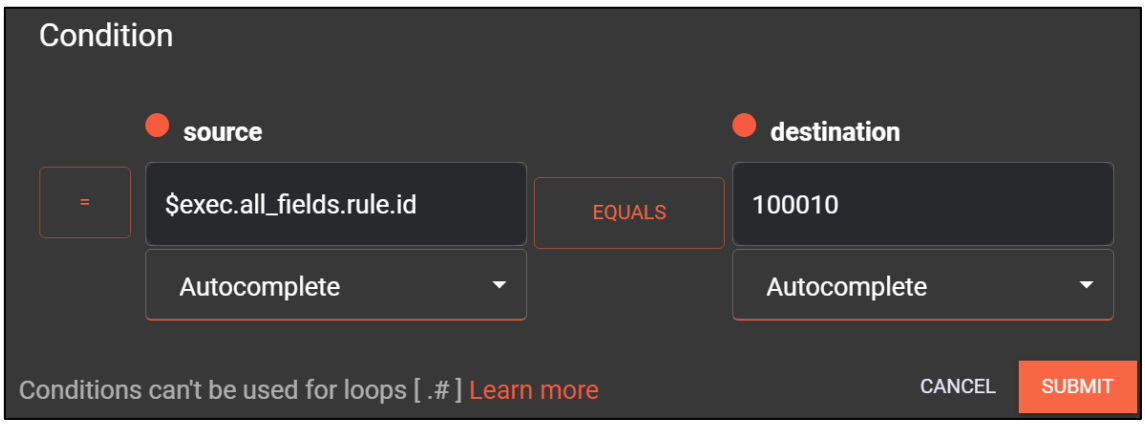

Bild 48 - Filterung der Wazuh Alerts in Shuffle

Zur Verwendung der API in OPNsense wird zunächst ein technischer User für

Shuffle eingerichtet, um vollständigen Root-Zugriff auf OPNSense durch Shuffle für verhindern. Für den User wird die Gruppe „technical_users“ angelegt und nur mit den Berechtigungen „Firewall: Rules“ und „Firewall: Automation: Filter“ ausgestattet (siehe Bild 49).

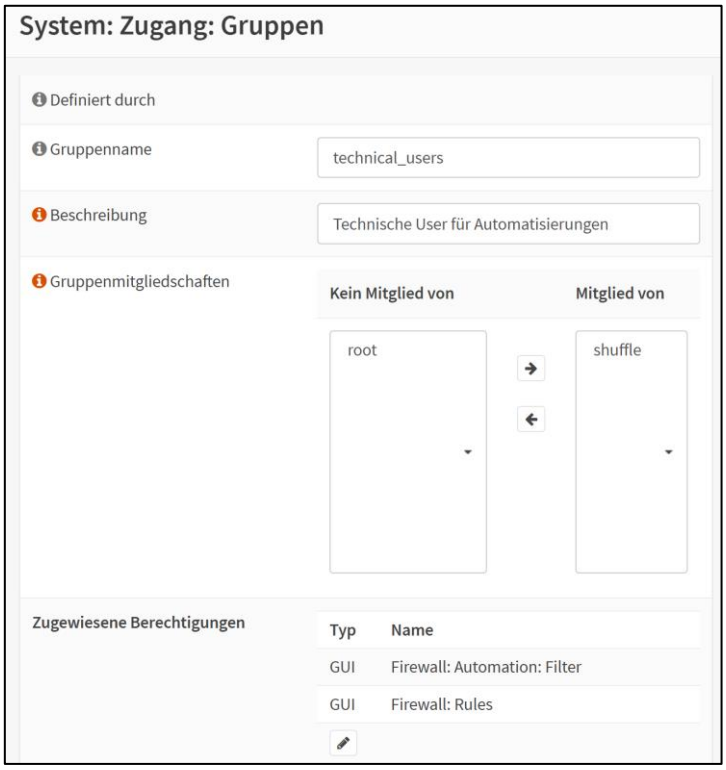

Bild 49 - Berechtigungen des Shuffle-Users in OPNsense

Für den User wird nun in den Benutzereinstellungen ein API-Key angelegt, wie in der OPNsense Dokumentation beschrieben [107] und in den Shuffle-Nodes für die HTTP-Aufrufe als Anmeldedaten hinterlegt.

Um genauer festzustellen, welche Request-Parameter für die Neuanlage einer Firewallregel erforderlich sind, wird mit aktivierten Entwicklerwerkzeugen im Browser eine neue Firewall-Regel im Bereich Automatisierung eingerichtet, die einen nicht existierenden Client mit der IP-Adresse 192.168.112.25 vollständig an der Kommunikation an die Firewall hindern soll.

Die hierdurch entstehende Request wird in den Entwicklerwerkzeugen aufgezeichnet und dient als Vorlage für die Erstellung der Request in Shuffle.

Dieses Vorgehen wird in Bild 50 gezeigt und auch für den Klick auf den „Anwenden“-Button nach Anlage der Regel durchgeführt.

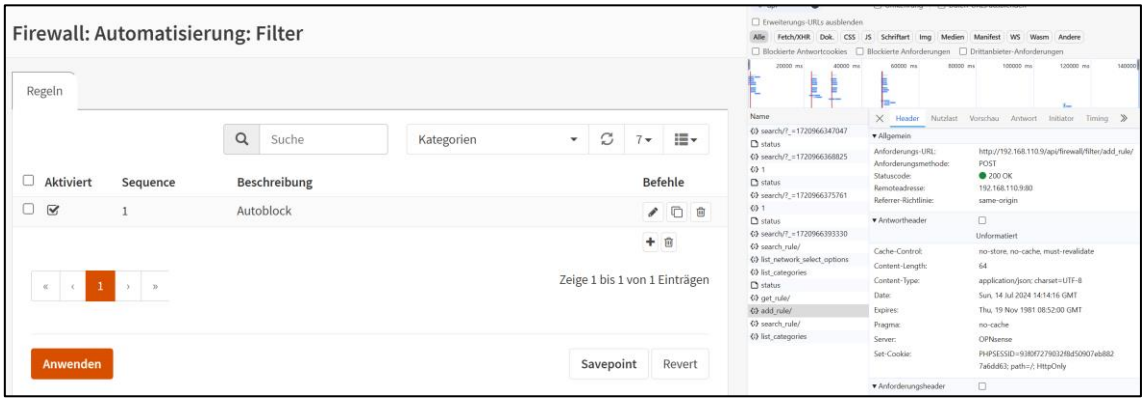

Bild 50 - Aufzeichnung der OPNsense Webinterface API-Requests

Die aufgezeichneten Requests sind in Tabelle 31 aufgeschlüsselt und werden im nächsten Schritt in Shuffle übertragen.

Tabelle 31 - Aufgezeichnete API-Requests des OPNsense Webinterface

Request 1: Erstellen der Firewall-Regel	
URI	http://192.168.110.9/api/firewall/filter/add_rule/
Methode	POST
Body	{"rule": { "enabled": "1", "sequence": "1", "action": "block", "quick": "1", "interface": "opt1", "direction": "in",

	"ipprotocol": "inet", "protocol": "any", "source_net": "192.168.111.25", "source_port": "", "source_not": "0", "destination_net": "any", "destination_not": "0", "destination_port": "", "gateway": "", "log": "0", "categories": "", "description": "Autoblock"}}
Request 2: Anwenden der Änderungen	
URI	http://192.168.110.9/api/firewall/filter/apply
Methode	POST
Body	{}

Für beide Requests wird jeweils eine HTTP-Node im Shuffle-Workflow angelegt, die entsprechend als „OPNsense blockiere IP“ und „OPNsense übernehme Änderungen“ benannt werden. Zwischen den HTTP-Nodes wird eine weitere Shuffle Tools Node mit der Aktion „Repeat back to me“ eingesetzt, um die Antwort der Firewall auf die Anlage der Regel einsehen zu können (siehe Bild 51).

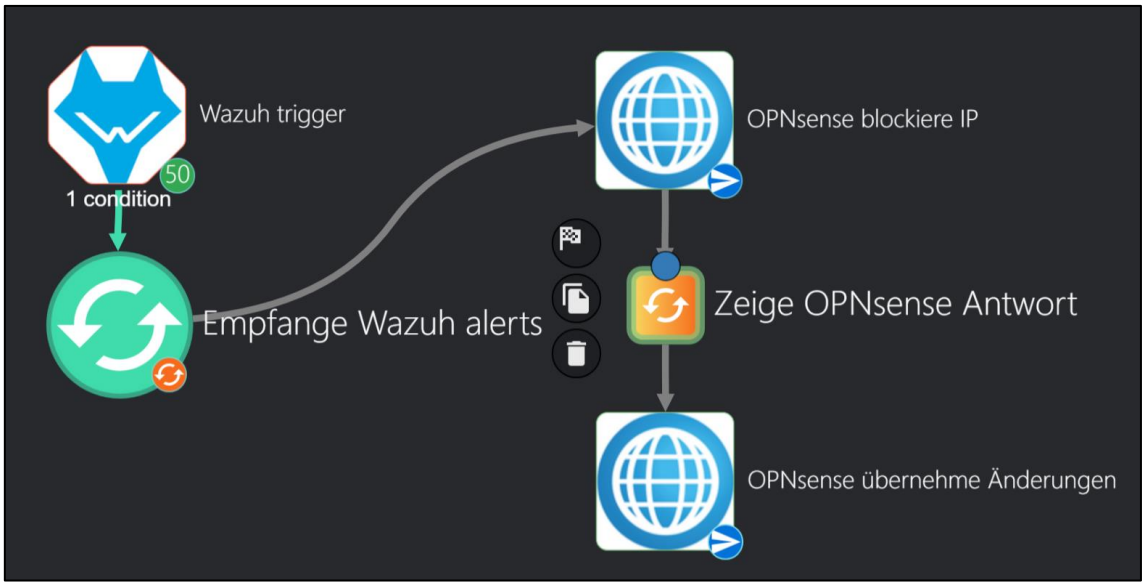

Bild 51 - OPNsense API Nodes in Shuffle

Die URIs der Requests aus Tabelle 31 werden übernommen, wobei die IP-Adresse von OPNsense zur direkten Adressierung aus dem Server-Netz zu 192.168.111.9 geändert wird.

Im Body der Request wird für die „OPNsense übernehme Änderungen“ Node der leere JSON-Body übernommen, für die Node „OPNsense blockiere IP“ soll jedoch als „source_net“ für die anzulegende Firewallregel jedoch die genaue IP des Clients automatisch ausgefüllt werden, der den Alert ausgelöst hat. Hierzu wird der Body aus Tabelle 31 übernommen. Unter „Autocomplete“ schlägt Shuffle nun die aus vorigen Durchläufen des Workflows, in denen bislang nur die von Wazuh empfangenen Daten wiederholt wurden, bekannten JSON-Schlüssel vor (siehe Bild 52).

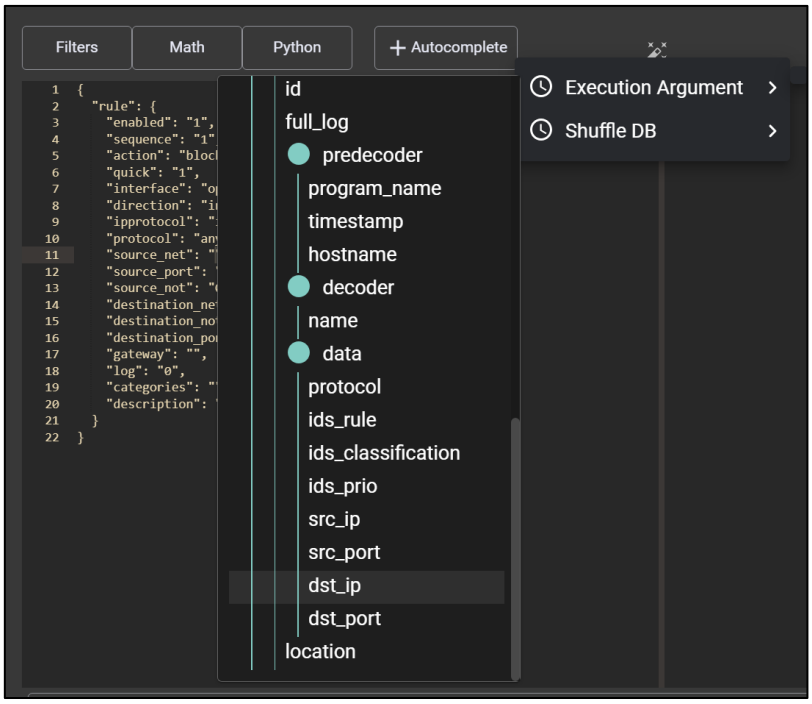

Bild 52 - Shuffle Autocomplete auf Basis vergangener Workflow-Durchläufe

So kann das Feld „dst_ip“ einfach gesucht und angeklickt werden, Shuffle generiert hierfür automatisch die Variable „$exec.all_fields.data.dst_ip“. Diese wird als Wert zum JSON-Schlüssel „source_net“ gesetzt. Um die in OPNsense auftauchende Regel nachvollziehbarer zu machen, wird die „description“ noch zu „Endpoint triggered Wazuh rule $exec.all_fields.rule.id“ geändert. So taucht die Wazuh-Regel, deren Auslösen letztendlich zur Firewall-Blockierung geführt hat, direkt in der Firewall-Regel auf. Shuffle befüllt in der Vorschau „Expected Output“ die Variablen automatisch mit den Werten des letzten Durchlaufs, sodass genau sichtbar ist, wie der Request-Body in den folgenden Durchläufen konstruiert wird (siehe Bild 53).

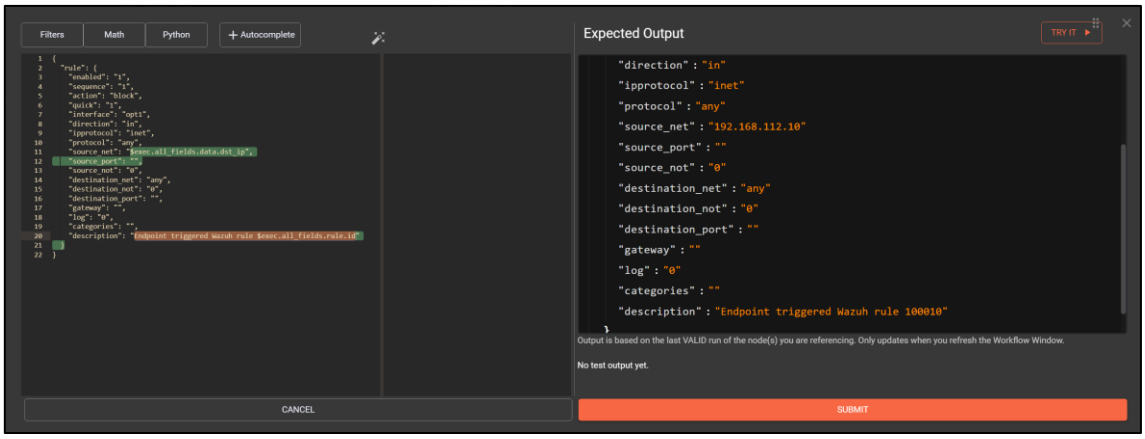

Bild 53 - Shuffle Vorschau auf Request-Variablen

Der Workflow wird nun gespeichert.

Kurz darauf werden Workflow-Durchläufe angezeigt, die nicht von der zuvor definierten Wazuh-Regel ausgelöst wurden und somit aufgrund der Filterung auf die Wazuh-Regel eigentlich ausgefiltert werden sollten (beispielsweise für Abmeldeereignisse wie in Bild 54).

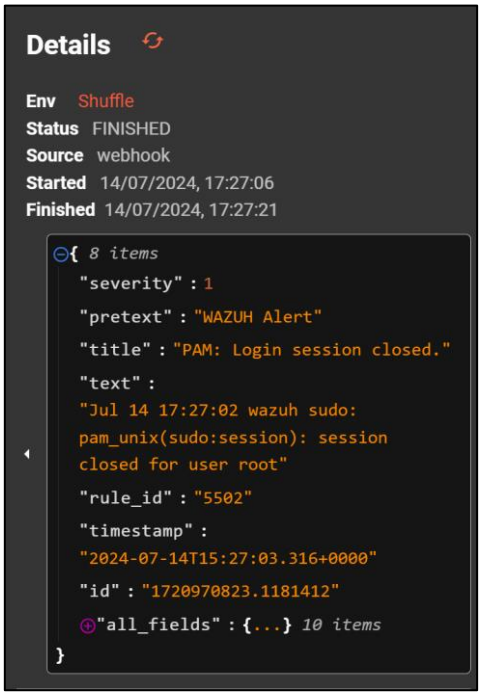

Bild 54 - Abmeldeereignis in Shuffle Workflow

Offensichtlich funktioniert die Filterung mit dem Conditional zwischen Webhook

und Shuffle Tool Node nicht wie erwartet, wobei gemäß der Workflows-Dokumentation von Shuffle die Condition auf dem Branch genügen sollte [108].

Um die Filterung expliziter zu gestalten, wird die Node „Empfange Wazuh Alerts“ zu „Extrahiere Regel“ umbenannt und gibt nun den Wert „$exec.all_fields.rule.id“ wieder, der zuvor als Conditional auf der Kante zwischen Webhook und „Empfange Wazuh Alerts“ lag. Der Conditional wird gelöscht. Stattdessen wird nun die Kante zwischen den Nodes „Extrahiere Regel“ und „OPNsense blockiere IP“ um einen Conditional erweitert, der prüft, dass „$extrahiere_regel“, also das Ergebnis der Regelextraktion der entsprechenden Node, „100010“, also der gesuchten Wazuh-Rule, entspricht (siehe Bild 55).

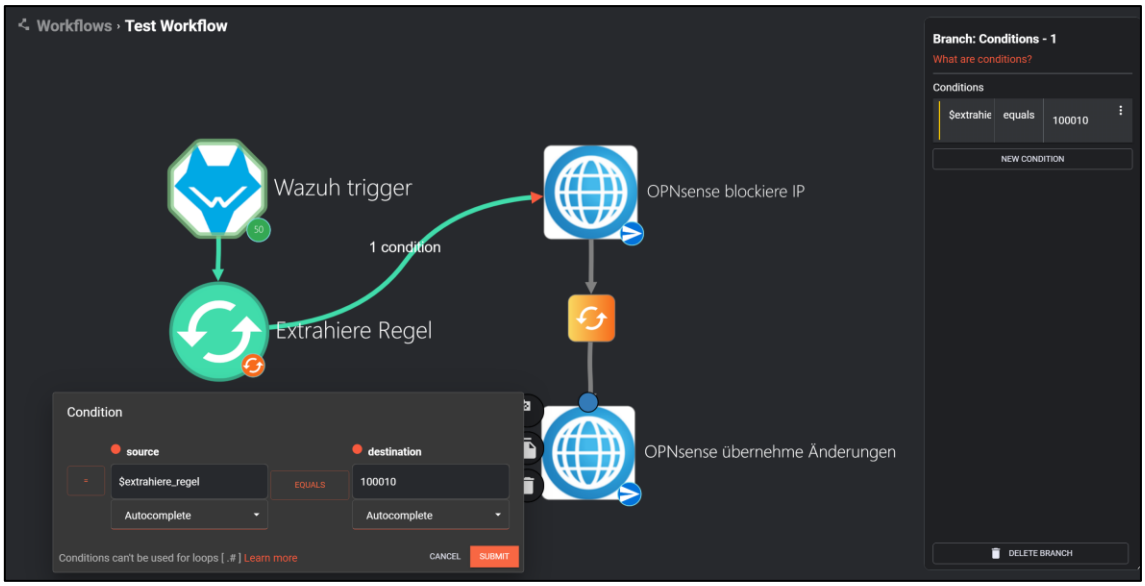

Bild 55 - Finaler Shuffle Workflow

Nach einem Test durch Ausführung von „sudo su“ und Rückkehr zum Recplast-Benutzer auf dem Wazuh-Server werden nun entsprechende Workflow-Durchläufe angezeigt, die drei der vier Nodes, also die für die API-Aufrufe in OPNsense zuständigen, wie erwartet überspringen (siehe Bild 56).

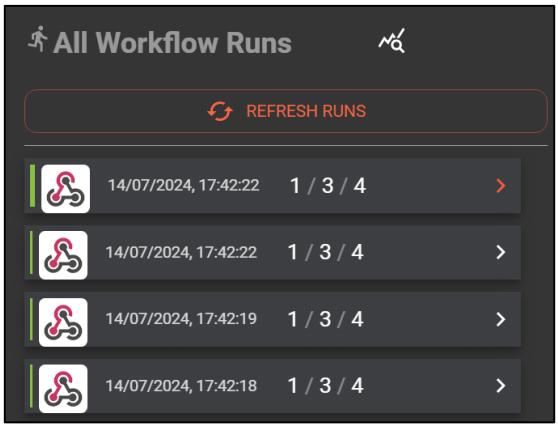

Bild 56 - Übersprungene Workflow-Durchläufe in Shuffle

Ein erneuter Test durch Download der EICAR-Testdatei auf dem Windows Client erzeugt einen Workflow-Durchlauf, der alle Nodes passiert und die Antwort „saved“ von OPNsense zur Folge hat (siehe Bild 57).

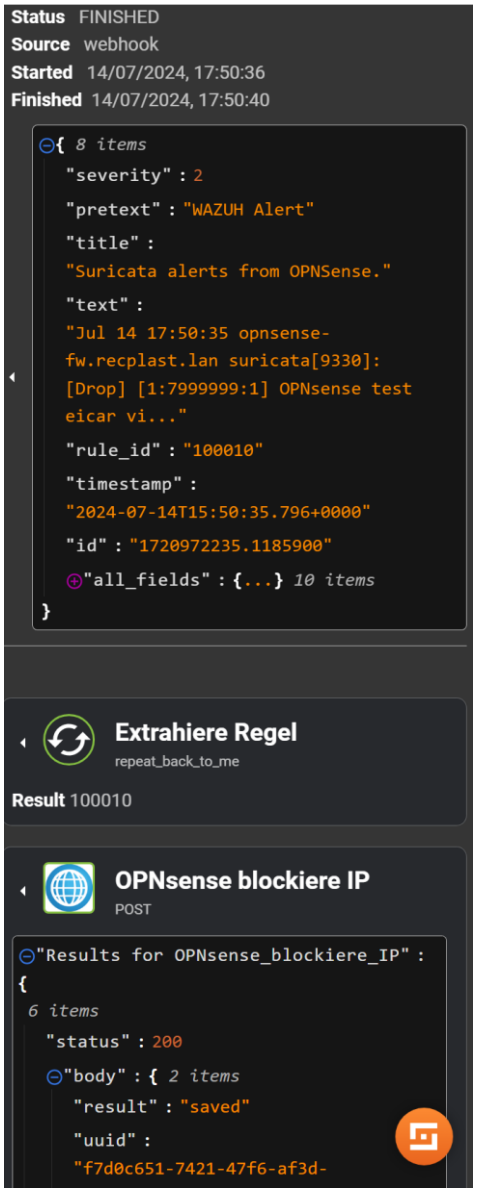

Bild 57 - Erfolgreicher Workflow-Durchlauf in Shuffle

Die neu angelegte Firewall-Regel ist auf der Weboberfläche von OPNsense in Bild 58 zu sehen.

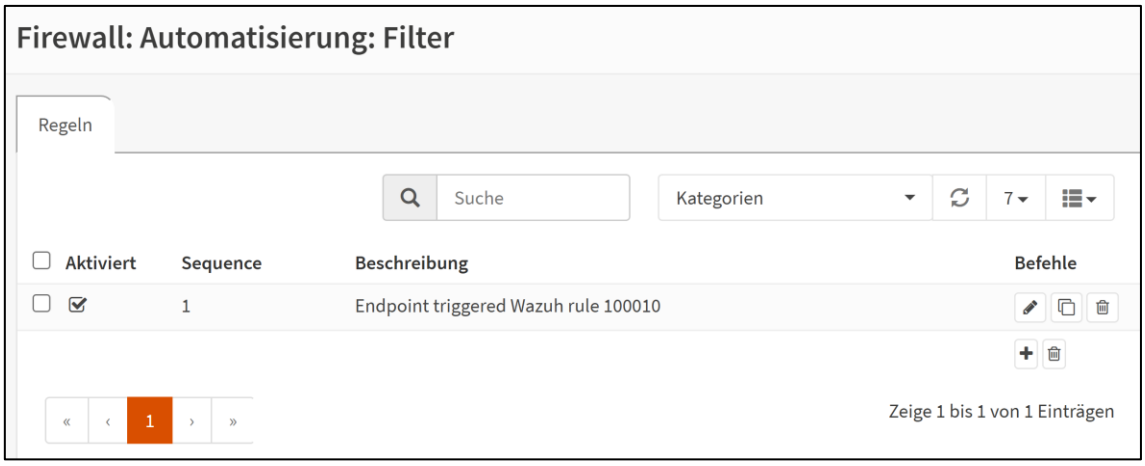

Bild 58 - Durch Shuffle automatisch generierte OPNsense-Firewallregel

Ein Test mittels Ping in Powershell zeigt, dass der Client von der Kommunikation in das Server-Netzwerk und das Internet bzw. das DMZ-Netzwerk isoliert ist (siehe Bild 59).

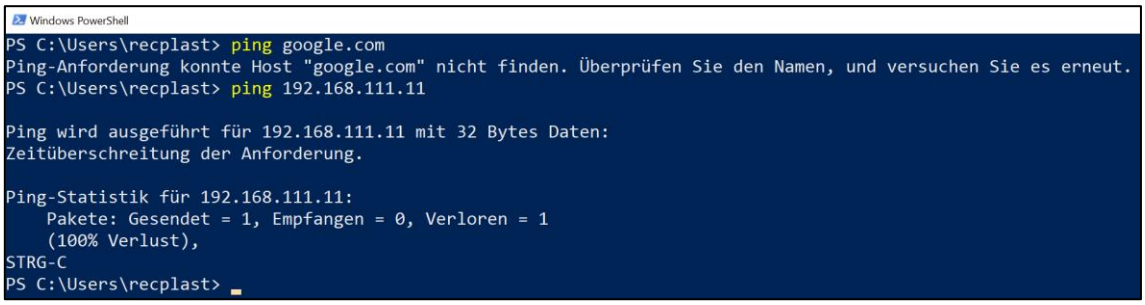

Bild 59 - Netzwerkisolierung des Windows Client

Der Prototyp hat somit die Fähigkeit demonstriert, einen schadhaften Download mittels Suricata als IPS zu erkennen, zu blockieren, in Wazuh als SIEM zu alarmieren und den betreffenden Endpunkt mittels Shuffle als SOAR automatisiert zu isolieren.

Der ausgeführte Workflow über die Systeme hinweg wird zur Verdeutlichung in Bild 60 visualisiert.

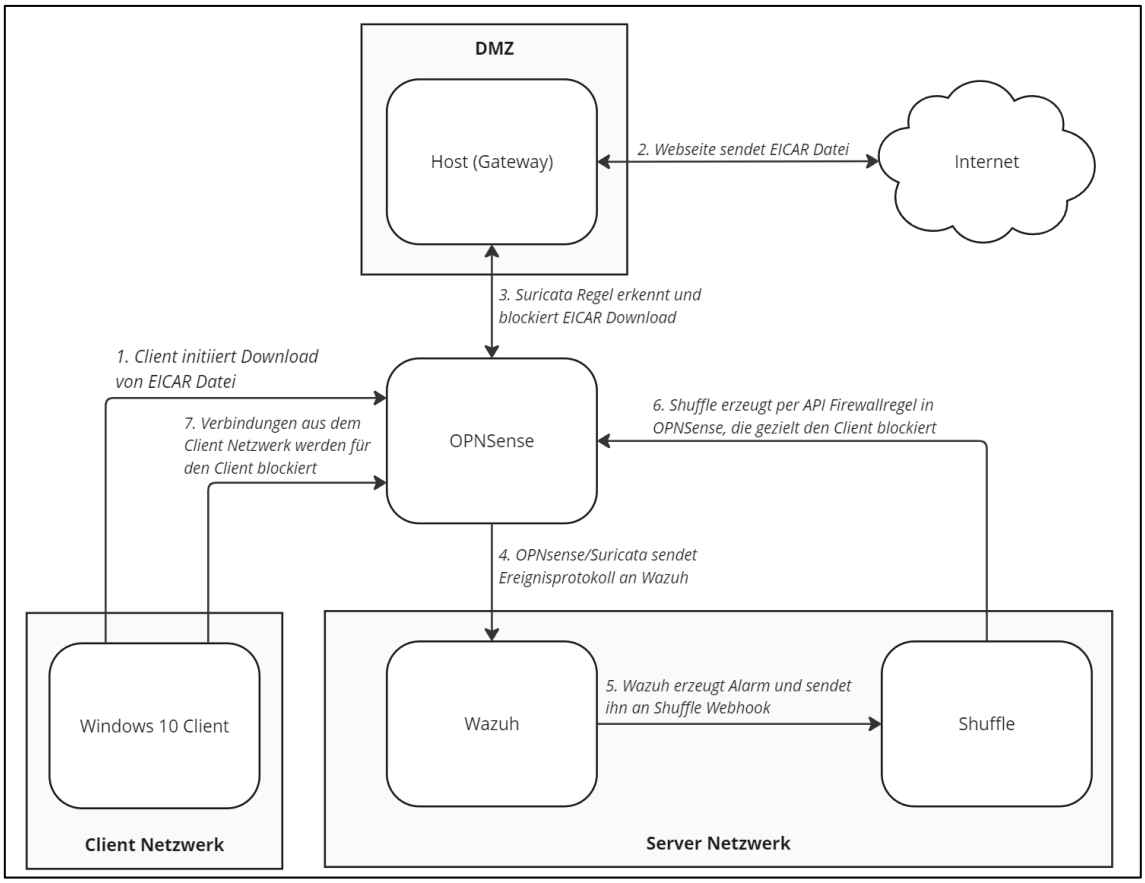

Bild 60 - Gesamtablauf des exemplarischen Prototyp-Workflows

6 Bewertung des Prototyps

In diesem Kapitel wird jedes in Kapitel 5 installierte FOSS Tool in einem eigenen Unterkapitel auf seine Erfüllung der Anforderungen der OH-SzA untersucht.

Im darauffolgenden Unterkapitel wird eine Gesamtauswertung über alle installierten FOSS Tools hinweg durchgeführt und die erfüllten technischen Anforderungen der OH-SzA durch den Gesamt-Prototypen identifiziert.

In einem weiteren Unterkapitel werden Schwierigkeiten in der prototypischen Umsetzung, nicht erfüllte Anforderungen oder Verbesserungspotenziale in der Verwaltung oder Bedienung der FOSS Tools genauer beschrieben. Hierdurch sollen in möglichen realen Umsetzungen Aufwände besser eingeschätzt oder Fehlerquellen vermieden werden können.

Durch die Identifikation erfüllter und nicht erfüllter Anforderungen in den beiden vorherigen Unterkapiteln wird in einem abschließenden ein Überblick erzeugt, welche Anforderungen der OH-SzA mittels FOSS Tools erfüllbar sind und welche mit den gewählten Tools nicht. Das Resultat wird auf das in der OH-SzA definierte Modell zur Nachweiserbringung übertragen, um ein in der Realität mögliches Auditergebnis zu simulieren.

Bereits in Kapitel 3 als nicht relevant erkannte Anforderungen werden nicht erneut geprüft.

6.1 Wazuh

Wazuh bietet, wie in Kapitel 4.2.2 beschrieben, Funktionen in den Bereichen der Protokollierung, Detektion und Reaktion und wird demnach in allen drei Bereichen geprüft.

Die vollständige Prüfmatrix ist in Anlage 16 angehängt.

Tabelle 32 - Anforderungserfüllung durch Wazuh im Prototyp

Bereich	Modalverb	Anforderungen	Erfüllt
Übergreifend	MUSS	1	1
Übergreifend	SOLL	0	0
Übergreifend	KANN	0	0
Protokollierung	MUSS	8	8
Protokollierung	SOLL	1	1
Protokollierung	KANN	2	1
Detektion	MUSS	19	18
Detektion	SOLL	0	0
Detektion	KANN	2	2
Reaktion	MUSS	2	2
Reaktion	SOLL	2	2
Reaktion	KANN	4	4
Gesamt	MUSS	30	29
Gesamt	SOLL	3	3
Gesamt	KANN	4	3

Wazuh erfüllt somit beinahe alle durch die SzA erfüllbaren Anforderungen. Die nicht erfüllte MUSS- und die nicht erfüllte KANN-Anforderung (Nummer 9 und 95) beziehen sich auf die Verwendung eines NIDS, was Wazuh nicht leisten kann, sowie die Nutzung zusätzlicher Systeme, sodass nicht jedes zu überwachende System protokollieren muss. Wazuh ist jedoch auf die Einlieferung von

Protokolldaten angewiesen und verfügt nicht über netzbasierte oder ähnliche Angriffserkennungsmethoden.

Die in Kapitel 4.2.2 identifizierte Lücke in der Erfüllung der Anforderung Nummer 115, bereits überprüfte Protokolldaten hinsichtlich sicherheitsrelevanter Ereignisse regelmäßig automatisch erneut zu untersuchen, konnte im Prototyp doch umgesetzt werden, indem Dashboards auf den Wazuh Archives eingerichtet und so bereits überprüfte Protokolldaten erneut angezeigt werden. Durch geschickte Gestaltung der Dashboards, zum Beispiel zur Anzeige fehlgeschlagener Logins, können so sicherheitsrelevante Ereignisse auch in bereits überprüften Protokolldaten sichtbar gemacht werden. Um eine regelmäßige Untersuchung der Dashboards sicherzustellen, muss ein entsprechender Prozess geschaffen werden.

6.2 Shuffle

Shuffle bietet, wie in Kapitel 4.2.4 beschrieben, Funktionen im Bereich der Reaktion und wird demnach in diesem Bereich geprüft.

Die vollständige Prüfmatrix ist in Anlage 17 angehängt.

Tabelle 33 - Anforderungserfüllung durch Shuffle im Prototyp

Bereich	Modalverb	Anforderungen	Erfüllt
Übergreifend	MUSS	1	1
Übergreifend	SOLL	0	0
Übergreifend	KANN	0	0
Reaktion	MUSS	2	2
Reaktion	SOLL	2	2
Reaktion	KANN	4	4

Bereich	Modalverb	Anforderungen	Erfüllt
Gesamt	MUSS	3	3
Gesamt	SOLL	2	2
Gesamt	KANN	4	4

Shuffle erfüllt somit alle durch die SzA erfüllbaren Anforderungen an die Reaktion sowie die übergreifende Anforderung.

Über Shuffle können theoretisch beliebige automatisierte Reaktionsabläufe erstellt und ausgeführt werden, insofern eine Integration für die Reaktion geeigneter Systeme möglich ist. Durch die Integration weiterer Systeme wie Mailservern, Schadsoftware-Scannern oder Ticketsystemen kann nicht nur die Reaktion, sondern auch die Detektion von Automatisierung profitieren, indem Analyseschritte ohne manuelle Aktionen von SOC-Personal automatisch durchgeführt werden. Beispielsweise könnte eine externe IP-Adresse, die eine Suricata-Regel in OPNsense auslöst, automatisch in einem Reputationsprüfer wie dem Talos Reputation Center (https://www.talosintelligence.com/reputation_center) bewertet werden.

6.3 Suricata

Suricata wird als NIDS verwendet und daher nur gegen die in Kapitel 4.2.3 genannten relevanten Anforderungen 9, 13 und 95 geprüft.

Die vollständige Prüfmatrix ist in Anlage 18 angehängt.

Tabelle 34 - Anforderungserfüllung durch Suricata im Prototyp

Bereich	Modalverb	Anforderungen	Erfüllt
Übergreifend	MUSS	1	1

Bereich	Modalverb	Anforderungen	Erfüllt
Übergreifend	SOLL	0	0
Übergreifend	KANN	0	0
Protokollierung	MUSS	0	0
Protokollierung	SOLL	1	1
Protokollierung	KANN	1	1
Detektion	MUSS	1	1
Detektion	SOLL	0	0
Detektion	KANN	0	0
Gesamt	MUSS	1	1
Gesamt	SOLL	1	1
Gesamt	KANN	1	1

Suricata erfüllt damit alle auf NIDS anwendbaren technischen Anforderungen im Bereich der Protokollierung und Detektion, sowie die übergreifende.

6.4 Erfüllte Anforderungen

Die Prüftabellen von Wazuh, Shuffle und Suricata werden übereinandergelegt, wobei aus Gründen der Übersichtlichkeit die Anforderungen nicht inhaltlich wiederholt werden, sondern auf ihre Nummer entsprechend Anlage 1 bis Anlage 4 verwiesen wird. Für jedes System wird die Erfüllung oder Nichterfüllung der Anforderung entsprechend Kapitel 6.1 bis Kapitel 6.3 vermerkt. Erfüllt eines der drei Systeme die Anforderung, wird sie insgesamt als erfüllt gewertet, andernfalls als nicht erfüllt.

Die als nicht durch die SzA, sondern organisatorisch oder prozessual zu erfüllenden Anforderungen werden anhand der theoretischen Maßnahmen aus Kapitel 5.2 mit dem Vermerk „Orga“ in der Spalte „Erfüllt: Gesamt“ als theoretisch berücksichtigt markiert.

Die dadurch entstehende Gesamtübersicht über die Anforderungserfüllung durch den Prototyp auf technischer Ebene sowie die theoretischen Maßnahmen auf organisatorischer Ebene wird in Tabelle 35 dargelegt.

Die Anforderungen Nummer 20, 59, 126 und 127 beschreiben keine eigenständigen Anforderungen, sondern fordern die Erfüllung aller Basisanforderungen der Grundschutz-Bausteine OPS.1.1.5, DER.1 und DER.2.1 sowie die Standardanforderungen von DER.2.1, die alle wiederum als eigenständige Anforderungen aufgenommen wurden (siehe Anlage 1 bis Anlage 4). Somit sind diese Anforderungen durch Erfüllung der mit aufgenommenen Anforderungen aus den Grundschutz-Bausteinen automatisch erfüllt und nicht durch eine explizite Maßnahme zu erfüllen, weshalb sie als „n.a.“ vermerkt werden.

Tabelle 35 - Gesamtübersicht der Anforderungserfüllung durch den Prototyp

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
1	MUSS	n.a.	n.a.	n.a.	Orga
2	MUSS	n.a.	n.a.	n.a.	Orga
3	MUSS	n.a.	n.a.	n.a.	Orga
4	MUSS	Ja	Ja	Ja	Ja
5	MUSS	n.a.	n.a.	n.a.	Orga
6	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
7	MUSS	n.a.	n.a.	n.a.	Orga
8	MUSS	Ja	n.a.	n.a.	Ja
9	KANN	Nein	n.a.	Ja	Ja
10	MUSS	n.a.	n.a.	n.a.	Orga
11	MUSS	Ja	n.a.	n.a.	Ja
12	MUSS	n.a.	n.a.	n.a.	Orga
13	SOLL	Ja	n.a.	Ja	Ja
14	KANN	n.a.	n.a.	n.a.	Orga
15	MUSS	n.a.	n.a.	n.a.	Orga
16	MUSS	n.a.	n.a.	n.a.	Orga
17	SOLL	n.a.	n.a.	n.a.	Orga
18	MUSS	n.a.	n.a.	n.a.	Orga
19	MUSS	n.a.	n.a.	n.a.	Orga
20	MUSS	n.a.	n.a.	n.a.	n.a.
21	MUSS	n.a.	n.a.	n.a.	Orga
22	MUSS	n.a.	n.a.	n.a.	Orga
23	MUSS	n.a.	n.a.	n.a.	Orga
24	MUSS	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
25	MUSS	n.a.	n.a.	n.a.	Orga
26	MUSS	n.a.	n.a.	n.a.	Orga
27	MUSS	n.a.	n.a.	n.a.	Orga
28	MUSS	n.a.	n.a.	n.a.	Orga
29	MUSS	n.a.	n.a.	n.a.	Orga
30	MUSS	n.a.	n.a.	n.a.	Orga
31	MUSS	n.a.	n.a.	n.a.	Orga
32	MUSS	n.a.	n.a.	n.a.	Orga
33	MUSS	n.a.	n.a.	n.a.	Orga
34	MUSS	n.a.	n.a.	n.a.	Orga
35	MUSS	Ja	n.a.	n.a.	Ja
36	MUSS	n.a.	n.a.	n.a.	Orga
37	MUSS	Ja	n.a.	n.a.	Ja
38	MUSS	n.a.	n.a.	n.a.	Orga
39	MUSS	n.a.	n.a.	n.a.	Orga
40	MUSS	n.a.	n.a.	n.a.	Orga
41	MUSS	n.a.	n.a.	n.a.	Orga
42	MUSS	Ja	n.a.	n.a.	Ja

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
43	MUSS	Ja	n.a.	n.a.	Ja
44	SOLL	n.a.	n.a.	n.a.	Orga
45	MUSS	n.a.	n.a.	n.a.	Orga
46	MUSS	n.a.	n.a.	n.a.	Orga
47	MUSS	Ja	n.a.	n.a.	Ja
48	MUSS	Ja	n.a.	n.a.	Ja
49	KANN	Ja	n.a.	n.a.	Ja
50	SOLL	n.a.	n.a.	n.a.	Orga
51	SOLL	n.a.	n.a.	n.a.	Orga
52	SOLL	n.a.	n.a.	n.a.	Orga
53	MUSS	n.a.	n.a.	n.a.	Orga
54	MUSS	n.a.	n.a.	n.a.	Orga
55	MUSS	Ja	n.a.	n.a.	Ja
56	MUSS	n.a.	n.a.	n.a.	Orga
57	KANN	Ja	n.a.	n.a.	Ja
58	KANN	n.a.	n.a.	n.a.	Orga
59	MUSS	n.a.	n.a.	n.a.	n.a.
60	MUSS	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
61	MUSS	n.a.	n.a.	n.a.	Orga
62	MUSS	n.a.	n.a.	n.a.	Orga
63	MUSS	n.a.	n.a.	n.a.	Orga
64	MUSS	n.a.	n.a.	n.a.	Orga
65	MUSS	n.a.	n.a.	n.a.	Orga
66	MUSS	n.a.	n.a.	n.a.	Orga
67	MUSS	n.a.	n.a.	n.a.	Orga
68	MUSS	n.a.	n.a.	n.a.	Orga
69	MUSS	n.a.	n.a.	n.a.	Orga
70	MUSS	n.a.	n.a.	n.a.	Orga
71	MUSS	n.a.	n.a.	n.a.	Orga
72	MUSS	n.a.	n.a.	n.a.	Orga
73	MUSS	n.a.	n.a.	n.a.	Orga
74	MUSS	n.a.	n.a.	n.a.	Orga
75	MUSS	n.a.	n.a.	n.a.	Orga
76	MUSS	n.a.	n.a.	n.a.	Orga
77	MUSS	n.a.	n.a.	n.a.	Orga
78	MUSS	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
79	MUSS	n.a.	n.a.	n.a.	Orga
80	MUSS	Ja	n.a.	n.a.	Ja
81	MUSS	n.a.	n.a.	n.a.	Orga
82	MUSS	n.a.	n.a.	n.a.	Orga
83	MUSS	n.a.	n.a.	n.a.	Orga
84	MUSS	Ja	n.a.	n.a.	Ja
85	MUSS	Ja	n.a.	n.a.	Ja
86	MUSS	n.a.	n.a.	n.a.	Orga
87	MUSS	Ja	n.a.	n.a.	Ja
88	KANN	Ja	n.a.	n.a.	Ja
89	MUSS	n.a.	n.a.	n.a.	Orga
90	MUSS	n.a.	n.a.	n.a.	Orga
91	MUSS	n.a.	n.a.	n.a.	Orga
92	MUSS	n.a.	n.a.	n.a.	Orga
93	MUSS	Ja	n.a.	n.a.	Ja
94	MUSS	n.a.	n.a.	n.a.	Orga
95	MUSS	Nein	n.a.	Ja	Ja
96	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
97	MUSS	Ja	n.a.	n.a.	Ja
98	MUSS	Ja	n.a.	n.a.	Ja
99	MUSS	Ja	n.a.	n.a.	Ja
100	MUSS	n.a.	n.a.	n.a.	Orga
101	MUSS	n.a.	n.a.	n.a.	Orga
102	MUSS	n.a.	n.a.	n.a.	Orga
103	MUSS	n.a.	n.a.	n.a.	Orga
104	MUSS	n.a.	n.a.	n.a.	Orga
105	SOLL	n.a.	n.a.	n.a.	Orga
106	SOLL	n.a.	n.a.	n.a.	Orga
107	MUSS	n.a.	n.a.	n.a.	Orga
108	MUSS	Ja	n.a.	n.a.	Ja
109	MUSS	Ja	n.a.	n.a.	Ja
110	MUSS	Ja	n.a.	n.a.	Ja
111	MUSS	Ja	n.a.	n.a.	Ja
112	MUSS	Ja	n.a.	n.a.	Ja
113	MUSS	n.a.	n.a.	n.a.	Orga
114	MUSS	Ja	n.a.	n.a.	Ja

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
115	MUSS	Ja	n.a.	n.a.	Ja
116	MUSS	Ja	n.a.	n.a.	Ja
117	MUSS	n.a.	n.a.	n.a.	Orga
118	SOLL	n.a.	n.a.	n.a.	Orga
119	SOLL	n.a.	n.a.	n.a.	Orga
120	SOLL	n.a.	n.a.	n.a.	Orga
121	MUSS	Ja	n.a.	n.a.	Ja
122	SOLL	n.a.	n.a.	n.a.	Orga
123	SOLL	n.a.	n.a.	n.a.	Orga
124	MUSS	n.a.	n.a.	n.a.	Orga
125	MUSS	n.a.	n.a.	n.a.	Orga
126	MUSS	n.a.	n.a.	n.a.	n.a.
127	SOLL	n.a.	n.a.	n.a.	n.a.
128	MUSS	n.a.	n.a.	n.a.	Orga
129	MUSS	n.a.	n.a.	n.a.	Orga
130	MUSS	n.a.	n.a.	n.a.	Orga
131	MUSS	n.a.	n.a.	n.a.	Orga
132	MUSS	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
133	MUSS	n.a.	n.a.	n.a.	Orga
134	MUSS	n.a.	n.a.	n.a.	Orga
135	MUSS	n.a.	n.a.	n.a.	Orga
136	MUSS	n.a.	n.a.	n.a.	Orga
137	MUSS	n.a.	n.a.	n.a.	Orga
138	MUSS	n.a.	n.a.	n.a.	Orga
139	MUSS	n.a.	n.a.	n.a.	Orga
140	MUSS	n.a.	n.a.	n.a.	Orga
141	MUSS	n.a.	n.a.	n.a.	Orga
142	MUSS	n.a.	n.a.	n.a.	Orga
143	MUSS	n.a.	n.a.	n.a.	Orga
144	MUSS	n.a.	n.a.	n.a.	Orga
145	MUSS	n.a.	n.a.	n.a.	Orga
146	MUSS	n.a.	n.a.	n.a.	Orga
147	MUSS	n.a.	n.a.	n.a.	Orga
148	MUSS	n.a.	n.a.	n.a.	Orga
149	MUSS	n.a.	n.a.	n.a.	Orga
150	MUSS	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
151	MUSS	n.a.	n.a.	n.a.	Orga
152	MUSS	n.a.	n.a.	n.a.	Orga
153	MUSS	n.a.	n.a.	n.a.	Orga
154	MUSS	n.a.	n.a.	n.a.	Orga
155	MUSS	n.a.	n.a.	n.a.	Orga
156	MUSS	n.a.	n.a.	n.a.	Orga
157	MUSS	n.a.	n.a.	n.a.	Orga
158	MUSS	n.a.	n.a.	n.a.	Orga
159	MUSS	n.a.	n.a.	n.a.	Orga
160	MUSS	n.a.	n.a.	n.a.	Orga
161	MUSS	n.a.	n.a.	n.a.	Orga
162	MUSS	n.a.	n.a.	n.a.	Orga
163	MUSS	n.a.	n.a.	n.a.	Orga
164	MUSS	n.a.	n.a.	n.a.	Orga
165	MUSS	n.a.	n.a.	n.a.	Orga
166	SOLL	n.a.	n.a.	n.a.	Orga
167	SOLL	n.a.	n.a.	n.a.	Orga
168	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
169	SOLL	n.a.	n.a.	n.a.	Orga
170	SOLL	n.a.	n.a.	n.a.	Orga
171	SOLL	n.a.	n.a.	n.a.	Orga
172	SOLL	n.a.	n.a.	n.a.	Orga
173	SOLL	n.a.	n.a.	n.a.	Orga
174	SOLL	n.a.	n.a.	n.a.	Orga
175	SOLL	n.a.	n.a.	n.a.	Orga
176	SOLL	n.a.	n.a.	n.a.	Orga
177	SOLL	n.a.	n.a.	n.a.	Orga
178	SOLL	n.a.	n.a.	n.a.	Orga
179	SOLL	n.a.	n.a.	n.a.	Orga
180	SOLL	n.a.	n.a.	n.a.	Orga
181	SOLL	n.a.	n.a.	n.a.	Orga
182	SOLL	n.a.	n.a.	n.a.	Orga
183	SOLL	n.a.	n.a.	n.a.	Orga
184	SOLL	n.a.	n.a.	n.a.	Orga
185	SOLL	n.a.	n.a.	n.a.	Orga
186	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
187	SOLL	n.a.	n.a.	n.a.	Orga
188	SOLL	n.a.	n.a.	n.a.	Orga
189	SOLL	n.a.	n.a.	n.a.	Orga
190	SOLL	n.a.	n.a.	n.a.	Orga
191	SOLL	n.a.	n.a.	n.a.	Orga
192	SOLL	n.a.	n.a.	n.a.	Orga
193	SOLL	n.a.	n.a.	n.a.	Orga
194	SOLL	n.a.	n.a.	n.a.	Orga
195	SOLL	n.a.	n.a.	n.a.	Orga
196	SOLL	n.a.	n.a.	n.a.	Orga
197	SOLL	n.a.	n.a.	n.a.	Orga
198	SOLL	n.a.	n.a.	n.a.	Orga
199	SOLL	n.a.	n.a.	n.a.	Orga
200	SOLL	n.a.	n.a.	n.a.	Orga
201	SOLL	n.a.	n.a.	n.a.	Orga
202	SOLL	n.a.	n.a.	n.a.	Orga
203	SOLL	n.a.	n.a.	n.a.	Orga
204	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
205	SOLL	n.a.	n.a.	n.a.	Orga
206	SOLL	n.a.	n.a.	n.a.	Orga
207	SOLL	n.a.	n.a.	n.a.	Orga
208	SOLL	n.a.	n.a.	n.a.	Orga
209	SOLL	n.a.	n.a.	n.a.	Orga
210	SOLL	n.a.	n.a.	n.a.	Orga
211	SOLL	n.a.	n.a.	n.a.	Orga
212	SOLL	n.a.	n.a.	n.a.	Orga
213	SOLL	n.a.	n.a.	n.a.	Orga
214	SOLL	n.a.	n.a.	n.a.	Orga
215	SOLL	n.a.	n.a.	n.a.	Orga
216	SOLL	n.a.	n.a.	n.a.	Orga
217	SOLL	n.a.	n.a.	n.a.	Orga
218	SOLL	n.a.	n.a.	n.a.	Orga
219	SOLL	n.a.	n.a.	n.a.	Orga
220	SOLL	n.a.	n.a.	n.a.	Orga
221	SOLL	n.a.	n.a.	n.a.	Orga
222	SOLL	n.a.	n.a.	n.a.	Orga

Anforderung	Modalverb	Erfüllt: Wazuh?	Erfüllt: Shuffle?	Erfüllt: Suricata?	Erfüllt: Gesamt
223	SOLL	n.a.	n.a.	n.a.	Orga
224	MUSS	Ja	Ja	n.a.	Ja
225	MUSS	n.a.	n.a.	n.a.	Orga
226	MUSS	n.a.	n.a.	n.a.	Orga
227	MUSS	n.a.	n.a.	n.a.	Orga
228	MUSS	n.a.	n.a.	n.a.	Orga
229	MUSS	n.a.	n.a.	n.a.	Orga
230	SOLL	Ja	Ja	n.a.	Ja
231	MUSS	Ja	Ja	n.a.	Ja
232	SOLL	Ja	Ja	n.a.	Ja

Insgesamt sind von 150 MUSS-Anforderungen 30 durch die SzA im Prototyp erfüllt, 117 organisatorisch erfüllt und 3 nicht selbst anwendbar, jedoch über die Erfüllung der weiteren ebenfalls erfüllt.

Von 76 SOLL-Anforderungen sind 3 durch die SzA im Prototyp erfüllt, 72 organisatorisch erfüllt und 1 nicht selbst anwendbar, jedoch über die Erfüllung der weiteren ebenfalls erfüllt.

Von 6 KANN-Anforderungen sind 4 durch die SzA im Prototyp erfüllt und 2 organisatorisch erfüllt.

In Summe sind also 37 Anforderungen durch die SzA im Prototyp und 191 Anforderungen organisatorisch erfüllt, 4 Anforderungen durch die Erfüllung der anderen ebenfalls.

Es sind keine nicht erfüllten Anforderungen vorhanden.

6.5 Herausforderungen und nicht erfüllte Anforderungen

Der Prototyp erfüllt in Verbindung mit den in Kapitel 5.2 beschriebenen organisatorischen Maßnahmen alle Anforderungen der OH-SzA für die RECPLAST GmbH.

Zwar sind die Anforderungen der OH-SzA somit erfüllt, dennoch haben sich in der Umsetzung des Prototyps stellenweise Herausforderungen und ersichtliche Verbesserungspotenziale ergeben, die im Folgenden genauer erläutert werden.

So haben sich in der Einrichtung von Wazuh Schwierigkeiten in der Verwendung von Wazuh Archives ergeben, genauer in der Durchsuchbarmachung der enthaltenen Daten. Die Auswahl des Index Pattern, das definiert, welche Indizes vom Dashboard durchsucht werden sollen, ist in der Dokumentation zur eingesetzten Version von Wazuh anders beschrieben, als es tatsächlich umgesetzt werden musste (siehe Kapitel 5.3.2). Die Dokumentation zumindest in Teilen nicht auf das reale System zu passen, was in der Einrichtung zwar durch Durchsuchen des Menüs gelöst werden konnte, im laufenden Betrieb insbesondere bei Störungen allerdings ein großes Problem sein kann.

Eine ähnliche Herausforderung ergab sich in der Einrichtung des Shuffle Workflows, worin zwar die Verwendung von Conditionals zur Filterung von Daten und Steuerung des Workflow-Ablaufs beschrieben steht, in der Umsetzung jedoch unerwartetes Verhalten erzeugt hat. Der Conditional scheint, wenn direkt an den Wazuh Webhook angebunden, nicht zu greifen, was aus der Dokumentation jedoch nicht hervorgeht. Die Einführung eines Zwischenschrittes zur Filterung über eine Shuffle Tools Node erzeugte dann das erwartete Verhalten.

Die Handhabung von Wazuh in der Erstellung von Rules und Decodern basiert vollständig auf der Bearbeitung von XML-Dateien, was sowohl über das Wazuh Dashboard als auch direkten Dateizugriff auf dem Wazuh Server möglich ist.

Zwar ist davon auszugehen, dass Decoder nur bei Anbindung neuer Protokolldatenquellen oder Änderungen derer Protokollformate beispielsweise nach Updates geändert werden müssen, Rules sollten jedoch regelmäßig angepasst werden, um auf veränderte Bedrohungslagen zu reagieren oder falsch positive Alerts zu reduzieren. Da hierzu manuell XML-Dateien angepasst werden müssen und keine unterstützenden Werkzeuge abgesehen von Testmöglichkeiten für bereits aktive Rules und Decoder bestehen, gestaltet sich die Bearbeitung von Rules fehleranfällig. Zwar kann für die Erstellung und das Testen regulärer Ausdrücke auf Drittsysteme zurückgegriffen werden, dadurch ist allerdings ein ständiges Wechseln zwischen Wazuh und dem Drittsystem erforderlich. Darüber hinaus werden Änderungen am Ruleset erst nach einem Neustart des Wazuh Servers wirksam, was zwar direkt über das Wazuh Dashboard möglich ist, bei einer Verwendung des Systems durch mehrere Personen jedoch die Definition von Wartungsfenstern für die Anpassung des Rulesets erforderlich macht, um sich nicht gegenseitig bei Analysen zu unterbrechen.

Optimierungspotenziale im Prototyp bestehen in der tieferen Integration von Shuffle mit Wazuh und Drittsystemen. So wäre in einer produktiven Umgebung die Anbindung eines Mailservers oder anderen Kommunikationssystems an Shuffle sinnvoll, um Mitarbeitende der IT im Rahmen von Shuffle-Workflows einerseits auf das Isolieren des Clients im erstellten Test Workflow sofort hinzuweisen, andererseits auch in anderen Workflows geeignete Benachrichtigungen auszulösen. Eine Erstellung weiterer spezifischer Workflows beispielsweise für die Alarmierung bei der Erkennung kritischer Schwachstellen durch den Wazuh Agent, oder auf dem Client erkannter Schadsoftware in Verbindung mit dem Auslösen einer Active Response zur Löschung der betroffenen Datei, ist ein weiteres Verbesserungspotenzial.

6.6 Übertrag auf Nachweiserbringung

Das Umsetzungsgradmodell der OH-SzA definiert, wie in Kapitel 3.2

beschrieben, die Stufe 4 als Zielwert zur Erfüllung der Anforderungen.

Für Stufe 4 gilt, dass ein kontinuierlicher Verbesserungsprozess etabliert ist sowie alle MUSS-Anforderungen und alle SOLLTE-Anforderungen erfüllt sind, wobei SOLLTE-Anforderungen mit geeigneter Begründung ausgeschlossen sein können. Stufe 5 erweitert dies um mit geeigneter Begründung ausschließbarer Umsetzung aller KANN-Anforderungen sowie die Umsetzung sinnvoller zusätzlicher Maßnahmen entsprechend der Risikoanalyse [4, S. 15].

In der theoretischen Umsetzung organisatorischer Anforderungen wird ein kontinuierlicher Verbesserungsprozess für die RECPLAST GmbH vorgesehen (siehe Tabelle 2). Der Prototyp in Verbindung mit der theoretischen Umsetzung der organisatorischen Anforderungen erfüllt zwar neben den MUSS- und SOLLTE-Anforderungen auch alle KANN-Anforderungen, allerdings sind keine Maßnahmen über die Anforderungen der OH-SzA hinaus vorgesehen. Somit entspricht der Umsetzungsgrad des Prototyps der Stufe 4 und erreicht somit den Zielwert, ab dem die gesetzlichen Anforderungen zu Systemen zur Angriffserkennung als erfüllt gelten. Mit der Etablierung zusätzlicher Maßnahmen ist mit der im Prototyp geschaffenen Basis auch eine Erreichung der Stufe 5 denkbar.

7 Vergleich mit kommerziellen Angriffserkennungssystemen

Mit Hilfe eines Interviews mit einem Vertreter kommerzieller Angriffserkennungssysteme wird in diesem Kapitel eine theoretische Einschätzung getroffen, unter welchen Voraussetzungen der Einsatz kommerzieller Lösungen gegenüber FOSS zu empfehlen ist, sowie wo die Vor- und Nachteile von FOSS-Umsetzungen gegenüber kommerziellen Lösungen liegen.

Das Interview fand am 14.08.2024 mit Splunk, einem Unternehmen von Cisco, in Form eines offenen Gesprächs statt.

Splunk bietet eine konsolidierte, skalierbare Plattform, die Daten aus beliebigen Quellen durchsuchbar macht. Darauf bauen im Bereich der Angriffserkennungssysteme unter anderen Splunk Enterprise Security als SIEM und Splunk SOAR als SOAR auf. Splunk Enterprise Security ermöglicht risikobasierte Alarmierung mittels 1300 mitgelieferter Erkennungen für Frameworks wie MITRE ATT&CK sowie die Integration von Threat Intelligence [109]. Splunk SOAR bietet nicht nur mehr als 350 fertige Integrationen von Drittanbieter-Tools, sondern liefert auch 100 vordefinierte Playbooks sowie ein integriertes Ticket-Management mit [110]. Splunk Enterprise Security und Splunk SOAR sind beide sowohl in der Cloud, on-premises und hybrid bereitstellbar. Neben Splunk Enterprise Security und Splunk SOAR umfasst das Security-Ökosystem weitere Lösungen wie den Splunk Universal Forwarder zur einfachen Sammlung und Weiterleitung von Daten, Splunk Attack Analyzer zur automatisierten Analyse von potenziell schadhaften Dateien und Splunk User Behavior Analytics zur Erkennung anormalen Benutzerverhaltens [111]. Das Marktforschungsunternehmen Gartner stuft Splunk in seiner SIEM-Marktanalyse für 2024 zum 10. Mal in Folge als „Leader“ ein. Unter den anderen Leadern befinden sich Microsoft, Securonix, Exabeam und IBM [112].

Zwischen FOSS-Lösungen und kommerziellen Angriffserkennungssysteme zeigen sich einige grundsätzliche Unterschiede, die vor allem auf die

Verfügbarkeit von Ressourcen für die Systempflege und Partnerunternehmen zurückzuführen sind.

Die Vorteile von FOSS liegen zwar offensichtlich in der Kostenfreiheit, was Lizenzen betrifft, allerdings ergeben sich tendenziell höhere Kosten im Betrieb. Dies liegt darin begründet, dass in einer Vollkostenbetrachtung von Angriffserkennungssystemen die Lizenzkosten nur einen Anteil der Gesamtkosten darstellen, die insbesondere durch Personalkosten, Betriebskosten und Entwicklungskosten der SzA getrieben werden. Speziell im Falle von FOSS werden zwar Lizenzkosten eliminiert, die Entwicklungskosten steigen jedoch durch höhere Aufwände in der Entwicklung eigener Integrationen mit Drittsystemen und oft weniger benutzerfreundlichen Konfiguration Splunk, persönliches Interview, siehe 0). Diese Aufwände und damit verbundene Kosten für internes oder externes Fachpersonal können die Lizenzkostenvorteile von FOSS schnell wieder ausgleichen.

Gegenüber kommerziellen SzA haben FOSS Lösungen tendenziell Nachteile in Umfang, Tiefe und Aktualität der Dokumentation. Anbieter kommerzieller Lösungen können aufgrund einer höheren Verfügbarkeit von Ressourcen einen größeren Fokus auf die Pflege der Dokumentation legen als kostenfreie Angebote, was vermutlich auch vor dem Hintergrund der Kundenbindung geschieht. Ein Kunde, der aufgrund mangelhafter Dokumentation der Lösung Mehraufwände und damit Kosten im Betrieb der Lösung hat, wird sich eher nach Alternativen umsehen, als Kunden, die bei Fragen und Problemen die Antwort schnell und einfach selbst finden können. FOSS Lösungen bieten hier allerdings den Vorteil, dass die Dokumentation öffentlich einsehbar sein muss, während manche Anbieter kommerzieller SzA ihre Dokumentation nur Kunden verfügbar machen. Dies erschwert die Bewertung der SzA mit nicht öffentlich verfügbarer Dokumentation auf Eignung für das Unternehmen, da vor einer Kaufentscheidung die Integrierbarkeit in die bestehende IT-Umgebung nicht mit detaillierten Informationen über die einzukaufende Lösung geprüft werden kann. Somit liegt ein Vorteil von FOSS im Prinzip der Offenheit, was nicht nur für den Quellcode und die Software selbst, sondern auch die Dokumentation gilt,

allerdings teilen sich kommerziellen SzA diesen Vorteil mit FOSS. Diese wiederum haben tendenziell aktuellere und umfangreichere Dokumentation als FOSS, da mehr Ressourcen für die Pflege der Dokumentation allokiert werden können Splunk, persönliches Interview, siehe 0).

FOSS kann als Konsequenz der Kostenfreiheit nicht direkt als SaaS-Lösung angeboten werden, da dies für den Entwickler mit Kosten behaftet ist. Zwar bieten Anbieter wie Shuffle und Wazuh SaaS-Deployments an, diese sind jedoch zwangsweise kostenpflichtig [76] und somit nicht mehr FOSS. Rein aus dem Prinzip der Kostenfreiheit bedingt können SaaS-Lösungen somit nicht als FOSS angeboten werden, wenn auch die Software unabhängig von der Bereitstellungs-Variante Open Source bleibt. Hier ist wichtig zu beachten, dass unabhängig davon, ob die Systeme lokal oder mittels SaaS bereitgestellt werden, Betriebskosten anfallen. Insofern wäre es wie oben erläutert ein Trugschluss anzunehmen, dass FOSS bei lokaler Bereitstellung kostenfrei sei.

Die Integrationen mit Drittanbieter-Systemen sind bei kommerziellen Anbietern von SzA tendenziell umfangreicher und stabiler, als dies bei FOSS der Fall ist. So bietet Splunk über 1800 Apps auf Splunkbase an, die neben zusätzlichen Funktionen innerhalb von Splunk auch fertige Integrationen mit Drittanbieter-Systemen wie beispielsweise Amazon Web Services oder OPNSense bieten [113]. Dem gegenüber stehen im Falle von Wazuh fünf dokumentierte Integrationen [114]. Die große Anzahl an Integrationen mit Drittanbieter-Systemen ist kommerziellen Anbietern von SzA dadurch möglich, dass mehr Ressourcen für die Entwicklung auf Seiten des Herstellers für die Entwicklung der Integrationen genutzt werden können. Auch steht großen Herstellern ein großes Partnernetzwerk zur Verfügung, das wie im Falle von Splunk Integrationen selbst erstellt und veröffentlicht. So sind auf Splunkbase beispielsweise Integrationen für Fortinet-Systeme verfügbar, die von Fortinet selbst entwickelt werden. Auch haben kommerzielle SzA-Anbieter aufgrund mehr verfügbarer Ressourcen mehr Möglichkeiten, was die Gestaltung der Integrationen betrifft. Im Falle von Splunk ist ein gutes Beispiel, dass eigens entwickelte und betriebene Konnektoren von Splunk angeboten werden, die API-

Anfragen von Kunden an Cloud-Provider bündeln und zentral absetzen, sodass die Kosten für die Nutzung der APIs für den einzelnen Kunden reduziert werden Splunk, persönliches Interview, siehe 0). Eine solche Lösung selbst zu entwickeln und für die Nutzer zu betreiben, würde bei FOSS auf Dauer nicht tragbare Kosten für die Entwickler verursachen.

Die Verfügbarkeit von Managed Security Service Providern ist bei FOSS gegenüber kommerziellen Lösungen eingeschränkt Splunk, persönliches Interview, siehe 0). Dies liegt vermutlich mit in den oben genannten Punkten begründet, dass die Dokumentation in kommerziellen Lösungen tendenziell aktueller und umfangreicher, die Bedienung benutzerfreundlicher und bedeutend mehr Integrationen mit Drittsystemen vorhanden sind. Die bessere Dokumentation beschleunigt die Lösung von Problemen, die besonders bei Servicebeeinträchtigungen gegenüber Kunden für den MSSP schnell zu Verletzungen von Servicevereinbarungen führen könnten. Insofern ist die Wahl einer Lösung mit aktuellerer und umfangreicherer Dokumentation eine Maßnahme zur Reduktion des Risikos künftiger Serviceeinschränkungen. Die benutzerfreundlichere Bedienung spart Zeit für MSSP, die für die Betreuung weiterer Kunden genutzt werden kann und somit unmittelbar Auswirkungen auf den möglichen Profit des Anbieters hat. Die höhere Verfügbarkeit von Integrationen mit Drittsystemen spart ebenso Zeit bei der Integration von Kundensystemen, da wahrscheinlich mehr bei Kunden potenziell eingesetzte Systeme bereits fertige Integrationen mit dem kommerziellen SzA haben, als dies bei FOSS der Fall wäre. Die Aufwände für die Integration von Kunden werden somit mittels standardisierter fertiger Integrationen reduziert.

Insgesamt bieten kommerzielle SzA tendenziell aufgrund mehr verfügbarer Ressourcen in der Entwicklung und Pflege der Systeme eine verlässlichere Dokumentation, eine höhere Verfügbarkeit von Dienstleistern und aufwandsärmere Integrationen mit anderen Systemen, als dies bei FOSS der Fall ist. Diese Vorteile können in einer Vollkostenbetrachtung die eigentlichen Mehrkosten durch Lizenzkosten wieder ausgleichen.

8 Empfehlungen für die Umsetzung in realen KMU

Auf Basis der gewonnenen Erkenntnisse in Kapitel 4 und 5 werden in diesem Kapitel Empfehlungen für reale KMU, welche die OH-SzA oder vergleichbare Anforderungen erfüllen wollen oder müssen, ausgesprochen. Dabei soll empfohlen werden, unter welchen Voraussetzungen FOSS oder kommerzielle Lösungen eingesetzt werden sollten und welche Herausforderungen bei der Verwendung von FOSS zu beachten sind.

Wie sich in Kapitel 6.6 gezeigt hat, sind die Anforderungen der OH-SzA mittels FOSS Lösungen erfüllbar. Allerdings sollte die reine Umsetzbarkeit der Anforderungen nicht das einzige Kriterium für die Entscheidung zwischen kommerziellen und FOSS Lösungen sowie die Art des Betriebs und der Nutzung der ausgewählten Lösung sein.

In der Einrichtung und Nutzung des Prototyps haben sich unzureichend beschriebene Sonderfälle als Hindernis speziell bei der Konfiguration von Shuffle Workflows ergeben. Wie in Kapitel 7 beschrieben können FOSS Lösungen dazu tendieren, aufgrund Ressourcenknappheit einen geringeren Fokus auf Dokumentation zu legen, als es kommerziellen Anbietern möglich ist. Aufgrund dessen sollten beim Einsatz von FOSS eingerichtete Konfigurationen vor produktivem Einsatz in einer Testumgebung umfangreich getestet werden, um unerwartetes Verhalten durch unvollständige oder fehlerhafte Dokumentation vor Produktivsetzung zu vermeiden. Dieses Vorgehen empfiehlt sich zwar unabhängig von der Verwendung von FOSS oder kommerziellen SzA, bei FOSS-Einsatz sollte jedoch besonders sorgfältig getestet werden.

Grundsätzlich sollte unabhängig vom Einsatz von FOSS oder kommerziellen SzA die Bereitstellungsvariante beziehungsweise die Verantwortung für den Betrieb der Lösung geeignet gewählt werden. Zur Optimierung interner Betriebsaufwände sollte die Verantwortung für den Betrieb auf einen SaaS-Anbieter ausgelagert werden, was sowohl für viele kommerziell als auch als FOSS angebotene Lösungen möglich ist. So muss das KMU keine zusätzlichen

internen Betriebsaufwände für die SzA mit leisten und kann sich in der IT auf jene Aufwände konzentrieren, die nicht an Dritte ausgelagert werden können. Sind ausreichend interne Ressourcen für einen vollständigen internen Betrieb der Lösungen vorhanden, sollte geprüft werden, ob eine interne Bereitstellung sinnvoll ist. Diese Entscheidung hängt maßgeblich vom Risikoappetit des Unternehmens ab, wobei die Bereitstellung über SaaS ein höheres Risiko darstellt, in Gegenüberstellung zum Bedarf nach interner Aufwandsminderung ab. Die Bereitstellung ist intern daher risikoärmer, da ein Ausfall der Internet- beziehungsweise Cloudkonnektivität nicht automatisch zu einem Ausfall der zentralen SzA-Komponenten führt. Zwar sollten bei SaaS-Bereitstellung dezentrale Komponenten wie auf Endpunkten installierte EDR-Agenten oder Protokollierungsserver weiterhin autark funktionieren, jedoch können sie ihre Daten nicht an die zentralen SzA zur Auswertung bereitstellen und sind somit nur eingeschränkt, falls überhaupt, benutzbar. Dieses Problem stellt sich bei interner Bereitstellung nicht in Verbindung mit dem Ausfall der Internetkonnektivität.

Nicht nur die Bereitstellung der SzA ist eine wichtige Entscheidung, sondern auch, ob die fachliche Nutzung der Lösung im Sinne des Betriebs eines SOC intern oder extern passieren soll. MSSP bieten externe SOC-Dienstleistungen an, die jedoch wie in Kapitel 7 genannt tendenziell auf kommerzielle SzA setzen. Die Entscheidung für FOSS-Lösungen schränkt den Markt entweder sehr stark ein oder führt zur vollständigen Nichtverfügbarkeit von Anbietern, was den Zwang zu einem internen SOC zur Folge hat. Ein internes SOC bedeutet offensichtlich Personalbedarf, da die OH-SzA die Auswertung von Protokolldaten durch speziell damit beauftragtem Personal als dessen überwiegende Aufgabe fordert [4, S. 12]. Die Umsetzung der in Kapitel 5.2 erarbeiteten organisatorischen Maßnahmen speziell im Bereich der Detektion und Reaktion erfordert offensichtlich hohen Aufwand, der entsprechend hohe interne Personalbedarfe zur Folge hat. Somit muss das Unternehmen entsprechendes Personal neu schulen oder am Arbeitsmarkt um entsprechende Fachkräfte mit anderen Unternehmen, darunter auch MSSP, konkurrieren. Mit der Beauftragung eines MSSP und damit Auslagerung der SOC-Tätigkeiten an einen spezialisierten Dienstleister können interne Aufwände auf ein Minimum reduziert werden, da

kein Fachpersonal für die Nutzung der SzA mehr erforderlich ist. Wie die Verwendung von SaaS-Lösungen ermöglicht auch dies die Reduktion interner Aufwände und eine Konzentration auf die IT-Arbeiten, die das Unternehmen selbst erbringen muss. Dabei ist zusätzlich zu berücksichtigen, dass selbst beim Aufbau eines internen SOC in den meisten Fällen externe Kosten in Form von Beratungsdienstleistungen anfallen, da der Aufbau eines internen SOC inklusive Prozesse, Schnittstellendefinitionen, Verfahrensanweisungen und Personals eine sehr umfangreiche Aufgabe ist, für die erfahrenes Personal erforderlich ist. Unternehmen sollten sich auf Basis der Bereitschaft und Ressourcenverfügbarkeit für internen Personal- und Wissensaufbau entscheiden, ob ein internes SOC sinnvoll ist, oder die Aufwände an einen MSSP abgegeben werden sollen. Eine flexiblere Vorgehensweise wäre der initiale Aufbau der SzA und deren Betrieb über die erste Zeit mit einem MSSP, in der das Unternehmen Erfahrungen in der Zusammenarbeit mit einem SOC und Angriffserkennung im Allgemeinen sammeln kann, bevor eine teilweise oder vollständige Internalisierung des SOC durchgeführt wird. Die teilweise Internalisierung bietet die Chance, den Großteil des Aufwands extern zu halten, dabei aber internes Wissen und Kompetenzen aufzubauen, um langfristig zu internalisieren oder zumindest interne Fachexperten zur Verfügung zu haben. Die Entscheidung ist unter Berücksichtigung der allgemeinen IT-Strategie des Unternehmens zu fällen: Soll gemäß Strategie mehr IT internalisiert werden, kann auch der Aufbau eines internen SOC langfristig sinnvoll sein, bei Externalisierung als Ziel ist ein MSSP die bessere Wahl. Bei der Entscheidung für ein internes SOC sollte auch eine Risikoanalyse dahingehend durchgeführt und berücksichtigt werden, inwiefern ein kontinuierlicher oder nur innerhalb der Rahmenarbeitszeiten laufender SOC-Betrieb erforderlich ist. Da nicht ausgeschlossen werden kann, dass Cyberangriffe außerhalb der Rahmenarbeitszeiten stattfinden, kann ein kontinuierlicher SOC-Betrieb abhängig vom Risikoappetit des Unternehmens notwendig sein. Ein kontinuierlicher Betrieb ist für ein internes SOC enorm ressourcenintensiv, da entsprechend viel Personal für einen Schichtbetrieb unter Berücksichtigung möglicher Personalausfälle durch Krankheit, Urlaub und sonstiges vorgehalten

werden muss. In diesem Fall ist es insbesondere für KMU eher sinnvoll, einen MSSP mit dem SOC-Betrieb zu beauftragen, der kontinuierlichen Betrieb anbietet.

Grundsätzlich sollte ein KMU, das SzA anhand der OH-SzA umsetzt, die dahinterstehende Motivation hinterfragen.

Werden die SzA aus Eigenmotivation zum Schutz der IT-Umgebung des Unternehmens eingeführt, sollte das Unternehmen zunächst eine umfangreiche Markterkundung durchführen, in der die Anforderungen der OH-SzA und eigene Anforderungen des Unternehmens gegen in Frage kommende FOSS und kommerzielle SzA geprüft werden. Die SzA, die den Anforderungen am meisten gerecht werden, sollten einer umfassenden Vollkostenbetrachtung unter Berücksichtigung der betrieblichen Aufwände unterzogen werden. Zusätzlich sollte das Unternehmen anhand der oben beschriebenen Vor- und Nachteile der jeweiligen Modelle entscheiden, ob ein internes SOC strategisch sinnvoll ist, oder die fachliche Kompetenz eines MSSP für den SOC-Betrieb herangezogen soll. Ist die Entscheidung bezüglich des Betriebsmodells auf einen MSSP gefallen, sollte das kommerzielle SzA eingesetzt werden, das nach einer Vollkostenbetrachtung dem Budgetrahmen und den Anforderungen des Unternehmens am ehesten gerecht wird. Auf die Wahl von FOSS-Lösungen vor Auswahl eines MSSP sollte verzichtet werden, um den Markt vor der Suche eines Anbieters nicht zu sehr einzuschränken oder keine Anbieter zur Verfügung zu haben. Bei Aufbau eines internen SOC ist die Wahl auf Basis der Vollkostenbetrachtung und Anforderungserfüllung der Systeme theoretisch frei zwischen kommerziellen und FOSS SzA entscheidbar, praktisch sollte jedoch reflektiert werden, ob für die Anfangsphase nicht doch ein MSSP für einen hybriden SOC-Betrieb beauftragt werden soll, um erste Erfahrungen im SOC-Betrieb zu sammeln, bevor vollständig internalisiert wird. In diesem Fall sollte ebenfalls auf ein kommerzielles SzA gesetzt werden, das von geeigneten MSSP-Anbietern unterstützt wird.

Werden die SzA allerdings auf Basis einer rechtlichen Verpflichtung eingerichtet und der Schutz der IT-Umgebung stellt für die Unternehmensführung keine

Priorität dar, können die Anforderungen der OH-SzA wie in dieser Arbeit demonstriert mittels FOSS SzA erfüllt werden. Um den nicht-technischen Anforderungen der OH-SzA gerecht zu werden, sind auch adäquate organisatorische Maßnahmen wie in Kapitel 5.2 zu treffen, das SOC kann jedoch auf einen internen Minimalbetrieb reduziert werden. Ist der Risikoappetit des Unternehmens ausreichend groß, worauf der Wunsch nach einer Minimalerfüllung der OH-SzA bereits hindeutet, kann ein innerhalb der Rahmenarbeitszeiten betriebenes SOC aus zwei Mitarbeitenden, deren Aufgabe der Betrieb und fachliche Nutzung der FOSS-SzA ist, erfüllt werden. Zwar empfiehlt sich dennoch eine Vollkostenbetrachtung zur Gegenüberstellung dieser Variante mit mehreren MSSP, jedoch sind die Chancen hoch, mittels FOSS-SzA und personeller Minimalbesetzung den Anforderungen dennoch gerecht zu werden und entsprechende Nachweise erbringen zu können. Offensichtlich stellt eine solche Lösung jedoch einen geringeren Sicherheitsgewinn für das Unternehmen dar, als es ein vollständiges internes SOC oder die Beauftragung eines professionellen MSSP wäre. Die Unternehmensführung sollte auf die entstehenden Risiken durch die Fachverantwortlichen hingewiesen werden, um eine informierte Entscheidung treffen zu können.

Insgesamt hängt also von mehreren Faktoren ab, welcher Weg in der Umsetzung von SzA für ein KMU geeignet ist, darunter Ressourcenverfügbarkeit, strategische Ausrichtung und Motivation des Unternehmens. Die Entscheidung bezüglich internen oder externen Betriebs der SzA und des SOC sowie Einsatz von FOSS oder kommerziellen SzA sollte in jedem Fall nur nach sorgfältiger Prüfung all dieser Faktoren getroffen werden.

9 Zusammenfassung und Fazit

In diesem abschließenden Kapitel werden die gewonnenen Erkenntnisse und Empfehlungen der Arbeit kurz zusammengefasst und ein Fazit bezüglich der Umsetzbarkeit der OH-SzA mittels FOSS gezogen.

Ziel dieser Arbeit war die Untersuchung, ob sich die aktuell gültigen Anforderungen der OH-SzA mittels FOSS umsetzen lassen, wobei der Fokus auf die technischen Anforderungen gelegt wurde. Hierzu wurden zunächst Grundlagen und relevante Begrifflichkeiten erläutert und die Anforderungen der OH-SzA analysiert.

Im Anschluss wurden die für die Erfüllung der OH-SzA erforderlichen Systemtypen anhand der Anforderungsanalyse identifiziert. Eine Auswahl pro Systemtyp verfügbarer FOSS Tools wurde anhand deren Dokumentation auf ihren theoretischen Erfüllungsgrad der OH-SzA geprüft.

Die vielversprechendste herausgearbeitete Systemkombination aus Wazuh, Shuffle und Suricata (in OPNSense) wurden in einem Prototyp implementiert, dessen Aufbau dem Netzplan der Recplast GmbH nachempfunden wurde. Innerhalb des Prototyps wurde ein exemplarischer Funktionsablauf demonstriert, in dem der Download einer EICAR-Testdatei durch Suricata erkannt, blockiert und protokolliert, in Wazuh alarmiert und der betroffene Client durch Shuffle an OPNSense vom restlichen Netzwerk getrennt wurde.

Ergänzend zum technischen Prototyp wurden in der Recplast GmbH umzusetzende organisatorische Maßnahmen theoretisch beschrieben.

Dieser Prototyp wurde anhand der SzA auf den Erfüllungsgrad der Anforderungen bewertet, indem die eingesetzten Systeme einzeln gegen die OH-SzA Anforderungen geprüft und die Teilbewertungen zusammengeführt wurden. In Verbindung mit den theoretisch beschriebenen organisatorischen Maßnahmen ergab sich die Erreichung des Umsetzungsgrads Stufe 4, was einer Erfüllung aktueller gesetzlicher Anforderungen an KRITIS-Betreiber entspricht.

Um einen Vergleich mit kommerziellen SzA herstellen und Unterschiede zu FOSS SzA herausarbeiten zu können, wurde ein Interview mit Splunk als Anbieter kommerzieller SzA geführt.

Auf Basis der Erkenntnisse des Prototyps und des Interviews wurden abschließend Empfehlungen für die Umsetzung von SzA entlang der OH-SzA in realen KMU ausgesprochen, wobei insbesondere das Erfordernis einer Vollkostenbetrachtung aller möglichen Lösungen, die Motivation des Unternehmens sowie die Entscheidung für internen oder externen SzA- und SOC-Betrieb den Ausschlag für die Wahl zwischen FOSS und kommerziellen SzA geben sollte. Eine Erfüllung der Anforderungen der OH-SzA ist mit der Verwendung von FOSS, wie im Prototyp demonstriert, möglich.

Das Thema IT-Sicherheit und im speziellen auch das Thema Angriffserkennung sind durch das IT-Sicherheitsgesetz 2.0 und das NIS2UmsuCG in jüngster Vergangenheit stärker in den Fokus der Gesetzgebung gerückt. Zu diesen Themen werden künftig vermutlich weiterhin verschärfte Anforderungen an Unternehmen gestellt, von denen zumindest in Teilen auch KMU betroffen sein können. Diese Anforderungen können nicht nur von Seiten der Gesetzgebung, sondern auch sektorspezifischen Regularien, Anforderungen an Lieferanten von größeren Unternehmen oder Cyberversicherungen gestellt werden und somit auch mehr und mehr Relevanz für KMU gewinnen.

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik, „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)“. Zugegriffen: 3. April 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig_2-0.html?nn=937202

[2] Bundesministerium der Justiz, „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)“. Zugegriffen: 3. April 2024. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/__8a.html

[3] Bundesministerium des Innern und für Heimat, „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“. 22. Juli 2024. Zugegriffen: 26. Juli 2024. [Online]. Verfügbar unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

[4] Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“. 26. September 2022. Zugegriffen: 3. April 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=15

[5] M. Pilgermann, S. Stein, T. Schrader, und S. Weber, „Angriffserkennung beim Betrieb von KRITIS gemäß IT-Sicherheitsgesetz 2.0: Auswirkungen am Beispiel von Krankenhaus-IT“, *Datenschutz Datensicherheit - DuD*, Bd. 45, Nr. 11, S. 733–737, Nov. 2021, doi: 10.1007/s11623-021-1525-z.

[6] M. Kohpeiß, „Verpflichtung zur intelligenten Angriffserkennung?“, *Datenschutz Datensicherheit - DuD*, Bd. 47, Nr. 4, S. 220–224, Apr. 2023, doi: 10.1007/s11623-023-1749-1.

[7] IBM, „Was ist ein Security Operations Center (SOC)?“ Zugegriffen: 5. August 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/security-operations-center

[8] Microsoft, „Was ist SIEM?“ Zugegriffen: 30. Mai 2024. [Online]. Verfügbar unter: https://www.microsoft.com/de-de/security/business/security-101/what-is-siem

[9] IBM, „Was ist ein Intrusion Detection System (IDS)?“ Zugegriffen: 30. Mai 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/intrusion-detection-system

[10] IBM, „Was ist Endpoint Detection and Response (EDR)?“ Zugegriffen: 5. August 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/edr

[11] IBM, „Was ist Extended Detection and Response (XDR)?“ Zugegriffen: 5. August 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/xdr

[12] IBM, „Was ist SOAR (Security, Orchestration, Automation and Response)?“ Zugegriffen: 5. August 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/security-orchestration-automation-response

[13] Bundesamt für Sicherheit in der Informationstechnik, „OPS.1.1.5 Protokollierung“. Zugegriffen: 21. Mai 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_5_Protokollierung_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

[14] International Organization for Standardization, „ISO/IEC 27001:2022“, ISO. Zugegriffen: 6. August 2024. [Online]. Verfügbar unter: https://www.iso.org/standard/27001

[15] International Organization for Standardization, „ISO/IEC 27002:2022“, ISO. Zugegriffen: 6.

August 2024. [Online]. Verfügbar unter: https://www.iso.org/standard/75652.html

[16] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz“, Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 6. August 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz.html?nn=128656

[17] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standards“, Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 6. August 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards.html?nn=128646

[18] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit“, Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 6. August 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/itgrundschutzKompendium.html?nn=128568

[19] National Institute of Standards and Technology, „The NIST Cybersecurity Framework 2.0“. National Institute of Standards and Technology, 26. Februar 2024. Zugegriffen: 6. August 2024. [Online]. Verfügbar unter: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[20] CrowdStrike, „Was ist Log-Management? Best Practices“. Zugegriffen: 30. Mai 2024. [Online]. Verfügbar unter: https://www.crowdstrike.de/cybersecurity-101/observability/log-management/

[21] Splunk, „Was ist SOAR?“, Splunk. Zugegriffen: 30. Mai 2024. [Online]. Verfügbar unter: https://www.splunk.com/de_de/data-insider/what-is-soar.html

[22] Elastic, „Logstash Reference [8.13]“, Logstash Introduction. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/introduction.html

[23] Elastic, „ELK Stack: Elasticsearch, Kibana, Beats und Logstash“, Elastic Stack. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/de/elastic-stack

[24] Elastic, „Winlogbeat Reference [8.13]“, Winlogbeat Overview. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html

[25] Elastic, „Filebeat Reference [8.13]“, Filebeat overview. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html

[26] GitHub, „elastic/logstash“. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://github.com/elastic/logstash

[27] GitHub, „elastic/beats“. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://github.com/elastic/beats?tab=readme-ov-file

[28] Elastic, „Elastic Stack-Abonnements“. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/de/subscriptions

[29] Elastic, „Beats: Daten-Shipper für Elasticsearch“, Leichtgewichtige Daten-Shipper. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://www.elastic.co/de/beats

[30] GitHub, „logstash/licenses/ELASTIC-LICENSE.txt“, GitHub. Zugegriffen: 31. Mai 2024. [Online]. Verfügbar unter: https://github.com/elastic/logstash/blob/8.13/licenses/ELASTIC-LICENSE.txt

[31] Graylog, „Graylog Open“, Free & Open LogManagement. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://graylog.org/products/source-available/

[32] Graylog, „Installing Graylog“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/downloading_and_installing_graylog/installing_graylog.html?tocpath=Downloading%20an

d%20Installing%20Graylog%7CInstalling%20Graylog%7C_____0

[33] Graylog, „Ingest Windows Event Logs“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/getting_in_log_data/ingest_windows_eventlog.html

[34] Graylog, „Ingest from Files“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/getting_in_log_data/ingest_from_files.html

[35] GitHub, „Graylog2/graylog2-server“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://github.com/Graylog2/graylog2-server

[36] Graylog, „Graylog Pricing“, Graylog. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://graylog.org/pricing/

[37] GitHub, „graylog2-server/LICENSE“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://github.com/Graylog2/graylog2-server/blob/master/LICENSE

[38] Graylog, „Graylog Documentation“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/home.htm

[39] Graylog, „Correlation Engine“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/interacting_with_your_log_data/correlation_engine.html?TocPath=Managing%20Events%7C_____2

[40] Graylog, „Graylog Security“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/what_more_can_graylog_do_for_me/graylog_security.html?tocpath=Graylog%20Security%7C_____0

[41] Fluentd Project, „Open Source Data Collector“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://www.fluentd.org/

[42] Fluentd Project, „What is Fluentd?“ Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://www.fluentd.org/architecture

[43] GitHub, „fluent/fluentd“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://github.com/fluent/fluentd

[44] Fluentd Project, „Enterprise Services“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://www.fluentd.org/enterprise_services

[45] GitHub, „fluentd/LICENSE“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://github.com/fluent/fluentd/blob/master/LICENSE

[46] Fluentd Project, „Introduction“. Zugegriffen: 1. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org

[47] Wazuh, „Wazuh - Open Source XDR. Open Source SIEM.“, Wazuh. Zugegriffen: 4. Juni 2024. [Online]. Verfügbar unter: https://wazuh.com/

[48] Wazuh, „Architecture - Getting started with Wazuh“. Zugegriffen: 4. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/getting-started/architecture.html

[49] GitHub, „wazuh/wazuh“. Zugegriffen: 4. Juni 2024. [Online]. Verfügbar unter: https://github.com/wazuh/wazuh

[50] GitHub, „wazuh/LICENSE“. Zugegriffen: 4. Juni 2024. [Online]. Verfügbar unter: https://github.com/wazuh/wazuh/blob/master/LICENSE

[51] Wazuh, „Wazuh documentation“. Zugegriffen: 4. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/index.html

[52] OpenSearch contributors, „OpenSearch“, OpenSearch. Zugegriffen: 10. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/

[53] OpenSearch contributors, „About OpenSearch“, OpenSearch. Zugegriffen: 10. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/about.html

[54] GitHub, „opensearch-project/OpenSearch“. Zugegriffen: 10. Juni 2024. [Online]. Verfügbar unter: https://github.com/opensearch-project/OpenSearch

[55] OpenSearch contributors, „OpenSearch Documentation“, OpenSearch Documentation. Zugegriffen: 10. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/about/

[56] Security Onion Solutions, LLC, „Security Onion Solutions“. Zugegriffen: 11. Juni 2024. [Online]. Verfügbar unter: https://securityonionsolutions.com/

[57] GitHub, „Security-Onion-Solutions/securityonion“. Zugegriffen: 11. Juni 2024. [Online]. Verfügbar unter: https://github.com/Security-Onion-Solutions/securityonion/commits/2.4/main/

[58] Security Onion Solutions, LLC, „License“. Zugegriffen: 11. Juni 2024. [Online]. Verfügbar unter: https://securityonionsolutions.com/license

[59] Security Onion Solutions, LLC, „Security Onion Documentation“. Zugegriffen: 11. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/index.html

[60] GitHub, „snort3/snort3“. Zugegriffen: 26. Juni 2024. [Online]. Verfügbar unter: https://github.com/snort3/snort3

[61] Cisco, „Rule Subscriptions“. Zugegriffen: 26. Juni 2024. [Online]. Verfügbar unter: https://www.snort.org/products

[62] Cisco, „Snort License“. Zugegriffen: 26. Juni 2024. [Online]. Verfügbar unter: https://www.snort.org/license

[63] The Open Information Security Foundation, „Home“, Suricata. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://suricata.io/

[64] The Open Information Security Foundation, „Features“, Suricata. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://suricata.io/features/

[65] GitHub, „OISF/suricata“. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://github.com/OISF/suricata

[66] The Open Information Security Foundation, „Training Courses“, Suricata. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://suricata.io/learn/public-training/

[67] The Open Information Security Foundation, „Free and Open Source“, Suricata. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://suricata.io/features/open-source/

[68] The Zeek Project, „The Zeek Network Security Monitor“, Zeek. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://zeek.org/

[69] *zeek/zeek*. (27. Juni 2024). C++. Zeek Network Monitoring Project. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://github.com/zeek/zeek

[70] „Zeek: FAQs“, Zeek. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://zeek.org/faq/

[71] n8n, „n8n.io - a powerful workflow automation tool“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://n8n.io/

[72] GitHub, „n8n-io/n8n“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://github.com/n8n-io/n8n

[73] n8n, „n8n pricing“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://n8n.io/pricing/

[74] GitHub, „n8n/LICENSE.md at master“, GitHub. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://github.com/n8n-io/n8n/blob/master/LICENSE.md

[75] n8n, „Welcome | n8n Docs“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/

[76] Shuffle, „The Open Source SOAR for all purposes“. Zugegriffen: 25. Juni 2024. [Online].

Verfügbar unter: https://shuffler.io

[77] GitHub, „Shuffle/Shuffle“. Zugegriffen: 25. Juni 2024. [Online]. Verfügbar unter: https://github.com/Shuffle/Shuffle

[78] GitHub, „Shuffle/LICENSE at main“. Zugegriffen: 25. Juni 2024. [Online]. Verfügbar unter: https://github.com/Shuffle/Shuffle/blob/main/LICENSE

[79] Shuffle, „Shuffle App for Wazuh API“. Zugegriffen: 27. Juni 2024. [Online]. Verfügbar unter: https://shuffler.io/apps/fb715a176a192687e95e9d162186c97f

[80] Wazuh, „Network IDS integration - Proof of Concept guide“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html

[81] Bundesamt für Sicherheit in der Informationstechnik, „Arbeitsbeispiel RECPLAST GmbH“. Zugegriffen: 2. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/Recplast.html?nn=128440

[82] Bundesamt für Sicherheit in der Informationstechnik, „Beschreibung des Beispielunternehmens RECPLAST GmbH“. 2020. Zugegriffen: 2. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/Beschreibung_Recplast.pdf?__blob=publicationFile&v=1

[83] Bundesamt für Sicherheit in der Informationstechnik, „Remote-Controlled Browsers System (ReCoBS)“, Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 2. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Buero/Remote-Controlled-Browser-System/remote-controlled-browser-system.html?nn=129058

[84] Bundesamt für Sicherheit in der Informationstechnik, „Strukturanalyse der RECPLAST GmbH“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A1_Strukturanalyse_RECPLAST_GmbH.xlsx?__blob=publicationFile&v=2

[85] Bundesamt für Sicherheit in der Informationstechnik, „Leitlinie zur Informationssicherheit“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A01_Sicherheitsleitlinie.pdf?__blob=publicationFile&v=2

[86] Bundesamt für Sicherheit in der Informationstechnik, „Definition der Schutzbedarfskategorien“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A21_Definition_Schutzbedarfskategorien.pdf?__blob=publicationFile&v=1

[87] Bundesamt für Sicherheit in der Informationstechnik, „Richtlinie zur internen ISMS-Auditierung“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A04_Richtlinie_internen_ISMS_Auditierung.pdf?__blob=publicationFile&v=1

[88] Bundesamt für Sicherheit in der Informationstechnik, „OPS.1.2.6 NTP-Zeitsynchronisation“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_2_6_NTP_Zeitsynchronisation_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

[89] Bundesamt für Sicherheit in der Informationstechnik, „Cyber-Sicherheitswarnungen“. Zugegriffen: 4. Juli 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Cyber-

Sicherheitswarnungen/cyber-sicherheitswarnungen.html?nn=129300

[90] Deciso B.V., „Welcome to OPNsense's documentation!" Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/index.html

[91] Deciso B.V., „Intrusion Prevention System". Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/manual/ips.html

[92] Deciso B.V., „Initial Installation & Configuration". Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/manual/install.html

[93] Wazuh, „Quickstart". Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/quickstart.html

[94] GitHub, „Shuffle/.github/install-guide.md", GitHub. Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://github.com/Shuffle/Shuffle/blob/main/.github/install-guide.md

[95] Deciso B.V., „Download". Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://opnsense.org/download/

[96] Deciso B.V., „Hardware sizing & setup". Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/manual/hardware.html

[97] Deciso B.V., „Network Time". Zugegriffen: 10. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/manual/ntpd.html

[98] Canonical, „Get Ubuntu Server", Ubuntu. Zugegriffen: 5. Juli 2024. [Online]. Verfügbar unter: https://ubuntu.com/download/server

[99] Docker Inc., „Install Docker Engine on Ubuntu", Docker Documentation. Zugegriffen: 12. Juli 2024. [Online]. Verfügbar unter: https://docs.docker.com/engine/install/ubuntu/

[100] Microsoft, „Windows 10 herunterladen". Zugegriffen: 12. Juli 2024. [Online]. Verfügbar unter: https://www.microsoft.com/de-de/software-download/windows10

[101] Wazuh, „Configuring syslog on the Wazuh server". Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/syslog.html

[102] Wazuh, „Event logging". Zugegriffen: 14. Juli 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/manager/event-logging.html

[103] GitHub, „rules/src/opnsense.test.rules at master". Zugegriffen: 13. Juli 2024. [Online]. Verfügbar unter: https://github.com/opnsense/rules/blob/master/src/opnsense.test.rules

[104] EICAR, „Download Anti Malware Testfile", EICAR. Zugegriffen: 13. Juli 2024. [Online]. Verfügbar unter: https://www.eicar.org/download-anti-malware-testfile/

[105] Wazuh und F. T. Jeremiah, „Integrating Wazuh with Shuffle", Wazuh. Zugegriffen: 13. Juli 2024. [Online]. Verfügbar unter: https://wazuh.com/blog/integrating-wazuh-with-shuffle/

[106] Wazuh und J. P. Saez, „Creating decoders and rules from scratch", Wazuh. Zugegriffen: 14. Juli 2024. [Online]. Verfügbar unter: https://wazuh.com/blog/creating-decoders-and-rules-from-scratch/

[107] Deciso B.V., „Use the API". Zugegriffen: 14. Juli 2024. [Online]. Verfügbar unter: https://docs.opnsense.org/development/how-tos/api.html

[108] Shuffle, „Workflows". Zugegriffen: 25. Juni 2024. [Online]. Verfügbar unter: https://shuffler.io/docs/workflows

[109] Splunk, „Splunk Enterprise Security", Splunk. Zugegriffen: 17. August 2024. [Online]. Verfügbar unter: https://www.splunk.com/de_de/products/enterprise-security.html

[110] Splunk, „Splunk SOAR", Splunk. Zugegriffen: 17. August 2024. [Online]. Verfügbar unter: https://www.splunk.com/de_de/products/splunk-security-orchestration-and-automation.html

[111] Splunk, „Splunk-Produkte", Splunk. Zugegriffen: 17. August 2024. [Online]. Verfügbar

unter: https://www.splunk.com/de_de/products.html

[112] Splunk, „Gartner Magic Quadrant für SIEM 2024“, Splunk. Zugegriffen: 17. August 2024. [Online]. Verfügbar unter: https://www.splunk.com/de_de/form/gartner-siem-magic-quadrant.html

[113] Splunk, „Splunkbase | Apps“. Zugegriffen: 20. August 2024. [Online]. Verfügbar unter: https://splunkbase.splunk.com/apps?page=1&filters=product%3Asplunk

[114] Wazuh, „Integration with third-party APIs - Wazuh server“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/manager/manual-integration.html

[115] Elastic, „Syslog input plugin“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-syslog.html

[116] Elastic, „Output plugins“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/output-plugins.html

[117] Elastic, „Mutate filter plugin“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/plugins-filters-mutate.html

[118] Elastic, „Date filter plugin“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/plugins-filters-date.html

[119] Elastic, „Persistent queues (PQ)“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/persistent-queues.html#configuring-persistent-queues

[120] Elastic, „Drop filter plugin“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/plugins-filters-drop.html

[121] Elastic, „Aggregate filter plugin“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/plugins-filters-aggregate.html

[122] Elastic, „Accessing event data and fields“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/logstash/current/event-dependent-configuration.html

[123] Graylog, „Graylog Inputs“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/getting_in_log_data/inputs.htm?tocpath=Getting%20in%20Logs%7CGraylog%20Inputs%7C_____0

[124] Graylog, „Syslog Inputs“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/current/getting_in_log_data/syslog_inputs.html?tocpath=Getting%20in%20Logs%7CGraylog%20Inputs%7C_____22

[125] Graylog, „Operations Output Framework“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/interacting_with_your_log_data/operations_output_framework.html?tocpath=Archiving%20and%20Outputs%7COutputs%7COperations%20Output%20Framework%7C_____0

[126] Graylog, „Functions by Category“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/making_sense_of_your_log_data/functions_by_category.html?tocpath=Sorting%20and%20Enriching%20Logs%7CProcessing%20Pipelines%7CFunctions%7C_____2

[127] Graylog, „Permissions Management“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/setting_up_graylog/permission_management.html?tocpath=Setting%20up%20Graylog%7CSecuring%20Graylog%7C_____7

[128] Graylog, „Widgets“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/interacting_with_your_log_data/widgets.html?tocpath=Aggregating%C2%A0Data%7CWidgets%7C_____0

[129] Graylog, „Writing Search Queries“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://go2docs.graylog.org/5-0/making_sense_of_your_log_data/writing_search_queries.html?tocpath=Searching%20Your%20Log%20Data%7C_____1

[130] Fluentd Project, „windows_eventlog“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/input/windows_eventlog

[131] Fluentd Project, „tail“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/input/tail

[132] Fluentd Project, „Input Plugins“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/input

[133] Fluentd Project, „Output Plugins“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/output

[134] Fluentd Project, „record_transformer“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/filter/record_transformer

[135] Fluentd Project, „parser“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/filter/parser

[136] Fluentd Project, „file“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/buffer/file

[137] Fluentd Project, „grep“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/filter/grep

[138] Fluentd Project, „List of All Plugins“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://www.fluentd.org/plugins/all

[139] Fluentd Project, „none“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://docs.fluentd.org/parser/none

[140] Wazuh, „Threat intelligence“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/compliance/nist/threat-intelligence.html

[141] Wazuh, „VirusTotal integration“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/virus-total-integration.html

[142] Wazuh, „Configuring log collection for different operating systems“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/configuration.html

[143] Wazuh, „Agentless monitoring“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/index.html

[144] Wazuh, „Custom decoders“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/ruleset/decoders/custom.html

[145] Wazuh, „Malware detection“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/index.html

[146] Wazuh, „File integrity monitoring“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html

[147] Wazuh, „Active response“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html

[148] Wazuh, „Log data analysis“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/log-data-analysis.html

[149] Wazuh, „Index life management“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/wazuh-indexer/index-life-management.html

[150] Wazuh, „RBAC Reference“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/api/rbac/reference.html

[151] Wazuh, „Wazuh archives“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/manager/wazuh-archives.html

[152] Wazuh, „Wazuh dashboard“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/index.html

[153] Wazuh, „Enhancing detection with MITRE ATT&CK framework“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html

[154] Wazuh, „How it works - File integrity monitoring“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/how-it-works.html

[155] Wazuh, „Creating custom FIM rules - File integrity monitoring“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/creating-custom-fim-rules.html

[156] Wazuh, „How it works - Log data collection“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/how-it-works.html

[157] Wazuh, „Checking connection with the Wazuh manager - Agent management“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/agent/agent-management/agent-connection.html

[158] Wazuh, „Update ruleset - Ruleset“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/ruleset/update.html

[159] Wazuh, „Wazuh server - Components“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/getting-started/components/wazuh-server.html

[160] Wazuh, „Alert threshold - Wazuh server“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/manager/alert-threshold.html

[161] Wazuh, „Ruleset - User manual“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/ruleset/index.html

[162] Wazuh, „How it works - Vulnerability detection“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/how-it-works.html

[163] Wazuh, „Rules classification - Ruleset“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html

[164] Wazuh, „Additional information - Active response“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/additional-information.html

[165] Wazuh, „active-response - Local configuration (ossec.conf)“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/active-response.html

[166] Wazuh, „Reference - Wazuh RESTful API“. Zugegriffen: 17. Juni 2024. [Online]. Verfügbar unter: https://documentation.wazuh.com/current/user-manual/api/reference.html

[167] OpenSearch contributors, „Working with detectors“, OpenSearch Documentation.

Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/usage/detectors/

[168] OpenSearch contributors, „About Security Analytics“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/

[169] OpenSearch contributors, „The Overview page“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/usage/overview/

[170] OpenSearch contributors, „Creating detectors“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/sec-analytics-config/detectors-config/

[171] OpenSearch contributors, „Notifications“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/observing-your-data/notifications/index/

[172] OpenSearch contributors, „Creating correlation rules“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/sec-analytics-config/correlation-config/

[173] OpenSearch contributors, „Analyzing data“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/dashboards/discover/index-discover/

[174] OpenSearch contributors, „Working with detection rules“, OpenSearch Documentation. Zugegriffen: 18. Juni 2024. [Online]. Verfügbar unter: https://opensearch.org/docs/latest/security-analytics/usage/rules/

[175] Security Onion Solutions, LLC, „Third Party Integrations“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/third-party-integrations.html#supported-integrations

[176] Security Onion Solutions, LLC, „Ingest“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/ingest.html

[177] Security Onion Solutions, LLC, „Suricata“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/suricata.html#suricata

[178] Security Onion Solutions, LLC, „Strelka“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/strelka.html

[179] Security Onion Solutions, LLC, „Elasticsearch“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/elasticsearch.html#parsing

[180] Elasticsearch B. V., „Gsub processor“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/elasticsearch/reference/current/gsub-processor.html

[181] Security Onion Solutions, LLC, „Elastic Agent“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/elastic-agent.html

[182] Security Onion Solutions, LLC, „Network Visibility“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/network.html

[183] Elasticsearch B. V., „Date processor“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/elasticsearch/reference/current/date-processor.html

[184] Elasticsearch B. V., „Ingest processor reference“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/elasticsearch/reference/current/processors.html

[185] Security Onion Solutions, LLC, „ElastAlert 2“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/elastalert.html

[186] Security Onion Solutions, LLC, „Dashboards“. Zugegriffen: 23. Juni 2024. [Online].

Verfügbar unter: https://docs.securityonion.net/en/2.4/dashboards.html

[187] Security Onion Solutions, LLC, „Hunt“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/hunt.html

[188] Elasticsearch B. V., „_source field“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-source-field.html

[189] Security Onion Solutions, LLC, „ATT&CK Navigator“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/attack-navigator.html

[190] Security Onion Solutions, LLC, „Alerts“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/alerts.html

[191] Security Onion Solutions, LLC, „Sigma“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/sigma.html

[192] Security Onion Solutions, LLC, „Rules“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/rules.html

[193] Security Onion Solutions, LLC, „Cases“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.securityonion.net/en/2.4/cases.html

[194] n8n, „Best cybersecurity integrations“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://n8n.io/integrations/categories/cybersecurity/

[195] n8n, „Integrations“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/integrations/

[196] n8n, „Creating Nodes“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/integrations/creating-nodes/overview/

[197] n8n, „Stop And Error“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/integrations/builtin/core-nodes/n8n-nodes-base.stopanderror/

[198] n8n, „If“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/integrations/builtin/core-nodes/n8n-nodes-base.if/

[199] n8n, „Create a workflow“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/workflows/create/

[200] n8n, „Manual trigger“. Zugegriffen: 23. Juni 2024. [Online]. Verfügbar unter: https://docs.n8n.io/integrations/builtin/core-nodes/n8n-nodes-base.manualworkflowtrigger/

Bilderverzeichnis

Tabellenverzeichnis

Anlagenverzeichnis und Anlagen

Anlage 1 Übergreifende Anforderungen

Begründung					
	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Angriffserkennung nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Angriffserkennung nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Angriffserkennung nicht zu erfüllen.	Die SzA müssen eine Möglichkeit bieten, ihre Signaturen zu aktualisieren. Signaturen können z.B. Virensignaturen, bekannt schadhafte IP-Adressen, URLs und sonstiges sein.	
Anwendbar?	Nein	Nein	Nein	Ja	
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden MÜSSEN.	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden MÜSSEN.	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass alle zur durchgängig effektiven Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden MUSS.	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN.	
Modalverb	MUSS	MUSS	MUSS	MUSS	
Seite	8	8	8	8	
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA	
Nummer	1	2	3	4	

Begründung	Diese Anforderung betrifft die relevanten Systeme (die Protokolldatenquellen) und ist durch die Systeme zur Angriffserkennung nicht zu erfüllen.
Anwendbar?	Nein
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche […], dass alle relevanten Systeme so konfiguriert sein MÜSSEN, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	5

Anlage 2 Anforderungen zur Protokollierung

Begründung	Die SzA müssen eine Erhebung, Speicherung und Bereitstellung zur Auswertung der Protokolldaten ermöglichen, um SRE erkennen und bewerten zu können.	Die SzA können anderweitig für eine Protokollierung sorgen, sodass nicht jedes einzelne relevante System die Protokolldaten selbst aufzeichnen muss. Dies kann z.B. durch NIDS realisiert werden, die zur Angriffserkennung ausreichende Protokollierungsdaten über die relevanten Systeme generieren, ohne dass die systemeigene Protokollierung verwendet wird.	Während der legale Umgang mit den Protokolldaten organisatorisch geprüft werden muss, müssen die SzA zumindest eine Anonymisierung bzw. Pseudonymisierung der Daten ermöglichen.
Anwendbar?	Ja	Ja	Ja
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	Da die Protokollierung teilweise datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.
Modalverb	MUSS	KANN	MUSS
Seite	9	9	9
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	8	9	11

Begründung	Die SzA müssen auch ohne auskömmliche Protokolldaten in der Lage sein, Detektion und Reaktion im Rahmen eines gewissen Umfangs zu leisten. Mögliche Systemtypen hierfür wären z.B. NIDS oder HIDS. Im allgemeinen wird hier keine Risikoanalyse betrachtet, sondern die Anforderungen der Bereiche Detektion und Reaktion, die nicht explizit auf Protokolldaten Bezug nehmen.	Diese Anforderung ist analog zu Anforderung Nummer 9 - siehe oben.	Diese Anforderung kann mangels Konfigurationsmöglichkeiten auf manchen protokollierenden Systemen in vielen Fällen vermutlich nicht realisiert werden. Die SzA müssen daher eine Möglichkeit bieten, das Datums- und Zeitformat aller Protokolldaten zu vereinheitlichen bzw. zu normalisieren.
Anwendbar?	Ja	Ja	Ja
Anforderung	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.
Modalverb	SOLL	MUSS	MUSS
Seite	9	5	5
Quelle	OH-SzA	OPS.1.1.5	OPS.1.1.5
Nummer	13	35	37

Begründung	Die SzA, die Protokolldaten speichern, müssen ein unkontrolliertes Löschen oder Verändern der Daten technisch verhindern. Dazu können z.B. granulare Berechtigungssteuerungen oder kryptographische Sicherungsmechanismen eingesetzt werden.	Die SzA müssen eine Weiterleitung der Protokolldaten sowie deren Speicherung an zentralen Stellen ermöglichen. Im Sinne der Speicherung an zentralen Stellen muss also auch eine Aggregation von Protokolldaten verschiedener Quellen ermöglicht werden.	Die Filterung, Normalisierung, Aggregation und Korrelation der Protokolldaten muss durch die SzA ermöglicht werden.	Die bearbeiteten Protokolldaten müssen für die Auswertung, speziell durch die Systeme des Bereichs Detektion, verfügbar gemacht werden.
Anwendbar?	Ja	Ja	Ja	Ja
Anforderung	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	5	10	10	10
Quelle	OPS.1.1.5	OH-SzA	OH-SzA	OH-SzA
Nummer	42	43	47	48

Begründung	Die unbearbeiteten, also ungefilterten und nicht normalisierten Protokolldaten, sollten durch die SzA zusätzlich zu den bearbeiteten gespeichert werden können.
Anwendbar?	Ja
Anforderung	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	KANN
Seite	10
Quelle	OH-SzA
Nummer	49

Anlage 3 Anforderungen zur Detektion

Begründung	Die Systeme zur Angriffserkennung müssen eine Bestimmung der abgedeckten Bedrohungslandschaft ermöglichen.	Die Systeme zur Angriffserkennung müssen eine Bestimmung der abgedeckten Bedrohungslandschaft ermöglichen, die Bestimmung der Bedrohungslandschaft selbst ist jedoch prozessual/organisatorisch zu leisten.	Die Systeme zur Angriffserkennung müssen eine standardisierte Methode für die Bestimmung der Bedrohungslandschaft einsetzen.	Die Betrachtung der Detektionsmechanismen kann organisatorisch/prozessual separat für die IT- und OT-Umgebung erfolgen, die SzA müssen
Anwendbar?	Ja	Nein	Ja	Nein
Anforderung	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.	Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden.	Zur Bestimmung der Abdeckung KANN es (und empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS).	In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.
Modalverb	MUSS	MUSS	KANN	KANN
Seite	11	11	11	11
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	55	56	57	58

Begründung	Die Anforderungen von DER.1 werden im Folgenden einzeln als MUSS-Anforderung betrachtet.	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 Detektion von sicherheitsrelevanten Ereignissen [...] erfüllt werden.	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen erstellt werden.	In der spezifischen Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie die Detektion von sicherheitsrelevanten Ereignissen geplant, aufgebaut und sicher betrieben werden kann.	Die spezifische Sicherheitsrichtlinie MUSS allen im Bereich Detektion zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	11	4	4	4
Quelle	OH-SzA	DER.1	DER.1	DER.1
Nummer	59	60	61	62

Begründung	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.	Eine Sicherheitsrichtlinie für die Detektion macht Vorgaben für den Einsatz von Systemen zur Detektion und kann daher nicht durch diese erstellt werden.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Falls die spezifische Sicherheitsrichtlinie verändert wird oder von den Anforderungen abgewichen wird, dann MUSS dies mit dem oder der verantwortlichen ISB abgestimmt und dokumentiert werden.	Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist.	Die Ergebnisse der Überprüfung MÜSSEN sinnvoll dokumentiert werden.	Wenn Protokollierungsdaten ausgewertet werden, dann MÜSSEN dabei die Bestimmungen aus den aktuellen Gesetzen zum Bundes- und Landesdatenschutz eingehalten werden.	Wenn Detektionssysteme eingesetzt werden, dann MÜSSEN die Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitenden-vertretungen gewahrt werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.1	DER.1	DER.1	DER.1	DER.1
Nummer	63	64	65	66	67

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden, z. B. das Telemediengesetz (TMG), das Betriebsverfassungsgesetz und das Telekommunikationsgesetz.	Für sicherheitsrelevante Ereignisse MÜSSEN geeignete Melde- und Alarmierungswege festgelegt und dokumentiert werden.	Es MUSS bestimmt werden, welche Stellen wann zu informieren sind.	Es MUSS aufgeführt sein, wie die jeweiligen Personen erreicht werden können.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4
Quelle	DER.1	DER.1	DER.1	DER.1
Nummer	68	69	70	71

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Je nach Dringlichkeit MUSS ein sicherheitsrelevantes Ereignis über verschiedene Kommunikationswege gemeldet werden.	Alle Personen, die für die Meldung bzw. Alarmierung relevant sind, über MÜSSEN über ihre Aufgaben informiert sein.	Alle Schritte des Melde- und Alarmierungs-prozesses MÜSSEN ausführlich beschrieben sein.	Die eingerichteten Melde- und Alarmierungswege SOLLTEN regelmäßig geprüft, erprobt und aktualisiert werden, falls erforderlich.	Alle Benutzenden MÜSSEN dahingehend sensibilisiert werden, dass sie Ereignismeldungen ihrer Clients nicht einfach ignorieren oder schließen.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.1	DER.1	DER.1	DER.1	DER.1
Nummer	72	73	74	75	76

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist nicht durch die dedizierten Systeme zur Detektion, sondern bereits im Bestand eingesetzte Systeme zu erfüllen.
Anwendbar?	Nein	Nein	Nein
Anforderung	Sie MÜSSEN die Meldungen entsprechend der Alarmierungswege an das verantwortliche Incident Management weitergeben (siehe DER.2.1 Behandlung von Sicherheitsvorfällen).	Alle Mitarbeitenden MÜSSEN einen von ihnen erkannten Sicherheitsvorfall unverzüglich dem Incident Management melden.	Falls eingesetzte IT-Systeme oder Anwendungen über Funktionen verfügen, mit denen sich sicherheitsrelevante Ereignisse detektieren lassen, dann MÜSSEN diese aktiviert und benutzt werden.
Modalverb	MUSS	MUSS	MUSS
Seite	4	4	5
Quelle	DER.1	DER.1	DER.1
Nummer	77	78	79

Begründung	Diese Anforderung lässt Interpretationsspielraum dahingehend, was mit den "Meldungen der betroffenen IT-Systeme" gemeint ist. Insofern damit die Meldungen im System zur Detektion bezüglich der vom sicherheitsrelevanten Vorfall betroffenen IT-Systeme gemeint sind, muss das System zur Detektion diese Meldungen auswertbar bereitstellen. Sind damit die durch die betroffenen IT-Systeme produzierten Meldungen im Sinne von Protokolldaten gemeint, muss die Auswertung der Protokolldaten zum bereits durch das System zur Detektion gemeldeten Vorfall organisatorisch/prozessual erfolgen. Hier wird diese Anforderung so interpretiert, dass die SzA die Meldungen zu von ihnen detektierten sicherheitsrelevanten Ereignissen auswertbar bereitstellen müssen.	Durch Anforderung Nummer 48 wird eine Bereitstellung aller gesammelten Protokolldaten bzw. protokollierter Ereignisse für die Auswertung bereits gefordert. Die tatsächliche Prüfung der Protokolldaten anderer IT-Systeme muss prozessual geleistet werden, nicht durch das System zur Detektion selbst.
Anwendbar?	Ja	Nein
Anforderung	Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden.	Zusätzlich MÜSSEN die protokollierten Ereignisse anderer IT-Systeme überprüft werden.
Modalverb	MUSS	MUSS
Seite	5	5
Quelle	DER.1	DER.1
Nummer	80	81

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Wird Anforderung Nummer 93 verschärft dahingehend, dass Schadcodedetektionssysteme eingesetzt werden MÜSSEN. Die Prüfung ist damit hinfällig.	Erweitert die Anforderung Nummer 93 geforderten Schadcodedetektion dass ein zentraler Zugriff Meldungen und Protokolle ermöglichen muss.	Erweitert die in Anforderung Nummer 93 geforderten Schadcodedetektionssysteme darum, dass sie sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Ja	Ja	Nein
Anforderung	Auch SOLLTEN die gesammelten Meldungen in verbindlich festgelegten Zeiträumen stichpunktartig kontrolliert werden.	Es MUSS geprüft werden, ob zusätzliche Schadcodescanner auf zentralen IT-Systemen installiert werden sollen.	Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten.	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Die Zuständigen MÜSSEN die Meldungen auswerten und untersuchen.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	5	5	5	5	5
Quelle	DER.1	DER.1	DER.1	DER.1	DER.1
Nummer	82	83	84	85	86

Begründung	Die kontinuierliche Überwachung und Auswertung der Protokolldaten muss durch die Systeme zur Detektion ermöglicht oder selbst geleistet werden. Diese Anforderung doppelt sich mit Anforderung Nummer 111 - siehe dort für weitere Erläuterungen.	Die Auswertung der Protokolldaten kann von den Systemen zur Detektion automatisiert geleistet werden, es muss dabei bei erkannten relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen erfolgen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Ja	Ja	Nein	Nein
Anforderung	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.	Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen.	Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.
Modalverb	MUSS	KANN	MUSS	MUSS
Seite	11	11	11	11
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	87	88	89	90

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Die Systeme zur Detektion müssen zentral verwaltbare Schadcodedetektionssysteme umfassen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Ja	Nein
Anforderung	Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, MÜSSEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.	Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.	Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden.	Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	11	11	11	11
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	91	92	93	94

Begründung	Die Systeme zur Detektion müssen NIDS umfassen.	Anforderung Nummer 37 fordert ein einheitliches Format der Zeitstempel bereits im Bereich der Protokollierung. Die zeitliche Synchronisierung der Protokolldaten selbst kann durch die Systeme zur Detektion allerdings nicht geleistet werden, da nach Eintreffen der Daten eine eventuelle zeitliche Verschiebung der Zeitstempel nicht erkannt werden kann. Daher müssen bereits die Protokolldatenquellen zeitlich synchron sein, idealerweise durch Nutzung einer gemeinsamen Zeitquelle.	Die Kontrolle der Ereignismeldungen auf Auffälligkeiten muss durch die Systeme zur Detektion ermöglicht werden, oder automatisiert stattfinden.
Anwendbar?	Ja	Nein	Ja
Anforderung	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden.	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.
Modalverb	MUSS	SOLL	MUSS
Seite	11	11	11
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	95	96	97

Begründung	Es muss eine Möglichkeit durch die Systeme zur Detektion bereitgestellt werden, Signaturen zu aktualisieren. Signaturen in Angriffserkennungssystemen werden hier interpretiert als Schadcodesignaturen für Schadcodedetektionssysteme, aber auch sogenannte Indicators of Compromise (IoC), die in Form von IP-Adressen, URLs, Datei-Hashes oder ähnlichem Indikatoren für einen möglichen Angriff darstellen, da sie in der Vergangenheit im Zusammenhang mit Cyberangriffen aufgetreten sind.	Die Formulierung "Erkenntnisse über sicherheitsrelevante Ereignisse" ist schwer zu interpretieren und wird hier verstanden als IoC (siehe Anforderung Nummer 98), da IoC Erkenntnisse über sicherheitsrelevante Ereignisse in anderen Informationsverbünden darstellen, die im eigenen Informationsverbund geprüft werden können. Die Systeme zur Detektion müssen eine Integrationsmöglichkeit von IoC aus externen Quellen bieten.
Anwendbar?	Ja	Ja
Anforderung	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.
Modalverb	MUSS	MUSS
Seite	11	12
Quelle	OH-SzA	OH-SzA
Nummer	98	99

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, MUSS sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden.	Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden.	Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind.	Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	100	101	102	103

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme nicht zur Detektion zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Die Systeme zur Detektion müssen eine solche zentrale Komponente bereitstellen.
Anwendbar?	Nein	Nein	Nein	Nein	Ja
Anforderung	Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten.	Die Auswertung der Protokoll- und Protokollierungsdaten SOLLTE bei diesen höher priorisiert sein, als ihre übrigen Aufgaben. Daher empfiehlt es sich, dass dies ihre überwiegende Aufgabe ist.	Dieses Personal SOLLTE spezialisierte und weiterführende Schulungen zu Qualifikationen erhalten.	Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.
Modalverb	MUSS	SOLL	SOLL	MUSS	MUSS
Seite	12	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	104	105	106	107	108

Begründung	Die Systeme zur Detektion müssen solche zentralen automatisierten Analysen durchführen.	Die Systeme zur Detektion müssen eine Protokollverwaltung umfassen und die Auswertung aller eingelieferten Protokolldaten ermöglichen.	Eine kontinuierliche Auswertung ohne weitere Einschränkung bedeutet, dass eine solche Auswertung auch nachts oder außerhalb der regulären Arbeitszeiten des Unternehmens stattfinden muss. Daher müssen die Systeme zur Detektion eine automatisierte Auswertung der Protokolldaten vornehmen, wenn nicht genügend personelle Ressourcen für eine manuelle kontinuierliche Auswertung bereitstehen. Diese Anforderung doppelt sich mit Anforderung Nummer 87, die ebenfalls eine kontinuierliche Auswertung aller Protokolldaten fordert.
Anwendbar?	Ja	Ja	Ja
Anforderung	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	Die Daten MÜSSEN kontinuierlich ausgewertet werden.
Modalverb	MUSS	MUSS	MUSS
Seite	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	109	110	111

Begründung	Die Systeme zur Detektion müssen einerseits auf definierbare Schwellwerte prüfen können, andererseits im Falle einer Überschreitung automatisch alarmieren.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Die Systeme zur Detektion müssen eine Anpassung der Analyseparameter ermöglichen.	Die Systeme zur Detektion müssen zusätzlich zur kontinuierlichen Auswertung der eingelieferten Protokolldaten (siehe Anforderungen Nummern 110 und 111) eine erneute Prüfung bereits überprüfter Protokolldaten automatisch durchführen können.
Anwendbar?	Ja	Nein	Ja	Ja
Anforderung	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.	Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird.	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	112	113	114	115

Begründung	Die Formulierung "Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten" ist schwer verständlich. IoC (siehe Anforderung Nummer 98) können als Angriffsmuster für technische Vulnerabilitäten verstanden werden, da sie Muster vergangener Angriffe auf technische Schwachstellen darstellen. Ein Beispiel ist hier der Hash einer schadhaft präparierten Word-Datei, die versucht, technische Schwachstellen in Microsoft Office auszunutzen, um schädliche Aktivitäten auf dem Wirtssystem auszuführen. Unter dieser Interpretation müssen die Systeme zur Detektion nicht nur eine Einbindung von externen Informationsquellen ermöglichen (siehe Anforderung Nummer 99), sondern dies auch fortlaufend ermöglichen und idealerweise selbst erledigen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Ja	Nein
Anforderung	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	Dazu MÜSSEN fortlaufend Meldungen der Hersteller (Hard- und Software), von Behörden, den Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen.
Modalverb	MUSS	MUSS
Seite	12	12
Quelle	OH-SzA	OH-SzA
Nummer	116	117

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Die manuelle Überprüfung und Bewertung von SRE muss durch die Systeme zur Detektion ermöglicht werden. Gleichzeitig sollten sie eine Möglichkeit zur automatisierten Qualifizierung bieten. In Verbindung mit Anforderung 112 wird eine automatisierte Qualifizierung so verstanden, dass die Systeme automatisiert ein Auslösen der Reaktion ermöglichen sollen.
Anwendbar?	Nein	Nein	Nein	Ja
Anforderung	Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining).	Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind.	Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.
Modalverb	SOLL	SOLL	SOLL	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	118	119	120	121

Begründung	Diese Anforderung ist organisatorischer Art, da bei manueller Prüfung der SRE auch manuell sichergestellt werden muss, dass der Prozess der Reaktion nur bei qualifizierten SRE ausgelöst wird. Sollten Systeme zur Detektion automatisch qualifizieren, sollten sie auch automatisch den Prozess der Reaktion auslösen - dies wird allerdings bereits in Anforderung Nummer 122 abgedeckt.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Detektion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen.	Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden.	Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.
Modalverb	SOLL	SOLL	MUSS	MUSS
Seite	12	12 f.	13	13
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	122	123	124	125

Anlage 4 Anforderungen zur Reaktion

Begründung	Die Anforderungen von DER.2.1 werden im Folgenden einzeln betrachtet.	Die Anforderungen von DER.2.1 werden im Folgenden einzeln betrachtet.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 Behandlung von Sicherheitsvorfällen erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.	Es SOLLTEN zudem die Standardanforderungen aus DER.2.1 Behandlung von Sicherheitsvorfällen umgesetzt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.	In einer Institution MUSS klar definiert sein, was ein Sicherheitsvorfall ist.	Ein Sicherheitsvorfall MUSS so weit wie möglich von Störungen im Tagesbetrieb abgegrenzt sein.
Modalverb	MUSS	SOLL	MUSS	MUSS
Seite	14	14	3	3
Quelle	OH-SzA	OH-SzA	DER.2.1	DER.2.1
Nummer	126	127	128	129

Begründung	Diese Anforderung ist organisatorischer Art und durch die Art und Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Art und Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Art und Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Art und Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Alle an der Behandlung von Sicherheitsvorfällen beteiligten Mitarbeitenden MÜSSEN die Definition eines Sicherheitsvorfalls kennen.	Die Definition und die Eintrittsschwellen eines solchen Vorfalls SOLLTEN sich nach dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Systeme bzw. Anwendungen richten.	Eine Richtlinie zur Behandlung von Sicherheitsvorfällen MUSS erstellt werden.	Darin MÜSSEN Zweck und Ziel der Richtlinie definiert sowie alle Aspekte der Behandlung von Sicherheitsvorfällen geregelt werden.	So MÜSSEN Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen beschrieben sein.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	3	3	4	4	4
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	130	131	132	133	134

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Zusätzlich MUSS es für alle Mitarbeitenden zielgruppenorientierte und praktisch anwendbare Handlungsanweisungen geben.	Weiterhin SOLLTEN die Schnittstellen zu anderen Managementbereichen berücksichtigt werden, z. B. zum Notfallmanagement.	Die Richtlinie MUSS allen Mitarbeitenden bekannt sein.	Sie MUSS mit dem IT-Betrieb abgestimmt und durch die Institutionsleitung verabschiedet sein.	Die Richtlinie MUSS regelmäßig geprüft und aktualisiert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	135	136	137	138	139

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Es MUSS geregelt werden, wer bei Sicherheitsvorfällen wofür verantwortlich ist.	Für alle Mitarbeitenden MÜSSEN die Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt werden.	Insbesondere Mitarbeitende, die Sicherheitsvorfälle bearbeiten sollen, MÜSSEN über ihre Aufgaben und Kompetenzen unterrichtet werden.	Dabei MUSS auch geregelt sein, wer die mögliche Entscheidung für eine forensische Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll.	Die Ansprechpartner oder Ansprechpartnerinnen für alle Arten von Sicherheitsvorfällen MÜSSEN den Mitarbeitenden bekannt sein.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	140	141	142	143	144

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Kontaktinformationen MÜSSEN immer aktuell und leicht zugänglich sein.	Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden.	Dabei MUSS geprüft werden, ob der oder die Datenschutzbeauftragte, der Betriebs- und Personalrat sowie Mitarbeitende aus der Rechtsabteilung einbezogen werden müssen.	Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden.	Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	145	146	147	148	149

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Damit ein Sicherheitsvorfall erfolgreich behoben werden kann, MÜSSEN die Zuständigen zunächst das Problem eingrenzen und die Ursache finden.	Danach MÜSSEN die erforderlichen Maßnahmen auswählt werden, um das Problem zu beheben.	Die Leitung des IT-Betriebs MUSS eine Freigabe erteilen, bevor die Maßnahmen umgesetzt werden.	Anschließend MUSS die Ursache beseitigt und ein sicherer Zustand hergestellt werden.	Eine aktuelle Liste von internen und externen Sicherheitsfachleuten MUSS vorhanden sein, die bei Sicherheitsvorfällen für Fragen aus den erforderlichen Themenbereichen hinzugezogen werden können.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	4
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	150	151	152	153	154

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Es MÜSSEN sichere Kommunikations-verfahren mit diesen internen und externen Stellen etabliert werden.	Nach einem Sicherheitsvorfall MÜSSEN die betroffenen Komponenten vom Netz genommen werden.	Zudem MÜSSEN alle erforderlichen Daten gesichert werden, Aufschluss über die Art und Ursache des Problems geben könnten.	Auf allen betroffenen Komponenten MÜSSEN das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden.	Die Originaldaten MÜSSEN von schreibgeschützten Datenträgern wieder eingespielt werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	4	4	4	4	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	155	156	157	158	159

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Dabei MÜSSEN alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden.	Wenn Daten aus Datensicherungen wieder eingespielt werden, MUSS sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren.	Nach einem Angriff MÜSSEN alle Zugangsdaten auf den betroffenen Komponenten geändert werden, bevor sie wieder in Betrieb genommen werden.	Die betroffenen Komponenten SOLLTEN einem Penetrationstest unterzogen werden, bevor sie wieder eingesetzt werden.	Bei der Wiederherstellung der sicheren Betriebsumgebung MÜSSEN die Benutzenden in die Anwendungsfunktionstests einbezogen werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	5	5	5	5	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	160	161	162	163	164

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Nachdem alles wiederhergestellt wurde, MÜSSEN die Komponenten inklusive der Netzübergänge gezielt überwacht werden.	Es SOLLTE eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert werden.	Die Abläufe, Prozesse und Vorgaben für die verschiedenen Sicherheitsvorfälle SOLLTEN dabei eindeutig geregelt und dokumentiert werden.	Die Institutionsleitung SOLLTE die festgelegte Vorgehensweise in Kraft setzen und allen Beteiligten zugänglich machen.	Es SOLLTE regelmäßig überprüft werden, ob die Vorgehensweise noch aktuell und wirksam ist.
Modalverb	MUSS	SOLL	SOLL	SOLL	SOLL
Seite	5	5	5	5	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	165	166	167	168	169

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Bei SOLLTE Bedarf die Vorgehensweise angepasst werden.	Für den Umgang mit Sicherheitsvorfällen SOLLTEN geeignete Organisationsstrukturen festgelegt werden.	Es SOLLTE ein Sicherheitsvorfall-Team aufgebaut werden, dessen Mitglieder je nach Art des Vorfalls einberufen werden können.	Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Fall zusammentritt, SOLLTEN bereits im Vorfeld geeignete Mitglieder benannt und in ihre Aufgaben eingewiesen sein.	Es SOLLTE regelmäßig geprüft werden, ob die Zusammensetzung des Sicherheitsvorfall-Teams noch angemessen ist.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	5	5	5	5	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	170	171	172	173	174

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Gegebenenfalls SOLLTE das Sicherheitsvorfall-Team neu zusammengestellt werden.	Für die verschiedenen Arten von Sicherheitsvorfällen SOLLTEN die jeweils passenden Meldewege aufgebaut sein.	Es SOLLTE dabei sichergestellt sein, dass Mitarbeitende die über verlässliche und vertrauenswürdige Kanäle schnell und einfach melden können.	Wird eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen eingerichtet, SOLLTE dies an alle Mitarbeitende kommuniziert werden.	Eine Kommunikations- und Kontaktstrategie SOLLTE vorliegen.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	5	5	5	5	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	175	176	177	178	179

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Darin SOLLTE geregelt sein, wer grundsätzlich informiert werden muss und wer informiert werden darf, durch wen dies in welcher Reihenfolge erfolgt und in welcher Tiefe informiert wird.	Es SOLLTE definiert sein, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt.	Ebenso SOLLTE sichergestellt sein, dass keine unautorisierten Personen Informationen über den Sicherheitsvorfall weitergeben.	Parallel zur Ursachenanalyse eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären.	Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, SOLLTEN ausreichend Informationen vorliegen.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	5	5	5	5	5
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	180	181	182	183	184

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Für ausgewählte Sicherheitsvorfalls zenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.	Ein einheitliches Verfahren SOLLTE festgelegt werden, um Sicherheitsvorfälle und Störungen einzustufen.	Das Einstufungsverfahren für Sicherheitsvorfälle SOLLTE zwischen Sicherheitsmanagement und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt sein.	Die Schnittstellen zwischen Störungs- und Fehlerbehebung, Notfallmanagement und Sicherheitsmanagement SOLLTEN analysiert werden.	Dabei SOLLTEN auch eventuell gemeinsam benutzbare Ressourcen identifiziert werden.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	5 f.	6	6	6	6
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	185	186	187	188	189

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Die bei der Störungs- und Fehlerbehebung beteiligten Mitarbeitenden SOLLTEN für die Behandlung von Sicherheitsvorfällen sowie für das Notfallmanagement sensibilisiert werden.	Das Sicherheits-management SOLLTE lesenden Zugriff auf eingesetzte Incident-Management-Werkzeuge haben.	Die Behandlung von Sicherheitsvorfällen SOLLTE mit dem Notfallmanagement abgestimmt sein.	Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, SOLLTE auch diese mit einbezogen werden.	Über die Kommunikations- und Kontaktstrategie hinaus SOLLTE eine Eskalationsstrategie formuliert werden.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	6	6	6	6	6
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	190	191	192	193	194

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Diese SOLLTE zwischen den Verantwortlichen für Störungs- und Fehlerbehebung und dem Informations-sicherheits-management abgestimmt werden.	Die Eskalationsstrategie SOLLTE eindeutige Handlungsanweisungen enthalten, wer auf welchem Weg bei welcher Art von oder erkennbaren vermuteten Sicherheitsstörungen wann einzubeziehen ist.	Es SOLLTE geregelt sein, zu welchen Maßnahmen eine Eskalation führt und wie reagiert werden soll.	Für die festgelegte Eskalationsstrategie SOLLTEN geeignete Werkzeuge wie z. B. Ticket-Systeme ausgewählt werden.	Diese SOLLTEN sich auch dafür eignen, vertrauliche Informationen zu verarbeiten.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	6	6	6	6	6
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	195	196	197	198	199

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Es SOLLTE sichergestellt sein, dass die Werkzeuge auch während eines Sicherheitsvorfalls bzw. Notfalls verfügbar sind.	Die Eskalations-strategie SOLLTE regelmäßig überprüft und gegebenenfalls aktualisiert werden.	Die Checklisten (Matching Szenarios) für Störungs- und Fehlerbehebung SOLLTEN regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert werden.	Die festgelegten Eskalationswege SOLLTEN in Übungen erprobt werden.	Dem Personal des Service Desk SOLLTEN geeignete Hilfsmittel zur Verfügung stehen, damit sie Sicherheitsvorfälle erkennen können.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	6	6	6	6	6
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	200	201	202	203	204

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Sie SOLLTEN ausreichend geschult sein, um die Hilfsmittel selbst anwenden zu können.	Die Mitarbeitenden des Service Desk SOLLTEN den Schutzbedarf der betroffenen Systeme kennen.	Die Behebung von Sicherheitsvorfällen SOLLTE nach einem standardisierten Verfahren dokumentiert werden.	Es SOLLTEN alle durchgeführten Aktionen inklusive der Zeitpunkte sowie die der betroffenen Komponenten dokumentiert werden.	Dabei SOLLTE die Vertraulichkeit bei der Dokumentation und Archivierung der gewährleistet sein. Berichte
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	6	6	6	6 f.	7
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	205	206	207	208	209

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Die benötigten Informationen SOLLTEN in die jeweiligen Dokumentations-systeme eingepflegt werden, bevor die Störung als beendet und als abgeschlossen markiert wird.	Im Vorfeld SOLLTEN mit dem oder der ISB die dafür erforderlichen Anforderungen an die Qualitätssicherung definiert werden.	Sicherheitsvorfälle SOLLTEN standardisiert nachbereitet werden.	Dabei SOLLTE untersucht werden, wie schnell die Sicherheitsvorfälle erkannt und behoben wurden.	Weiterhin SOLLTE untersucht werden, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung verfügbar und ob die Detektions-maßnahmen wirksam waren.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	7	7	7	7	7
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	210	211	212	213	214

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein	Nein
Anforderung	Ebenso SOLLTE geprüft werden, ob die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient waren.	Die Erfahrungen aus vergangenen Sicherheitsvorfälle n SOLLTEN genutzt werden, um daraus Handlungsanweisu ngen für vergleichbare Sicherheitsvorfälle zu erstellen.	Diese Handlungs-anweisungen SOLLTEN den relevanten Personengruppen bekanntgegeben und auf Basis neuer Erkenntnisse regelmäßig aktualisiert werden.	Die Institutionsleitung SOLLTE jährlich über die Sicherheitsvorfälle unterrichtet werden.	Besteht sofortiger Handlungsbedarf, MUSS die Institutionsleitung umgehend informiert werden.
Modalverb	SOLL	SOLL	SOLL	SOLL	SOLL
Seite	7	7	7	7	7
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	215	216	217	218	219

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Nachdem ein Sicherheitsvorfall analysiert wurde, SOLLTE untersucht werden, ob die Prozesse und Abläufe im Rahmen der Behandlung von Sicherheitsvorfällen geändert oder weiterentwickelt werden müssen.	Dabei SOLLTEN alle Personen, die an dem Vorfall beteiligt waren, über ihre jeweiligen Erfahrungen berichten.	Es SOLLTE geprüft werden, ob es neue Entwicklungen im Bereich Incident Management und in der Forensik gibt und ob diese in die jeweiligen Dokumente und Abläufe eingebracht werden können.	Werden Hilfsmittel und Checklisten eingesetzt, z. B. für Service-Desk-Mitarbeitende, SOLLTE geprüft werden, ob diese um relevante Fragen und Informationen zu erweitern sind.
Modalverb	SOLL	SOLL	SOLL	SOLL
Seite	7	7	7	7
Quelle	DER.2.1	DER.2.1	DER.2.1	DER.2.1
Nummer	220	221	222	223

Begründung	Die SzA müssen die Funktion bieten, auf automatisiert sicherheitsrelevante Ereignisse zu melden und darauf zu reagieren. Um die Gefährdung der kritischen Dienstleistung auszuschließen, muss der gezielte Ausschluss von Netzen aus der automatisierten Reaktion möglich sein.	Da Anforderung Nummer 230 den automatisierten Eingriff in den Datenstrom durch die SzA fordert, wird diese Anforderung so interpretiert, dass die Möglichkeit des automatisierten Eingriffs durch die IT-Systemlandschaft erst geschaffen werden muss. Diese Anforderung ist somit durch die IT-Umgebung des Unternehmens, nicht die SzA, zu erfüllen. Dies erfolgt dadurch, dass der durch die SzA in Anforderung Nummer 230 geforderten Aktivitäten ermöglicht werden, beispielsweise durch Bereitstellung entsprechender Schnittstellen an Firewalls, die die automatisierte Blockade von Netzwerkkommunikation ermöglichen.
Anwendbar?	Ja	Nein
Anforderung	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.	In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, MUSS es möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.
Modalverb	MUSS	MUSS
Seite	14	14
Quelle	OH-SzA	OH-SzA
Nummer	224	225

Begründung	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.	Diese Anforderung ist organisatorischer Art und durch die Systeme zur Reaktion nicht zu erfüllen.
Anwendbar?	Nein	Nein	Nein	Nein
Anforderung	Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird.	Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion, bzw. dem Eingriff in den Datenstrom MUSS schlüssig begründet sein.	Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.	Bei Störungen und Sicherheitsvorfällen insbesondere im vermeintlichen Zusammenhang mit Angriffen MUSS überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. § 11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	14	14	14	14
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	226	227	228	229

Begründung	Die Formulierung "automatisch in den Datenstrom einzugreifen" bietet Interpretationsspielraum dahingehend, was mit dem "Datenstrom" gemeint ist. Die Anforderung wird hier so interpretiert, dass allgemein die SzA Funktionen bieten müssen, mit denen die Netzwerkkommunikation oder einzelne Vorgänge auf einem System gezielt unterbunden werden können. So wird in die Datenverarbeitung und -verbreitung, also den "Datenstrom", eingegriffen.	Dies ist zwar vorrangig organisatorisch/prozessual durch entsprechende Risikobewertungen sicherzustellen, die SzA müssen jedoch die Möglichkeit bieten, die automatisiert ergriffenen Maßnahmen zu Konfigurieren und den Zielbereich zu definieren, um kritische Netze oder Systeme auszuschließen.	Eine manuelle Qualifizierung wird bereits in Anforderung Nummer 121 gefordert. Die eingesetzten SzA sollten aber eine manuelle Behandlung von Ereignissen ermöglichen, beispielsweise indem vordefinierte Reaktionsabläufe manuell gestartet, aber durch das SzA ausgeführt werden können.
Anwendbar?	Ja	Ja	Ja
Anforderung	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.
Modalverb	SOLL	MUSS	SOLL
Seite	14	14	14
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	230	231	232

Anlage 5 Vorlage Prüfmatrix SzA

Übergreifende Anforderungen

Begründung	
Erfüllt?	
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Protokollierung

Begründung	
Erfüllt?	
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.
Modalverb	MUSS
Seite	9
Quelle	OH-SzA
Nummer	8

		Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.
		KANN	MUSS	SOLL
		9	9	9
		OH-SzA	OH-SzA	OH-SzA
		9	11	13

		Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.			
		MUSS	MUSS	MUSS	MUSS
		5	5	10	10
		OPS.1.1.5	OPS.1.1.5	OH-SzA	OH-SzA
		35	37	42	43	47
			Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.			
			MUSS			
			5			
			OPS.1.1.5			
			37			
				Es MUSS technisch unterbunden werden, dass Protokollierungs-daten unkontrolliert gelöscht oder verändert werden.		
				MUSS		
				5		
				OPS.1.1.5		
				42		
					Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	
					MUSS	
					10	
					OH-SzA	
					43	
						Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.
						MUSS
						10
						OH-SzA
						47

Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN verfügbar gemacht werden, damit sie ausgewertet werden können		
MUSS		
10		
OH-SzA		
48		
Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN zusätzlich unterstützen.		
KANN		
10		
OH-SzA		
49		

Anforderungen zur Detektion

Begründung		
	Erfüllt?	**Anforderung**
		Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.
		Modalverb
		Seite
		Quelle
		Nummer
		MUSS
		11
		OH-SzA
		55

Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS).		Falls ein sicherheitsrelevant er Vorfall vorliegt, dann MÜSSEN die betroffenen Systeme ausgewertet werden.		Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN die diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten.	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.
KANN		MUSS		MUSS	MUSS	MUSS
11		5		5	5	11
OH-SzA		DER.1		DER.1	DER.1	OH-SzA
57		80		84	85	87

Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.		Es MÜSSEN Schadcodedetektions-systeme eingesetzt und zentral verwaltet werden.	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.
KANN		MUSS	MUSS	MUSS	MUSS
11		11	11	11	11
OH-SzA		OH-SzA	OH-SzA	OH-SzA	OH-SzA
88		93	95	97	98

		Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.		Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.		
		MUSS		MUSS		
		12		12		
		OH-SzA		OH-SzA		
		99		108		
		Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten zu aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.		Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.		
		MUSS		MUSS		
		12		12		
		OH-SzA		OH-SzA		
		109		110		
				Die Daten MÜSSEN kontinuierlich ausgewertet werden.		
				MUSS		
				12		
				OH-SzA		
				111		

		Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.
		MUSS	MUSS	MUSS	MUSS	MUSS
		12	12	12	12	12
		OH-SzA	OH-SzA	OH-SzA	OH-SzA	OH-SzA
		112	114	115	116	121

Anforderungen zur Reaktion

Begründung				
Erfüllt?				
Anforderung	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.
Modalverb	MUSS	SOLL	MUSS	SOLL
Seite	14	14	14	14
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	224	230	231	232

Anlage 6 Prüfmatrix Logstash

Anforderungen zur Protokollierung

Begründung	Winlogbeat und Filebeat können sicherheitsrelevante Protokolldaten von Windows- und Linux-Endpunkten erheben und an Logstash weiterleiten. Logstash kann über das Syslog Input Plugin per Syslog zusätzliche Protokolldaten empfangen [115], speichern und für die Auswertung in anderen Systemen über eine Vielzahl von Output-Plugins bereitstellen [116].	Weder Logstash noch Winlogbeat und Filebeat erzeugen Protokolldaten über Drittsysteme. Logstash dient der Weiterleitung und Verarbeitung empfangener Daten, Winlogbeat und Filebeat leiten nur die durch ihr jeweiliges Wirtssystem generierten Daten weiter.
Erfüllt?	Ja	Nein
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.
Modalverb	MUSS	KANN
Seite	9	9
Quelle	OH-SzA	OH-SzA
Nummer	8	9

Begründung	Ist eine Anonymisierung bzw. Pseudonymisierung der Protokolldaten erforderlich, ist das mit dem "mutate" Filter Plugin von Logstash umsetzbar, indem entsprechende Datenfelder entfernt oder durch Platzhalter ersetzt werden [117].	Weder Logstash noch Winlogbeat und Filebeat erzeugen Protokolldaten über Drittsysteme. Logstash dient der Weiterleitung und Verarbeitung empfangener Daten, Winlogbeat und Filebeat leiten nur die durch ihr jeweiliges Wirtssystem generierten Daten weiter. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.	Weder Logstash noch Winlogbeat und Filebeat erzeugen Protokolldaten über Drittsysteme. Logstash dient der Weiterleitung und Verarbeitung empfangener Daten, Winlogbeat und Filebeat leiten nur die durch ihr jeweiliges Wirtssystem generierten Daten weiter. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.
Erfüllt?	Ja	Nein	Nein
Anforderung	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.
Modalverb	MUSS	SOLL	MUSS
Seite	9	9	5
Quelle	OH-SzA	OH-SzA	OPS.1.1.5
Nummer	11	13	35

Begründung	Logstash bietet über das Date Filter Plugin die Möglichkeit, das Datums- und Zeitformat der Protokolldateien zu normalisieren [118].	Logstash dient zwar nur der Weiterleitung von Daten, kann diese aber in persistenten Queues zwischenspeichern. Die Queues können kontrolliert gelöscht werden, liegen allerdings als Dateien auf dem jeweiligen System ab [119]. Diese Dateien könnten theoretisch unkontrolliert gelöscht werden, weshalb das Betriebssystem entsprechende Zugriffsbeschränkungen umsetzen muss.	Logstash bietet über eine Vielzahl von Output Modulen die Möglichkeit, die gesammelten Protokolldaten an eine zentrale Stelle weiterzuleiten [116].
Erfüllt?	Ja	Ja	Ja
Anforderung	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.
Modalverb	MUSS	MUSS	MUSS
Seite	5	5	10
Quelle	OPS.1.1.5	OPS.1.1.5	OH-SzA
Nummer	37	42	43

Begründung	Logstash bietet über das Drop Filter Plugin die Möglichkeit, Protokolldaten auszufiltern [120], über das Mutate Filter Plugin zu verändern bzw. normalisieren [117], sowie über das Aggregate Filter Plugin zu aggregieren und korrelieren [121].	Logstash bietet über eine Vielzahl von Output Modulen die Möglichkeit, die gesammelten Protokolldaten einer großen Anzahl an Analysewerkzeugen verfügbar zu machen [116].	Logstash bietet die Möglichkeit, neben den extrahierten Datenfeldern im "message" Feld die unbearbeiteten Protokolldaten zu transportieren [122].
Erfüllt?	Ja	Ja	Ja
Anforderung	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	MUSS	MUSS	KANN
Seite	10	10	10
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	47	48	49

Anlage 7 Prüfmatrix Graylog Open

Anforderungen zur Protokollierung

Begründung	Graylog kann Protokolldaten über eine Vielzahl von Inputs [123], darunter auch Syslog [124] und Windows Event Logs über Winlogbeat [33] empfangen und speichern. Zur Erfassung der Protokolldaten auf den Endpunkten sind separate Lösungen wie Winlogbeat, Filebeat oder andere Syslog-Lösungen erforderlich. Die gesammelten Daten können für die Auswertung in anderen Systemen über TCP in Raw Plaintext oder Syslog Formaten bereitgestellt werden [125].	Graylog erzeugt keine Protokolldaten über Drittsysteme, sondern dient dem Empfang, Verarbeitung und Bereitstellung empfangener Daten.
Erfüllt?	Ja	Nein
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.
Modalverb	MUSS	KANN
Seite	9	9
Quelle	OH-SzA	OH-SzA
Nummer	8	9

Begründung	Ist eine Anonymisierung bzw. Pseudonymisierung der Protokolldaten erforderlich, ist das über die Pattern-Matching- und String-Funktionen in Graylog umsetzbar, indem entsprechende Datenfelder entfernt oder durch Platzhalter ersetzt werden [126].	Graylog erzeugt keine Protokolldaten über Drittsysteme, sondern dient dem Empfang, Verarbeitung und Bereitstellung empfangener Daten. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.	Graylog erzeugt keine Protokolldaten über Drittsysteme, sondern dient dem Empfang, Verarbeitung und Bereitstellung empfangener Daten. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.
Erfüllt?	Ja	Nein	Nein
Anforderung	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.
Modalverb	MUSS	SOLL	MUSS
Seite	9	9	5
Quelle	OH-SzA	OH-SzA	OPS.1.1.5
Nummer	11	13	35

Begründung	Graylog bietet über diverse Date/Time-Funktionen die Möglichkeit, das Datums- und Zeitformat der verarbeiteten Daten zu vereinheitlichen [126].	Graylog bietet über ein Rollen- und Berechtigungskonzept die Möglichkeit, das Berechtigung zum Löschen von Daten granular zu steuern [127].	Graylog bietet über TCP-Outputs die Möglichkeit, Protokolldaten an eine zentrale Stelle weiterzuleiten oder kann selbst als diese dienen.	Graylog bietet über diverse Funktionen die Möglichkeit zur Filterung und Bearbeitung bzw. Normalisierung von Daten [126]. Daten können nur über Dashboards und Reports aggregiert [128] werden, eine interne Aggregationsmöglichkeit geht aus der Dokumentation nicht hervor. Die zur Korrelation verwendete Correlation Engine ist exklusiv in Graylog Enterprise verfügbar und wird daher mit Graylog Open nicht erfüllt [39].
Erfüllt?	Ja	Ja	Ja	Nein
Anforderung	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	5	5	10	10
Quelle	OPS.1.1.5	OPS.1.1.5	OH-SzA	OH-SzA
Nummer	37	42	43	47

Begründung	Daten können in Graylog selbst über Dashboards und Reports [128] oder Search Queries [129] ausgewertet, oder über TCP Output für Detektionssysteme verfügbar gemacht werden [125].	Aus der Dokumentation [38] wird nicht ersichtlich, ob Graylog die unbearbeiteten Protokolldaten beibehält.
Erfüllt?	Ja	Nein
Anforderung	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	MUSS	KANN
Seite	10	10
Quelle	OH-SzA	OH-SzA
Nummer	48	49

Anlage 8 Prüfmatrix Fluentd

Anforderungen zur Protokollierung

Begründung	Fluentd kann sicherheitsrelevante Protokolldaten auf Windows- [130] und Linux-Endpunkten [131] erheben, über Syslog- und weitere Input-Plugins zusätzliche Protokolldaten empfangen [132], speichern und über eine Vielzahl von Output Plugins für die Auswertung in anderen Systemen bereitstellen [133].	Fluentd erzeugt keine Protokolldaten über Drittsysteme, sondern dient der Erhebung, dem Empfang, der Verarbeitung und der Weiterleitung von Protokolldaten.	Ist eine Anonymisierung bzw. Pseudonymisierung der Protokolldaten erforderlich, ist das mit dem "record_transformer" Filter Plugin von Fluentd umsetzbar, indem entsprechende Datenfelder entfernt oder durch Platzhalter ersetzt werden [134].
Erfüllt?	Ja	Nein	Ja
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.
Modalverb	MUSS	KANN	MUSS
Seite	9	9	9
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	8	9	11

Begründung	Fluentd erzeugt keine Protokolldaten über Drittsysteme, sondern dient der Erhebung, dem Empfang, der Verarbeitung und der Weiterleitung von Protokolldaten. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.	Fluentd erzeugt keine Protokolldaten über Drittsysteme, sondern dient der Erhebung, dem Empfang, der Verarbeitung und der Weiterleitung von Protokolldaten. Hierfür wären ergänzende Detektionssysteme eine denkbare Lösung.	Fluentd bietet über das parser Plugin die Möglichkeit, das Datums- und Zeitformat der Protokolldateien zu normalisieren [135].	Fluentd bietet abgesehen von Buffer Plugins [136] keine Speichermöglichkeiten für die Protokolldaten, weshalb eine Löschung nicht seitens Fluentd kontrolliert werden kann.
Erfüllt?	Nein	Nein	Ja	Nein
Anforderung	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.
Modalverb	SOLL	MUSS	MUSS	MUSS
Seite	9	5	5	5
Quelle	OH-SzA	OPS.1.1.5	OPS.1.1.5	OPS.1.1.5
Nummer	13	35	37	42

Begründung	Fluentd bietet über eine Vielzahl von Output Modulen die Möglichkeit, die gesammelten Protokolldaten an eine zentrale Stelle weiterzuleiten [133].	Fluentd bietet über den grep Filter die Möglichkeit, auszufiltern Protokolldaten [137], über die parser [135] und record_transformer [134] Filter Plugins zu verändern bzw. normalisieren. Für die Aggregation und Korrelation steht eine Vielzahl anderer Plugins zur Verfügung [138].	Fluentd bietet über eine Vielzahl von Output Modulen die Möglichkeit, die gesammelten Protokolldaten einer großen Anzahl an Analysewerkzeugen verfügbar zu machen [133].	Fluentd bietet die Möglichkeit, die unbearbeiteten Protokolldaten mittels des none Parsers beizubehalten [139].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	MUSS	MUSS	MUSS	KANN
Seite	10	10	10	10
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	43	47	48	49

Anlage 9 Prüfmatrix Wazuh

Übergreifende Anforderungen

Begründung	Wazuh bietet über API-Integrationen die Möglichkeit, Signaturen in Form von IoCs beispielsweise über Maltiverse abzurufen [140] oder direkt gegen entsprechende APIs beispielsweise von VirusTotal zu prüfen [141].
Erfüllt?	Ja
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Protokollierung

Begründung	Der Wazuh Server kann Protokolldaten auf Basis von Syslog direkt empfangen [101] und von Windows, Linux und MacOS über den Wazuh Agent selbstständig erheben [142]. Kann auf einem Endpunkt kein Agent installiert werden, unterstützt Wazuh agentenlose Überwachung mittels SSH [143].
Erfüllt?	Ja
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.
Modalverb	MUSS
Seite	9
Quelle	OH-SzA
Nummer	8

Begründung	Wazuh ist auf die Anlieferung von Protokolldaten oder die Installation des Agenten bzw. agentenlose Anbindung der Systeme, die überwacht werden sollen, angewiesen.	Wenn eine Anonymisierung oder Pseudonymisierung erforderlich ist, können die Decoder für die Protokolldaten angepasst werden, um relevante Felder zu anonymisieren oder zu entfernen [144].	Wazuh bietet auf Endpunkten über Protokolldatenauswertung hinausgehende Detektionsmöglichkeiten für Malwareerkennung [145], Dateiintegritätsüberwachung [146] und aktive Reaktion auf Ereignisse [147].
Erfüllt?	Nein	Ja	Ja
Anforderung	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokollierungsdaten und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.
Modalverb	KANN	MUSS	SOLL
Seite	9	9	9
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	9	11	13

Begründung	Wazuh ist auf die Anlieferung von Protokolldaten oder die Installation des Agenten bzw. agentenlose Anbindung der Systeme, die überwacht werden sollen, angewiesen.	Wazuh kann mittels Decodern das Zeit- und Datumsformat der Protokolldateien normalisieren [148].	Das Löschen von Protokollierungsdaten erfolgt in Wazuh automatisiert über das Index Life Management nach einer definierten Zeit [149]. Eine manuelle oder unkontrollierte Löschung spezifischer Protokollierungsdaten ist nicht möglich. Das Löschen eines gesamten Daten-Index kann über das Role Based Access Control System granular berechtigt werden [150].
Erfüllt?	Nein	Ja	Ja
Anforderung	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.
Modalverb	MUSS	MUSS	MUSS
Seite	5	5	5
Quelle	OPS.1.1.5	OPS.1.1.5	OPS.1.1.5
Nummer	35	37	42

Begründung	Zur Speicherung aller gesammelten Protokolldaten kann auf dem Wazuh Server das Wazuh Archive aktiviert werden, das sämtliche gesammelten Protokolldaten speichert, unabhängig davon, ob diese einen Alarm ausgelöst haben [151].	Die gesammelten Daten können über Decoder gefiltert und normalisiert werden, während sie über Rules aggregiert und korreliert werden können [148].	Die gespeicherten Daten über das Wazuh Dashboard zur Visualisierung und Analyse zur Verfügung gestellt [152].	Die Speicherung der Protokolldaten über Wazuh Archives im unbearbeiteten Syslog-Format ist konfigurierbar [151].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	MUSS	MUSS	MUSS	KANN
Seite	10	10	10	10
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	43	47	48	49

Anforderungen zur Detektion

Begründung	Das MITRE ATT&CK Framework ist in Wazuh integriert, die mitgelieferten Detektionsregeln sind dagegen gemappt [153]. Die Abdeckung der Bedrohungslandschaft kann durch Aufnahme weiterer Regeln und mappen auf ATT&CK erhöht werden.	Das MITRE ATT&CK Framework ist in Wazuh integriert, die mitgelieferten Detektionsregeln sind dagegen gemappt [153].	Die Alerts zu sicherheitsrelevanten Vorfällen können über Wazuh Dashboards ausgewertet werden [152].	Die Meldungen des File Integrity Monitoring Moduls werden analog zu anderen, durch den Agenten erhobenen Protokolldaten an den Wazuh Manager weitergeleitet [154].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.	Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS).	Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN die Meldungen der betroffenen IT-Systeme ausgewertet werden.	Falls ein Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten.
Modalverb	MUSS	KANN	MUSS	MUSS
Seite	11	11	5	5
Quelle	OH-SzA	OH-SzA	DER.1	DER.1
Nummer	55	57	80	84

Begründung	Über Regeln kann eine Meldung definierter sicherheitsrelevante Ereignisse aus dem File Integrity Monitoring Modul eingerichtet werden [155].	Die eingelieferten Protokolldaten werden in Echtzeit dekodiert und mit den definierten Regeln und ausgewertet [156].	Die eingelieferten Protokolldaten werden in Echtzeit dekodiert und mit den definierten Regeln überwacht und ausgewertet [156]. Eine direkte Alarmierung kann über das Dashboard oder Integrationen mit Drittanbieter-Tools wie Slack, PagerDuty und Shuffle erfolgen [114].	Wazuh kann mittels des File Integrity Monitoring Moduls und Schadcodesignaturen z.B. von VirusTotal auf Schadcode prüfen [145]. Die Agenten werden zentral durch den Wazuh Manager verwaltet [157].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.	Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden.
Modalverb	MUSS	MUSS	KANN	MUSS
Seite	5	11	11	11
Quelle	DER.1	OH-SzA	OH-SzA	OH-SzA
Nummer	85	87	88	93

Begründung	Wazuh bietet keine NIDS-Funktionalität, wobei entsprechende Systeme als Datenquelle integriert werden können [80].	Das Wazuh Dashboard stellt die gesammelten Ereignismeldungen dar [152], was regelmäßig kontrolliert werden kann.	Das Ruleset von Wazuh wird mit jedem Release aktualisiert [158]. Darüber hinaus können Signaturen wie IoCs über Drittanbieter-Integrationen wie Maltiverse abgerufen werden [114].	In Wazuh können Signaturen wie IoCs über Drittanbieter-Integrationen wie Maltiverse abgerufen werden [114]. Darüber hinaus werden die Bedrohungsinformationen aus MITRE ATT&CK über das MITRE ATT&CK Modul zur Verfügung gestellt [153].
Erfüllt?	Nein	Ja	Ja	Ja
Anforderung	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	11	11	11	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	95	97	98	99

Begründung	Der Wazuh Server dient als zentrale Komponente zur Erkennung und Auswertung sicherheitsrelevanter Ereignisse [159].	Der Wazuh Server zeichnet die Daten in Wazuh Indexern auf und prüft auf sicherheitsrelevante Vorgänge [159], die im Wazuh Dashboard sichtbar gemacht werden [152].	In Wazuh Archives werden alle eingelieferten Protokolldaten gespeichert, unabhängig davon, ob sie eine Regel auslösen [151].	Der Wazuh Server wertet alle eingelieferten Protokolldaten in Echtzeit mittels der definierten Regeln aus [156].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	Die Daten MÜSSEN kontinuierlich ausgewertet werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	108	109	110	111

Begründung	Wird ein konfigurierbarer Schwellwert durch eine Regel überschritten, löst Wazuh einen Alert aus [160].	Wazuh bietet die Möglichkeit, das Ruleset frei zu konfigurieren [161].	Wazuh bietet nativ keine Funktion, bereits überprüfte Protokolldaten erneut automatisch zu untersuchen.	Der Wazuh Server holt aktuelle Schwachstellen-informationen aus diversen Quellen automatisch ein [162].
Erfüllt?	Ja	Ja	Nein	Ja
Anforderung	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.	Die System-verantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	112	114	115	116

Begründung	Regeln in Wazuh können klassifiziert werden, wodurch eine Unterscheidung zum Beispiel zwischen schwerwiegenden Angriffen (Level 12) oder Ereignissen, die ein durch Nutzer entstandener Fehler sind (Level 5) [163].
Erfüllt?	Ja
Anforderung	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.
Modalverb	MUSS
Seite	12
Quelle	OH-SzA
Nummer	121

Anforderungen zur Reaktion

Begründung	Wazuh löst bei erfüllten Regeln einen Alert aus [159] und bietet die Möglichkeit, über Active Response automatisiert zu reagieren [147].
Erfüllt?	Ja
Anforderung	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.
Modalverb	MUSS
Seite	14
Quelle	OH-SzA
Nummer	224

Begründung	Active Response Regeln können in Wazuh so konfiguriert werden, dass sie ab einer bestimmten Klassifizierung des SRE/Alert auslösen [147].	Wazuh bietet die Möglichkeit, einzelne Systeme über White Lists von der Active Response auszuschließen [164]. So können Systeme, bei denen automatisierte Maßnahmen die kritische Dienstleistung beeinträchtigen können, von der automatisierten Reaktion ausgenommen werden. Active Response kann auf Seite des Agenten auch gänzlich deaktiviert werden [165].	Im Bedarfsfall kann über die Wazuh API ein Active Response Command manuell ausgeführt werden [166].
Erfüllt?	Ja	Ja	Ja
Anforderung	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.
Modalverb	SOLL	MUSS	SOLL
Seite	14	14	14
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	230	231	232

Anlage 10 Prüfmatrix OpenSearch

Übergreifende Anforderungen

Begründung	OpenSearch bietet die Möglichkeit, Signaturen in Form von Sigma Regeln über Threat Intelligence Feeds zu integrieren [167].
Erfüllt?	Ja
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Detektion

Begründung	Das MITRE ATT&CK Framework ist in OpenSearch integriert, die mitgelieferten Detektionsregeln sind dagegen gemappt [168]. Die Abdeckung der Bedrohungslandschaft kann durch Aufnahme weiterer Regeln und mappen auf ATT&CK erhöht werden.
Erfüllt?	Ja
Anforderung	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.
Modalverb	MUSS
Seite	11
Quelle	OH-SzA
Nummer	55

Begründung	Das MITRE ATT&CK Framework ist in OpenSearch integriert, die mitgelieferten Detektionsregeln sind dagegen gemappt [168].	Die Findings zu sicherheitsrelevanten Vorfällen können über die Overview Seite von OpenSearch Security Analytics ausgewertet werden [169].	OpenSearch bietet keine auf zentralen IT-Systemen installierbaren Schadcodescanner.	OpenSearch bietet keine auf zentralen IT-Systemen installierbaren Schadcodescanner.	Die Detektoren können in konfigurierbaren Intervallen ausgeführt werden, wodurch eine kontinuierliche Auswertung realisiert werden kann [170].
Erfüllt?	Ja	Ja	Nein	Nein	Ja
Anforderung	Zur Bestimmung der Abdeckung KANN (und es wird empfohlen) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS).	Falls ein sicherheitsrelevanter Vorfall vorliegt, dann MÜSSEN Meldungen der betroffenen IT-Systeme ausgewertet werden.	Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN die diese es über einen zentralen Zugriff ermöglichen, ihre Meldungen und Protokolle auszuwerten.	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich und überwacht ausgewertet werden.
Modalverb	KANN	MUSS	MUSS	MUSS	MUSS
Seite	11	5	5	5	11
Quelle	OH-SzA	DER.1	DER.1	DER.1	OH-SzA
Nummer	57	80	84	85	87

Begründung	Die Detektoren führen eine automatisierte Überwachung der Protokolldaten in konfigurierbaren Intervallen durch und lösen bei Treffern einen Alert aus [170]. Ein Alert kann eine Notification über APIs, E-Mail oder Amazon SNS auslösen [171].	OpenSearch bietet keine Schadcode-detektions-möglichkeiten.	OpenSearch bietet keine NIDS-Funktionalität.	Die Overview Seite von OpenSearch Security Analytics stellt die gesammelten Alerts dar [169], was regelmäßig kontrolliert werden kann.
Erfüllt?	Ja	Nein	Nein	Ja
Anforderung	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.	Es MÜSSEN Schadcode-detektionssysteme eingesetzt und zentral verwaltet werden.	Insbesondere die im MÜSSEN Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.
Modalverb	KANN	MUSS	MUSS	MUSS
Seite	11	11	11	11
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	88	93	95	97

Begründung	In OpenSearch Security Analytics können Threat Intelligence Feeds, die Signaturen in Form von IoCs liefern, in Detectors integriert werden [167].	In OpenSearch Security Analytics können Threat Intelligence Feeds, die Signaturen in Form von IoCs liefern, in Detectors integriert werden [167].	Die Detectors und Correlation Rules [172] in OpenSearch Security Analytics dienen als zentrale Komponenten zur Erkennung sicherheitsrelevanter Ereignisse.	Die Detectors [170] und Correlation Rules [172] in OpenSearch Security Analytics dienen als zentrale Komponenten zur Ereignisse und lösen Alerts aus.
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	11	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	98	99	108	109

Begründung	In OpenSearch können alle eingelieferten Protokolldaten über die Discover Applikation [173] oder sonstige Dashboards eingesehen werden.	Die Detektoren können in konfigurierbaren Intervallen ausgeführt werden, wodurch eine kontinuierliche Auswertung realisiert werden kann [170].	Alerts können so konfiguriert werden, dass bei Auslösen konfigurierter Regeln mit einem definierten Schweregrad alarmiert wird [170].	Die Detectors [170] und Correlation Rules [172] in OpenSearch Security Analytics sind konfigurierbar.	Die Detektoren können in konfigurierbaren Intervallen ausgeführt werden, wodurch eine regelmäßige Auswertung auch bereits überprüfter Daten realisiert werden kann [170].
Erfüllt?	Ja	Ja	Ja	Ja	Ja
Anforderung	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	Die MÜSSEN Daten kontinuierlich ausgewertet werden.	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.	Die System-verantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Zusätzlich MÜSSEN bereits Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.
Modalverb	MUSS	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	110	111	112	114	115

Begründung	In OpenSearch Security Analytics können Threat Intelligence Feeds, die Angriffsmuster in Form von IoCs liefern, in Detectors integriert werden [167].	Detection Rules in OpenSearch sind nach Schweregrad klassifiziert, was eine automatisierte Qualifikation ermöglicht [174].
Erfüllt?	Ja	Ja
Anforderung	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.
Modalverb	MUSS	MUSS
Seite	12	12
Quelle	OH-SzA	OH-SzA
Nummer	116	121

Anlage 11 Prüfmatrix Security Onion

Übergreifende Anforderungen

Begründung	Security Onion bietet die Möglichkeit, Signaturen über Threat Intelligence Anbieter zu integrieren, zu denen Integrationen mit dem Präfix "ti_" verfügbar sind [175].
Erfüllt?	Ja
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Protokollierung

Begründung	Security Onion beinhaltet Elasticsearch, Logstash und Redis und kann Protokolldaten somit auf Basis von Syslog oder den Elastic Agent erheben und empfangen [176].
Erfüllt?	Ja
Anforderung	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.
Modalverb	MUSS
Seite	9
Quelle	OH-SzA
Nummer	8

Begründung	Security Onion umfasst NIDS-Funktionalitäten wie Suricata [177] und Strelka [178], die eine Angriffserkennung auf Netzwerkebene ohne Protokolldatenaufzeichnung jedes einzelnen Geräts ermöglichen.	Das Parsing von Protokolldaten erfolgt in Security Onion mit ElasticSearch [179]. ElasticSearch bietet mit dem gsub-Processor die Möglichkeit, Protokolldateninhalte mittels regulärer Ausdrücke zu anonymisieren bzw. pseudonymisieren [180].	Security Onion bietet die Möglichkeit, mittels des Elastic Agenten die Protokolldaten selbst auf kompatiblen Endpunkten zu erheben [181], oder über diverse Netzwerkvisibilitätswerkzeuge dort Detektion zu ermöglichen [182].
Erfüllt?	Ja	Ja	Ja
Anforderung	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.
Modalverb	KANN	MUSS	SOLL
Seite	9	9	9
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	9	11	13

Begründung	Security Onion kann mittels Netzwerkvisibilitäts-werkzeugen dort den Datenverkehr protokollieren [182].	Das Parsing von Protokolldaten erfolgt in Security Onion mit ElasticSearch [179]. ElasticSearch bietet mit dem date-Processor die Möglichkeit, das Datums- und Zeitformat der Protokolldaten zu vereinheitlichen [183].	In Security Onion werden die in den ElasticSeach für die Speicherung von Protokolldaten genutzten Indizes über ein Index Lifecycle Management verwaltet, das eine unkontrollierte Löschung der Daten verhindert [179]. Ergänzend dazu kann die manuelle Löschung von Indizes deaktiviert werden [179].	Die gesammelten Protokolldaten werden in Security Onion in ElasticSearch zentral gespeichert [179].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.	Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.	Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	5	5	5	10
Quelle	OPS.1.1.5	OPS.1.1.5	OPS.1.1.5	OH-SzA
Nummer	35	37	42	43

Begründung	Die gesammelten Daten können über ElasticSearch Processors gefiltert, normalisiert und aggregiert werden [184]. Die Korrelation erfolgt in Security Onion über ElastAlert [185].	Die gespeicherten Daten werden in Security Onion für die Auswertung in ElastAlert [185], den Dashboards [186] und dem Hunt-Interface [187] verfügbar gemacht.	ElasticSearch speichert in Security Onion die unbearbeiteten Daten im _source-Feld mit [188].
Erfüllt?	Ja	Ja	Ja
Anforderung	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.
Modalverb	MUSS	MUSS	KANN
Seite	10	10	10
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	47	48	49

Anforderungen zur Detektion

Begründung	Der MITRE ATT&CK Navigator ist in die Security Onion Console integriert [189], allerdings sind keine direkten Mappings von ATT&CK auf die Detektionsregeln in Security Onion ersichtlich. Eine Abdeckung der Bedrohungslandschaft muss daher prozessual sichergestellt werden, Security Onion liefert jedoch das Werkzeug dafür.	Der MITRE ATT&CK Navigator ist in Security Onion integriert und kann zur Bestimmung der Abdeckung mittels MITRE ATT&CK verwendet werden [189].	Die Alerts zu sicherheitsrelevanten Vorfällen können über das Interface in der Security Onion Console ausgewertet werden [190].	Security Onion bietet keine auf zentralen IT-Systemen installierbaren Schadcodescanner.
Erfüllt?	Ja	Ja	Ja	Nein
Anforderung	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.	Zur Bestimmung der Abdeckung (und es empfohlen) standardisierte Methode angewendet werden (z. B. MITRE ATT&CK for ICS).	Falls ein sicherheitsrelevanter Vorfall vorliegt, dann eine MÜSSEN Meldungen der betroffenen IT-Systeme bzw. ausgewertet werden.	Falls zusätzliche Schadcodescanner eingesetzt werden, dann MÜSSEN diese es über einen zentralen Zugriff ermöglichen, Meldungen und Protokolle auszuwerten.
Modalverb	MUSS	KANN	MUSS	MUSS
Seite	11	11	5	5
Quelle	OH-SzA	OH-SzA	DER.1	DER.1
Nummer	55	57	80	84

Begründung	Security Onion bietet keine auf zentralen IT-Systemen installierbaren Schadcodescanner.	Die Protokolldaten von Security Onion werden in Security Onion kontinuierlich mittels ElastAlert überwacht und ausgewertet [185].	ElastAlert führt über Sigma Regeln eine automatisierte Überwachung der Protokolldaten durch und löst bei Treffern einen Alert aus, der im Alerts Interface sichtbar wird [191].	Security Onion bietet keine Schadcodedetektions-möglichkeiten.	Security Onion beinhaltet eine Werkzeugsammlung für Netzwerkvisibilität [182], darunter das NIDS Suricata [177].
Erfüllt?	Nein	Ja	Ja	Nein	Ja
Anforderung	Es MUSS sichergestellt sein, dass die Schadcodescanner sicherheitsrelevante Ereignisse automatisch an die Zuständigen melden.	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.	Es MÜSSEN Schadcodedetektions-systeme eingesetzt und zentral verwaltet werden.	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.
Modalverb	MUSS	MUSS	KANN	MUSS	MUSS
Seite	5	11	11	11	11
Quelle	DER.1	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	85	87	88	93	95

Begründung	Das Alerts Interface der Security Onion Console stellt die gesammelten Alerts dar [190], was regelmäßig kontrolliert werden kann.	Security Onion bietet die Möglichkeit, Signaturen über Threat Intelligence Anbieter zu integrieren, zu denen Integrationen mit dem Präfix "ti_" verfügbar sind [175].	Security Onion bietet die Möglichkeit, Signaturen über Threat Intelligence Anbieter zu integrieren, zu denen Integrationen mit dem Präfix "ti_" verfügbar sind [175].	Security Onion bietet als zentrale Komponente Erkennungs- und Auswertungsmöglichkeiten für sicherheitsrelevante Ereignisse mittels NIDS, Sigma-Regeln und YARA-Regeln [192].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	11	11	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	97	98	99	108

Begründung	Die Sigma-Regeln in Security Onion setzen die gesammelten Protokolldaten in Bezug zueinander und generieren Alerts bei Treffern [191].	In den Security Onion Dashboards kann die Query-Funktion zur Durchsuchung der Protokolldaten verwendet werden [186].	Die eingelieferten Protokolldaten werden in Security Onion kontinuierlich mit Sigma-Regeln ausgewertet [191].	Sigma Regeln können frei konfiguriert und getuned werden, und lösen bei Treffern Alerts aus [191].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	Die Daten MÜSSEN kontinuierlich ausgewertet werden.	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	109	110	111	112

Begründung	Sigma Regeln können frei konfiguriert und getuned werden [191].	Die Sigma-Regeln in ElastAlert können mittels einer konfigurierbaren Buffer-Time auch bereits geprüfte Protokolldaten erneut in Auswertungen berücksichtigen [185].	Security Onion bietet die Möglichkeit, Signaturen über Threat Intelligence Anbieter zu integrieren, zu denen Integrationen mit dem Präfix "ti_" verfügbar sind [175].	Alerts können in der Security Onion Console zu Cases eskaliert und so qualifiziert werden. Über die Analyzer-Funktionen wird die Qualifizierung unterstützt [193].
Erfüllt?	Ja	Ja	Ja	Ja
Anforderung	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	Die SRE MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifizierter SRE) hindeuten. Die zur Angriffserkennung eingesetzten Systeme sollten, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.
Modalverb	MUSS	MUSS	MUSS	MUSS
Seite	12	12	12	12
Quelle	OH-SzA	OH-SzA	OH-SzA	OH-SzA
Nummer	114	115	116	121

Anlage 12 Prüfmatrix n8n

Übergreifende Anforderungen

Begründung	n8n bietet Integrationen mit mehreren großen Threat Intelligence Anbietern, wodurch in n8n verarbeitete Ereignisse gegen deren Signaturen geprüft werden können vgl. [194].
Erfüllt?	Ja
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche [...], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Reaktion

Begründung	n8n bietet eine Vielzahl vordefinierter Nodes bzw. Integrationen, die den Detektionssystemen als Schnittstelle für die Meldung von Ereignissen zur Reaktion dienen können [195]. Für Systeme ohne vordefinierte Nodes können Nodes selbst erstellt werden [196].
Erfüllt?	Ja
Anforderung	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.
Modalverb	MUSS
Seite	14
Quelle	OH-SzA
Nummer	224

Begründung	n8n kann über eine Vielzahl von Cybersecurity Integrationen Aktionen z.B. in Microsoft Entra ID oder diversen Firewalls auslösen, um betroffene Accounts zu sperren oder Netzwerkzugriffe zu blockieren [194].	Die Stop And Error Node kann genutzt werden, um den Workflow unter bestimmten Bedingungen abzubrechen [197]. Die Bedingungen können in einer vorgeschalteten If-Node geprüft [198] und so gestaltet werden, dass durch den Workflow die kritische Dienstleistung nicht relevant beeinträchtigt wird.	Workflows können in n8n ohne automatisierte Trigger Node erstellt und manuell ausgeführt werden [199]. Hierfür muss die Manual trigger Node in den Workflow eingebaut werden [200].
Erfüllt?	Ja	Ja	Ja
Anforderung	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.
Modalverb	SOLL	MUSS	SOLL
Seite	14	14	14
Quelle	OH-SzA	OH-SzA	OH-SzA
Nummer	230	231	232

Anlage 13 Prüfmatrix Shuffle

Übergreifende Anforderungen

Begründung	Shuffle bietet Integrationen mit mehreren großen Threat Intelligence Anbietern, wodurch in Shuffle verarbeitete Ereignisse gegen deren Signaturen geprüft werden können [76].
Erfüllt?	Ja
Anforderung	Grundsätzlich gilt für die Gesamtheit aller Bereiche […], dass die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN
Modalverb	MUSS
Seite	8
Quelle	OH-SzA
Nummer	4

Anforderungen zur Reaktion

Begründung	Shuffle bietet eine Vielzahl vordefinierter Apps bzw. Integrationen, die den Detektionssystemen wie Wazuh oder OpenSearch als Schnittstelle für die Meldung von Ereignissen zur Reaktion dienen können [76]. Für Systeme ohne vordefinierte App können Nodes selbst erstellt werden [76].
Erfüllt?	Ja
Anforderung	Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.
Modalverb	MUSS
Seite	14
Quelle	OH-SzA
Nummer	224

Begründung	Shuffle kann über eine Vielzahl von Apps Aktionen z.B. in EDR-Lösungen oder Firewalls auslösen, um Dateien zu löschen oder Netzwerkzugriffe zu blockieren [76].	Mittels Conditionals kann der Ablauf eines Workflows auf Bedingungen geprüft und so gestaltet werden, dass durch den Workflow die kritische Dienstleistung nicht relevant beeinträchtigt wird [108]. Für eine zusätzliche manuelle Prüfung von Aktionen vor der Ausführung kann mit dem Trigger "User Input" eine Prüfung durch einen Menschen auf potenzielle Beeinträchtigung der kritischen Dienstleistung erfolgen [76].	Der Trigger "User Input" kann für die manuelle Auslösung von Aktionen in Workflows integriert werden [76].	
Erfüllt?	Ja	Ja	Ja	
Anforderung	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.	
Modalverb	SOLL	MUSS	SOLL	
Seite	14	14	14	
Quelle	OH-SzA	OH-SzA	OH-SzA	
Nummer	230	231	232	

Anlage 14 Suricata-Decoder in Wazuh

```
<decoder name="suricata-custom">
   <program_name>suricata</program_name>
</decoder>
<decoder name="suricata-custom1">
   <parent>suricata-custom</parent>
   <regex type="pcre2">^.*suricata\[\d+\]:\s\[([a-zA-Z]+)\]</regex>
   <order>action</order>
</decoder>
<decoder name="suricata-custom1">
   <parent>suricata-custom</parent>
   <regex type="pcre2">\[\d+:\d+:\d+\]\s([^\[]+)</regex>
   <order>ids_rule</order>
</decoder>
<decoder name="suricata-custom1">
   <parent>suricata-custom</parent>
   <regex type="pcre2">\[Classification:\s(.+)\]\s\[Priority:\s(\d)\]</regex>
   <order>ids_classification, ids_prio</order>
</decoder>
<decoder name="suricata-custom1">
   <parent>suricata-custom</parent>
   <regex type="pcre2">{(\S+)}\s(\d+\.\d+\.\d+\.\d+):(\d+)\s-
>\s(\d+\.\d+\.\d+\.\d+):(\d+)</regex>
   <order>protocol, src_ip,src_port, dst_ip, dst_port</order>
</decoder>
```

Anlage 15 Suricata Rule in Wazuh

```
<group name="syslog,ids,">
  <rule id="100010" level="5">
    <decoded_as>suricata-custom</decoded_as>
    <description>Suricata alerts from OPNsense.</description>
  </rule>
</group>
```

Anlage 16 Realprüfung Wazuh

Übergreifend

Nummer	Modalverb	Erfüllt?	Begründung
4	MUSS	Ja	Wazuh bietet über API-Integrationen die Möglichkeit, Signaturen in Form von IoCs über Drittanbieter-Integrationen abzurufen. Das Ruleset kann immer aktuell gehalten werden und wird mit jedem Wazuh Update aktualisiert.

Protokollierung

Nummer	Modalverb	Erfüllt?	Begründung
8	MUSS	Ja	Wazuh hat im Prototyp die Fähigkeit demonstriert, Protokolldaten mittels des Wazuh Agenten zu erheben oder per Syslog zu empfangen, zu speichern und zur Auswertung bereitzustellen, um SRE zu

Nummer	Modalverb	Erfüllt?	Begründung
			erkennen.
9	KANN	Nein	Der Wazuh Agent unterstützt zwar Geräte in der Aufzeichnung von Protokolldaten, muss aber auf den Geräten selbst installiert sein. Wazuh erhebt keine eigenen Protokolldaten über Drittsysteme.
11	MUSS	Ja	Die Decoder, wie der für Suricata erstellte Decoder im Prototyp, können Felder verwerfen oder maskieren.
13	SOLL	Ja	Der Wazuh Agent kann als zusätzliche Maßnahme zur Malwareerkennung und Dateiintegritätsüberwachung oder Active Response dienen.
35	MUSS	Ja	Über den Wazuh Agenten können zusätzliche Ereignisse auf Systemebene wie Dateiänderungen protokolliert werden. Somit kann er als zusätzliches System zur Protokollierung dienen.
37	MUSS	Ja	Über die Wazuh-Decoder werden die Datums- und Zeitformate der Protokolldaten wie im Prototypen normalisiert.

Nummer	Modalverb	Erfüllt?	Begründung
42	MUSS	Ja	Eine Möglichkeit zur gezielten Löschung von Protokolldaten ist in Wazuh nicht gegeben, ein rollenbasiertes Berechtigungskonzept ermöglicht die Steuerung von Verwaltungsrechten.
43	MUSS	Ja	Der Wazuh Server dien im Prototypen als zentrale Stelle zur Speicherung aller gesammelten Protokolldaten.
47	MUSS	Ja	Die Protokolldaten werden über die Wazuh Decoder gefiltert und normalisiert, im Wazuh Dashboard aggregiert und korreliert.
48	MUSS	Ja	Die Protokolldaten werden einerseits über die Wazuh Rules ausgewertet, andererseits zur direkten Ansicht im Wazuh Dashboard verfügbar gemacht.
49	KANN	Ja	Die Wazuh Archives speichern die Protokolldaten in normalisierter Form, wobei die unbearbeiteten Originaldaten im Feld "full_log" verfügbar bleiben.

Detektion

Nummer	Modalverb	Erfüllt?	Begründung
55	MUSS	Ja	Das MITRE ATT&CK Framework ist auf der Startseite des Wazuh Dashboards verlinkt. Dort kann im Reiter "Intelligence" die

Nummer	Modalverb	Erfüllt?	Begründung
			Bedrohungslandschaft eingesehen werden, den Rules kann die Information beigefügt werden (und ist es im Standard-Regelwerk), zu welcher Technique die Rule gehört. So kann über das Dashboard die Bedrohungslandschaft der RECPLAST bestimmt sowie passende Detektionsmaßnahmen dafür definiert und ausgewählt werden.
57	KANN	Ja	Durch Bereitstellung der ATT&CK Matrix auf der Startseite von Wazuh kann diese als standardisierte Methode verwendet werden.
80	MUSS	Ja	Die sicherheitsrelevanten Vorfälle beziehungsweise Alerts aus treffenden Rules werden auf dem Wazuh Dashboard zur Auswertung bereitgestellt. Die weiteren Meldungen der betroffenen IT-Systeme sind über die Wazuh Archives auswertbar.
84	MUSS	Ja	Die File Integrity Monitoring Funktion ist von der Dashboard-Startseite zugreifbar, die Alerts werden auf dem Dashboard abgebildet.
85	MUSS	Ja	Die definierten File Integrity Monitoring Rules lösen, wie alle anderen Rules, bei passenden Ereignissen Alerts aus.
87	MUSS	Ja	Die in Wazuh per Agent oder Syslog

Nummer	Modalverb	Erfüllt?	Begründung
			eingebrachten Protokolldaten werden mittels des Rulesets kontinuierlich überwacht und ausgewertet.
88	KANN	Ja	Die eingelieferten Protokolldaten werden mittels der definierten Rules überwacht und ausgewertet, die bei Treffern unmittelbar Alerts erzeugen. Über Integrationen in der Konfiguration des Wazuh Servers kann eine Alarmierung an oder über Drittsysteme wie über Mail oder wie im Prototypen Shuffle erfolgen.
93	MUSS	Ja	Mittels der File Integrity Monitoring Funktion und der auf der Startseite des Dashboards verorteten VirusTotal-Integration können neue oder verdächtige Dateien auf Schadcode geprüft werden. Die Verwaltung erfolgt zentral vom Wazuh Server.
95	MUSS	Nein	Wazuh bietet keine NIDS-Funktionalität.
97	MUSS	Ja	Das Wazuh Dashboard stellt die Alerts gruppiert nach Kritikalität dar, die regelmäßig kontrolliert werden können.
98	MUSS	Ja	Das Ruleset von Wazuh wird mit jedem Release aktualisiert und kann manuell angepasst werden. Darüber hinaus können Signaturen wie IoCs über Drittanbieter-Integrationen abgerufen und in Listen zur Auswertung in eigenen Rules gespeichert

Nummer	Modalverb	Erfüllt?	Begründung
			werden.
99	MUSS	Ja	In Wazuh können Signaturen wie IoCs über Drittanbieter-Integrationen wie Maltiverse abgerufen werden. Darüber hinaus werden die Bedrohungsinformationen aus MITRE ATT&CK über das MITRE ATT&CK Modul zur Verfügung gestellt.
108	MUSS	Ja	Der Wazuh Servermit seinem Ruleset dient als zentrale Komponente zur Erkennung und Auswertung sicherheitsrelevanter Ereignisse.
109	MUSS	Ja	Der Wazuh Server zeichnet die Daten in Wazuh Indexern auf und setzt sie mittels des Rulesets und Decodern in Bezug zueinander. Die ausgelösten Alerts, also sicherheitsrelevanten Vorgänge, werden im Wazuh Dashboard sichtbar gemacht.
110	MUSS	Ja	In Wazuh Archives werden alle eingelieferten Protokolldaten gespeichert, unabhängig davon, ob sie eine Regel auslösen. Diese können im Wazuh Dashboard über die Discover-Funktion eingesehen und ausgewertet werden.
111	MUSS	Ja	Der Wazuh Server wertet alle eingelieferten Protokolldaten kontinuierlich mittels der

Nummer	Modalverb	Erfüllt?	Begründung
			definierten Rules aus.
112	MUSS	Ja	Im Wazuh Server kann mittels der Option "log_alert_level" zentral konfiguriert werden, ab welcher Kritikalität eines Alerts dieser einen Alarm auslöst.
114	MUSS	Ja	Das Ruleset von Wazuh ist frei einsehbar, anpassbar und erweiterbar.
115	MUSS	Ja	Bereits überprüfte Protokolldaten befinden sich in den Wazuh Archives. Über entsprechend gestaltete Queries und Visualisierungen können diese erneut hinsichtlich sicherheitsrelevanter Ereignisse automatisiert durchsucht werden, wobei ein manuelles Auslösen der automatisierten Suche durch Öffnen des entsprechenden Dashboards notwendig ist.
116	MUSS	Ja	Der Wazuh Server holt aktuelle Schwachstelleninformationen aus dem Wazuh Vulnerability Feed laufend ein, wobei das Update-Intervall auf dem Wazuh Server mittels der Option "feed-update-interval" konfiguriert werden kann.
121	MUSS	Ja	Regeln können in Wazuh klassifiziert werden und so im Falle höherer Klassifizierungen einen Alert als bereits qualifiziert ausweisen.

Reaktion

Nummer	Modalverb	Erfüllt?	Begründung
224	MUSS	Ja	Wazuh löst bei erkannten SRE einen Alert aus. Es können systembasierte Active Response Skripte definiert werden.
230	SOLL	Ja	Active Response Regeln können in Wazuh so konfiguriert werden, dass sie ab einer definierten Kritikalität des SRE greifen.
231	MUSS	Ja	Wazuh bietet die Möglichkeit, einzelne Systeme über White Lists von der Active Response auszuschließen oder in der Konfiguration des Agenten auf dem Zielsystem gänzlich zu deaktivieren.
232	SOLL	Ja	Im Bedarfsfall kann über die Wazuh API ein Active Response Command manuell ausgeführt werden, was beispielsweise in der Shuffle App genutzt werden kann.

Anlage 17 Realprüfung Shuffle

Übergreifend

Nummer	Modalverb	Erfüllt?	Begründung
4	MUSS	Ja	Über die Funktion "Parse file ioc" der Shuffle Tools Node können IOCs einfach automatisiert aus Dateien extrahiert und über Apps der Kategorie "Intel" wie MISP oder Recorded Future eingeholt werden. Die Verteilung an die Detektionssysteme kann mit deren Apps oder API-Aufrufe erfolgen.

Reaktion

Nummer	Modalverb	Erfüllt?	Begründung
224	MUSS	Ja	Eine automatische Meldung des Ereignisses von Wazuh an Shuffle funktioniert, dort kann mit einer Blockierung des betreffenden Clients an der Firewall reagiert werden.
230	SOLL	Ja	Shuffle kann automatisiert angriffsbedingte Störungen durch z.B. Isolierung des betreffenden Clients treffen, sowie das SRE vorab inhaltlich prüfen.
231	MUSS	Ja	Durch den Einbau eines Filters z.B. auf das Client-Netzwerk, kann eine relevante Beeinträchtigung des gesamten IT-Betriebs z.B. durch Isolierung eines kritischen Servers vermieden werden. Für

Nummer	Modalverb	Erfüllt?	Begründung
			eine zusätzliche manuelle Prüfung kann der Trigger "User Input" innerhalb des Workflows für eine Prüfung durch einen Menschen platziert werden.
232	SOLL	Ja	Der Trigger "User Input" kann innerhalb eines Workflows platziert werden, sodass Daten manuell geprüft werden können.

Anlage 18 Realprüfung Suricata

Übergreifend

Nummer	Modalverb	Erfüllt?	Begründung
4	MUSS	Ja	Suricata bietet die Möglichkeit, frei Signaturen beziehungsweise Regeln zu definieren. Viele Regelwerke sind frei im Internet zum Download verfügbar, so beispielsweise die in OPNSense integrierten Standard-Regelwerke, die im Rahmen des Prototypen heruntergeladen werden konnten.

Protokollierung

Nummer	Modalverb	Erfüllt?	Begründung
9	KANN	Ja	Mittels einer entsprechend definierten Suricata-Regel, die nur alarmiert/protokolliert anstelle zu blockieren, kann das Netzwerkverhalten von anderen Systemen zur Angriffserkennung protokolliert werden, ohne sie zu beeinträchtigen.
13	SOLL	Ja	Suricata dient im Prototyp als Maßnahme, die sowohl Detektion (Alarmierung auf Regelbasis) als auch Reaktion (Blockieren von Datenverkehr auf Regelbasis) ermöglicht.

Detektion

Nummer	Modalverb	Erfüllt?	Begründung
95	MUSS	Ja	Suricata ist ein NIDS und wurde innerhalb des Prototyps an dem definierten Übergangspunkt zwischen allen internen und externen Netzen verortet.

Anlage 19 Interviewprotokoll mit Splunk

Frage: In der Einrichtung des Prototyps ergaben sich Herausforderungen in der Erstellung von Detektionsregeln in Wazuh, da das Regelwerk durch die Bearbeitung von XML-Dateien gepflegt werden sowie nach Änderungen der Wazuh Server neu gestartet werden muss. Bieten kommerzielle SzA Vorteile in der Pflege des Regelwerks und Umfang der mitgelieferten Standardregeln gegenüber FOSS?

Antwort: Grundsätzlich ist die Verwendung von XML-Dateien für die Erstellung von Regeln kein schlechtes Vorgehen, da XML-Dateien den Vorteil der Versionierbarkeit in Systemen wie Git bieten. Splunk speichert Regeln bzw. Use Cases selbst auch in XML-Dateien, diese können allerdings mit einem grafischen Drag-and-Drop Editor erstellt, in Splunk Search Processing Language geschrieben oder direkt per API hochgeladen werden. Dabei sind Neustarts des Servers nicht erforderlich, im Gegenteil können Regeln erstellt und mit bereits gespeicherten Protokolldaten korreliert werden, um passende Ereignisse in der Vergangenheit zu detektieren, ohne auf erneutes Auftreten der gesuchten Ereignisse warten oder Testdaten verwenden zu müssen. Bezüglich des mitgelieferten Standardregelwerks beinhaltet die Splunk Security Essentials App über 1500 standardmäßig enthaltene Regeln, die sowohl vom Splunk Research Team selbst definiert oder aus Regeln der Splunk Community inspiriert sind. Die Regeln sind nach MITRE ATT&CK Techniken und Taktiken, Reifegrad, Komplexität und Wahrscheinlichkeit für False Positives kategorisiert. Auch verhaltensbasierte Regeln auf Basis maschinellen Lernens sind enthalten.

Frage: In der Einrichtung des Prototyps ergaben sich Herausforderungen in der Erstellung von Workflows im Shuffle SOAR, da die Dokumentation ein anderes Verhalten von Workflow-Elementen suggerierte, als es real der Fall war. Kann bei der Verwendung von kommerziellen SzA von einer umfangreichen, präzisen und aktuellen Dokumentation ausgegangen werden bzw. ist die Pflege der Dokumentation eine Priorität für Anbieter kommerzieller SzA?

Antwort: Splunk verfolgt als Unternehmensphilosophie die Aspekte „Open“ und

„Community“, wodurch ein großes Augenmerk auf eine ausführliche Dokumentation mit Beispielen liegt. Die Dokumentation ist öffentlich auch als Nicht-Kunde einsehbar und wurde dadurch auch in große KI-Sprachmodelle eingelesen, die die Inhalte der Dokumentation angelernt haben. Die Dokumentation ist sehr ausführlich auch in Bezug auf Limitierungen und Grenzen von Splunk, wodurch beispielsweise Einschränkungen in parallel laufenden Suchvorgängen und Edge Cases wie mangelnde freie Ports auf Linux-Systemen beschrieben sind. So soll das Troubleshooting erleichtert und möglichst einfach gestaltet werden. Die Dokumentation wird durch ein dediziertes Technical Documentation Team gepflegt, das aus vielen Mitarbeitern besteht, die auf Basis der laufenden Änderungen in den Systemen und auf Rückfragen von Nutzern hin dokumentieren. Die öffentliche Einsehbarkeit der Dokumentation ist allerdings kein grundsätzliches Merkmal von kommerziellen Systemen zu Angriffserkennung, es gibt manche Anbieter, die ihre Dokumentation nur Kunden zugänglich machen.

Frage: Die Einsparung von Lizenzkosten stellt einen offensichtlichen Vorteil von FOSS gegenüber kommerziellen SzA insbesondere bei KMU dar. Eignen sich kommerzielle SzA für Unternehmen, in denen mit eng begrenztem IT-Budget gearbeitet werden muss? Wenn ja, welche Maßnahmen können zur Kostenreduktion dienen, um ähnliche oder gar geringere Kosten als mit FOSS zu erreichen?

Antwort: Zwar können FOSS Lösungen ohne Lizenzkosten betrieben werden, jedoch sind diese nicht der einzige Anteil an den Kosten des Betriebs eines Systems zur Angriffserkennung. Um beide Varianten richtig vergleichen zu können, müsste eine Vollkostenrechnung durchgeführt werden. Grundsätzlich ist es mit einer Vollkostenbetrachtung eher ein Mythos, dass FOSS billiger ist. Auf der einen Seite muss die „Total Cost of Ownership“ betrachtet werden, die nicht nur Lizenzkosten, sondern auch Kosten für den Support, die darunterliegende Infrastruktur und das zum Betrieb erforderliche Fachpersonal berücksichtigt. Bei FOSS muss dabei mitberücksichtigt werden, ob eigene Anpassungen an der Lösung erfolgen müssen, um beispielsweise akute Schwachstellen zu schließen.

Hier müssen entweder über einen Servicevertrag mit einem Dienstleister entsprechende Verantwortungen für Updates und Patches geklärt, oder diese selbst erstellt werden. Das Risiko selbst aktiv werden zu müssen steigt mit geringerem Verbreitungsgrad und damit kleinerer Entwicklungscommunity der FOSS Lösung. Auch die Eigenentwicklung von Integrationen ist ein wichtiger Aspekt, da die Schwierigkeit der Integration mit Drittsystemen mit deren Anzahl ansteigt. Eine FOSS Lösung hat prinzipbedingt tendenziell weniger Ressourcen zur Verfügung, die in die Integration mit anderen Systemen genutzt werden können, als kommerzielle Anbieter. Auch der Aspekt des Lieferketten- beziehungsweise Supply Chain Managements ist wichtig. So kann ohne Supportverträge, die auch für FOSS Lösungen mit Kosten verbunden sind, kaum eine Kontrolle der Lieferkette für die Systeme stattfinden. Daher sind Supportverträge mit verlässlichen Partnern unerlässlich, unabhängig davon, ob FOSS oder kommerzielle Lösungen zum Einsatz kommen. Lizenzkosten machen so in der Vollkostenbetrachtung nach Erfahrungswerten von Splunk oft weniger als 20% aus. Splunk selbst hat unter anderem einen speziellen Vulnerability Reporting Prozess, Service Level Agreements und ein definiertes Software Lifecycle Management, die den Umgang mit den genannten Problemfeldern unterstützen. In der Gesamtkalkulation stehen kommerzielle Lösungen so nicht mehr schlecht gegenüber FOSS Lösungen da. So hat Splunk beinahe 900 Kunden, die jährlich mehr als eine Millionen Euro für Splunk ausgeben. Bei Ausgaben dieser Größenordnung kann davon ausgegangen werden, dass die meisten Unternehmen sehr genau durchgerechnet haben, ob es nicht günstigere Alternativen gibt. Zur Kostenoptimierung ist ein starker Trend zur Nutzung von Cloud-Lösungen ersichtlich, weil die Verantwortung für den Betrieb der Lösung und ihrer Infrastruktur weitestmöglich abgegeben werden soll, sofern das der Risikoappetit der Organisationen zulässt. So kann Personal für den Betrieb gespart und die erforderlichen Kernkompetenzen für die Nutzung der SzA aufgebaut und genutzt werden.

Frage: Eine ständige Herausforderung in der IT ist die Verfügbarkeit von Fachpersonal. Um personelle Aufwände in Betrieb und Nutzung von SzA zu reduzieren, können SzA über Software-as-a-Service Angebote ohne interne

Betriebsaufwände oder im Komplettpaket als Managed Security Service Angebote, in denen auch die inhaltliche Nutzung der SzA durch einen Dienstleister erfolgt, bezogen werden. Sind bei kommerziellen SzA SaaS- und MSSP-Angebote vergleichsweise mehr oder weniger verfügbar als mit FOSS?

Antwort: Bei Betrachtung des Marktes sind unter den MSSP-Anbietern sehr wenige verfügbar, die auf FOSS setzen. Insbesondere die großen Anbieter setzen primär auf ein oder zwei kommerzielle SzA, die angeboten werden. Das Partnernetzwerk von Splunk umfasst global ca. 460 Partnerunternehmen, die Beratungs- und MSSP-Leistungen für Splunk anbieten. Mit der Nutzung von SaaS und MSSP können interne Betriebsaufwände stark reduziert werden, es gibt jedoch immer Teile, die intern gemacht werden müssen. So muss der MSSP-Dienstleister gesteuert, die Architektur der SzA geplant und die Strategie zu deren Nutzung im Unternehmen selbst gepflegt werden. Auch bei Änderungen der IT-Umgebung sind vertragliche Anpassungen bei MSSP erforderlich, um sicherzustellen, dass auch neue Systeme im Rahmen der Angriffserkennung überwacht werden. Bezüglich SaaS hat Splunk die Erfahrung gemacht, dass SaaS-Kunden die Lösung langfristig nutzen.

Frage: Die Integration von FOSS SzA mit anderen SzA hat sich im Falle von Shuffle als sehr flexibel erwiesen, erfordert jedoch manuellen Aufwand, da alle Systemtypen von anderen FOSS-Projekten stammen. Bieten kommerzielle SzA Vorteile in der Integration mit anderen SzA, beispielsweise durch eigene voll integrierte Ökosysteme wie SIEM und SOAR, EDR und SIEM, … oder gepflegte Schnittstellen zu Ökosystemen von Drittanbietern?

Antwort: Erfahrungsgemäß kostet jede Integration eines SzA mit anderen Systemen fünf bis zehn Dienstleistungstage von Entwicklern zur Erstellung sowie laufenden Pflegeaufwand, um möglichst aufwandsfrei genutzt werden zu können. Bei solchen Aufwänden sind bei kostenfreien FOSS SzA tendenziell weniger schlüsselfertige Integrationen verfügbar als bei kommerziellen Anbietern, die wie im Fall von Splunk genau dafür Budget planen. Zwar kann auch von kommerziellen Anbietern nicht jede denkbare Integration erwartet werden, das verfügbare Ressourcenvolumen für die Pflege der Integrationen ist jedoch

deutlich größer. Splunk erstellt Integrationen einerseits selbst, hat aber auch Partneranbieter, die selbst Integrationen ihrer SzA für Splunk erstellen und eine Community aus Partnerunternehmen, die durch sie selbst erstellte Integrationen mit der gesamten Community teilen. Wie bei FOSS gilt auch hier: Je größer die Community hinter einem System ist, desto größer ist der Kollaborationseffekt.

Frage: Viele Unternehmen setzen zur Reduktion interner Betriebsaufwände nicht nur bei SzA auf SaaS, sondern nutzen Cloud-Umgebungen auch für die Bereitstellung weiter Teile von oder ihrer gesamten IT-Infrastruktur. Kann bei kommerziellen SzA von einer einfacheren Integration und Kompatibilität von Cloud-Umgebungen ausgegangen werden als bei FOSS?

Antwort: Die meisten SzA, unabhängig davon ob FOSS oder kommerziell, können sich die Protokolldaten von Cloud-Umgebungen über deren APIs herunterladen. Im Falle von Splunk als kommerzielles SzA wird dies aber nicht nur einfach unterstützt, sondern der kosteneffizienteste Weg für den Kunden gesucht. Dies wird bei Splunk so umgesetzt, dass die Integration von Cloud-Umgebungen auf Basis eigens dafür betriebene Collector-Infrastruktur von Splunk ermöglicht wird, die Verbindungen zu den Cloud-Anbietern bündelt und so kosteneffizienter bedient, als wenn die Kunden sich alle separat mit dem Cloud-Anbieter verbinden würden. Diese Möglichkeit ist für die großen Cloud-Anbieter, darunter Amazon Web Services und Microsoft Azure, gegeben.

Frage: Ergeben sich in der Verwendung kommerzieller SzA weitere Vorteile gegenüber FOSS?

Antwort: Ein wichtiger Punkt bei der Verarbeitung großer Datenmengen in einem SIEM ist die Skalierbarkeit. Kommerzielle SzA legen, da sie auch in großen IT-Infrastrukturen und kritischen Umgebungen eingesetzt werden, ein großes Augenmerk auf möglichst einfache und große Skalierbarkeit sowie Ausfallsicherheit. Darüber hinaus pflegen viele kommerzielle Anbieter, darunter Splunk, ein Schulungs- und Zertifizierungsprogramm, was die Ausbildung und Suche qualifizierten Personals erleichtert. Splunk verfügt über ein Ökosystem von Dienstleistungs-Partnern, die ebenfalls zertifiziert werden und Leistungen in

Beratung, Implementierungshilfe, Betrieb und Nutzung der SzA anbieten. Durch dieses Ökosystem können interne Aufwände in vielen Bereichen stark reduziert werden, während die Betreuung von FOSS tendenziell mehr Ressourcen in Anspruch nimmt. Splunk selbst verfolgt einen Plattform-Gedanken, der die Toolchain zur Überwachung verschiedenster Systeme in eine zentrale gepflegte Plattform konsolidieren soll. So können verteilte Monitoring-Lösungen für spezifische Systeme abgeschafft und mit Splunk ersetzt werden. Was explizit nicht der Fall ist, ist dass von einer grundlegend höheren Sicherheit von kommerziellen SzA gegenüber FOSS ausgegangen werden kann. Auch in kommerziellen SzA können schwerwiegende Fehler enthalten sein, genauso wie in FOSS langlebige Sicherheitslücken bekannt werden. Dennoch kann es der Fall sein, dass die Akzeptanz und das Vertrauen besonders seitens des Managements in marktführende kommerzielle Lösungen größer ist, als bei FOSS.

Frage: Unter welchen Bedingungen würden Sie KMU einen Einsatz von FOSS, unter welchen einen Einsatz von kommerziellen SzA empfehlen und weshalb?

Antwort: Grundsätzlich sind die Hauptkosten von SzA nicht die Lizenzkosten, sondern das Personal und die Prozesse dahinter. Erfahrungsgemäß liegt der Anteil der Lizenzkosten zwischen zehn und zwanzig Prozent der Gesamtkosten, der Rest verteilt sich auf die Betriebskosten. Daher sollte die Entscheidung für FOSS oder kommerzielle Lösungen keineswegs rein auf Basis der Lizenzkosten fallen. Gerade als KMU sollte überlegt werden, ob man sich nicht eher an großen Firmen, die teilweise schon seit Jahrzehnten ein SOC betreiben und durchweg auf kommerzielle SzA setzen, orientieren will. Es gab in der Vergangenheit eine Vielzahl von Open Source SIEM Lösungen, die nach einigen Jahren nach und nach aus der Entwicklung gefallen sind. Daher sollte gut überlegt werden, ob man eher den aufwendigeren Weg der Nutzung und Integration von FOSS gehen möchte, anstatt standardisierte, gepflegte und verbreitete Technologie heranzuziehen. Oft ist es auch der Fall, dass KMU bereits viel Geld für Tools ausgeben, die schlecht konfiguriert sind, nicht aktiv genutzt werden oder anderweitig suboptimal verwendet werden und anstelle derer Verbesserung eher

mehr neue Tools eingekauft werden. Somit sollte eher der Bestand betrachtet und dort Optimierungs- und Konsolidierungspotenzial gesucht werden, da die Integration der Bestandslösungen in neu eingeführte SzA auch ein Kostentreiber ist. So sollte eher eine Lösung gesucht werden, die möglichst gut durch Dienstleister unterstützt wird und gepflegte Integrationen bietet, sodass Betriebsaufwände möglichst gering gehalten können.

Verzeichnis der Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CSF	Cybersecurity Framework
EDR	Endpoint Detection and Response
FOSS	Free and Open Source Software
HIDS	Hostbasiertes Intrusion Detection System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
KMU	Kleine und mittlere Unternehmen
NIDS	Netzbasiertes Intrusion Detection System
NIS2UmsuCG	Gesetz zur Umsetzung von EU NIS2 und Stärkung der Cybersicherheit
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OH-SzA	Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
SIEM	Security Information and Event Management
SIRT	Security Incident Response Team, Sicherheitsvorfall-Team
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SRE	Sicherheitsrelevante(s) Ereignis(se)
SzA	Systeme zur Angriffserkennung
XDR	Extended Detection and Response

Thesen

Thema der Arbeit: Umsetzbarkeit der OH-SzA des BSI mittels Open Source Lösungen

Bearbeiter: Lukas Petrič

Thesen:

1. Die Anforderungen der OH-SzA des BSI sind mittels FOSS SzA bis zur Erreichung des Umsetzungsgrad 4 erfüllbar.
2. Ergänzend zu den technischen SzA sind umfangreiche organisatorische Maßnahmen zur Erfüllung der Anforderungen erforderlich.
3. KMU sollten die Entscheidung für FOSS oder kommerzielle SzA nicht rein auf Basis der Lizenzkosten, sondern nach Durchführung einer Vollkostenbetrachtung fällen.
4. Nur durch den Wegfall von Lizenzkosten kann nicht davon ausgegangen werden, dass der Einsatz von FOSS automatisch kostengünstiger als kommerzielle SzA ist.
5. Neben der Wahl der SzA sollte auch die Entscheidung für ein Betriebsmodell der SzA und des SOC unter Vollkostenbetrachtung und Beachtung weiterer Faktoren getroffen werden.
6. Die Entscheidung für ein Betriebsmodell und die Art der SzA ist maßgeblich mit abhängig von der Motivation des Unternehmens, SzA einzuführen.
7. Insbesondere bei der Verwendung von FOSS sollte aufgrund möglicher Dokumentationslücken die Konfiguration der SzA sorgfältig getestet werden.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Arbeit entspricht der elektronischen Fassung. Ich stimme zu, dass eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels Anti-Plagiatssoftware zu ermöglichen.

Kirchheim unter Teck, 27.08.2024 

Ort, Datum Unterschrift