Kolloquium zur Master-Thesis

Umsetzbarkeit der OH-SzA des BSI mittels Open Source Lösungen

Lukas Petrič

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

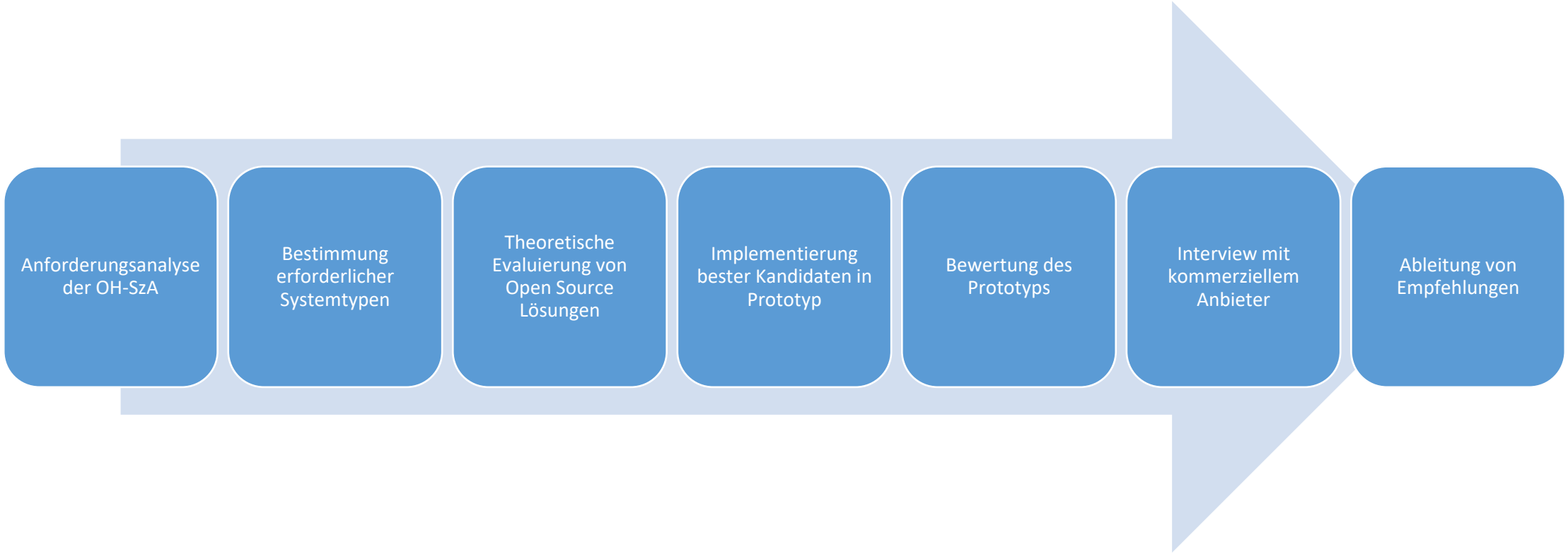
Motivation

- SzA bislang nur für Betreiber kritischer Infrastrukturen gefordert
- IT-Sicherheit rückt immer weiter in den Fokus des Gesetzgebers
  - IT-Sicherheitsgesetz 2.0
  - NIS2
- Künftig könnten Unternehmen abseits von KRITIS zum Einsatz von SzA verpflichtet werden
- Schwellwerte des NIS2UmsuCG können auch KMU umfassen [1]
- Herausforderung: KMU besonders in IT oft kostenoptimiert, kommerzielle SzA aber kostenintensiv

OH-SzA: Allgemeines

- §8a Abs. 1a BSIG fordert für KRITIS-Betreiber seit Mai 2023 den Einsatz von **Systemen zur Angriffserkennung (SzA)** [2] …
  - „durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“ [2]
- Konkretisiert durch „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ [3] des BSI
  - Verweist zu Anforderungen auf IT-Grundschutz-Bausteine
  - Beinhaltet:
    - Anforderungen zur Protokollierung, Detektion, Reaktion und übergreifend
    - Vorgaben zur Nachweiserbringung und Umsetzungsgradmodell

Vorgehensweise



Begrifflichkeiten: OH-SzA Begriffe

- **Protokollierung**: Sammlung der Datengrundlage für die Angriffserkennung [3]
- **Detektion**: Erkennung sicherheitsrelevanter Ereignisse u.a. in den Protokolldaten [3]
- **Reaktion**: Verhinderung der Auswirkungen von Angriffen [3]
- **Logging**: Gängiger Begriff synonym zu „Protokollierung“
  - „Protokollereignis“, „Protokollmeldung“, „Protokollierungsdaten“ → „Log“

Begrifflichkeiten: Systeme zur Angriffserkennung

- **Security Information and Event Management**: Automatische Korrelation und Analyse von Protokolldaten auf Sicherheitsvorfälle [4]
- **Network Intrusion Detection System**: Überwachen den Datenverkehr im Netzwerk auf verdächtige Aktivitäten [5]
- **Endpoint Detection and Response**: Überwachung von Endpunkten auf Bedrohungen und automatische Reaktion auf diese [6]
- **Security Orchestration, Automation and Response**: Plattformen, die Sicherheitswerkzeuge integrieren und automatisierte Arbeitsabläufe über diese hinweg ausführen können [7]
- **Security Operations Center**: Team aus IT-Sicherheitsexperten für die Erkennung von Sicherheitsvorfällen, deren Analyse und Reaktion auf sie [8]

OH-SzA: Verwandte Regularien

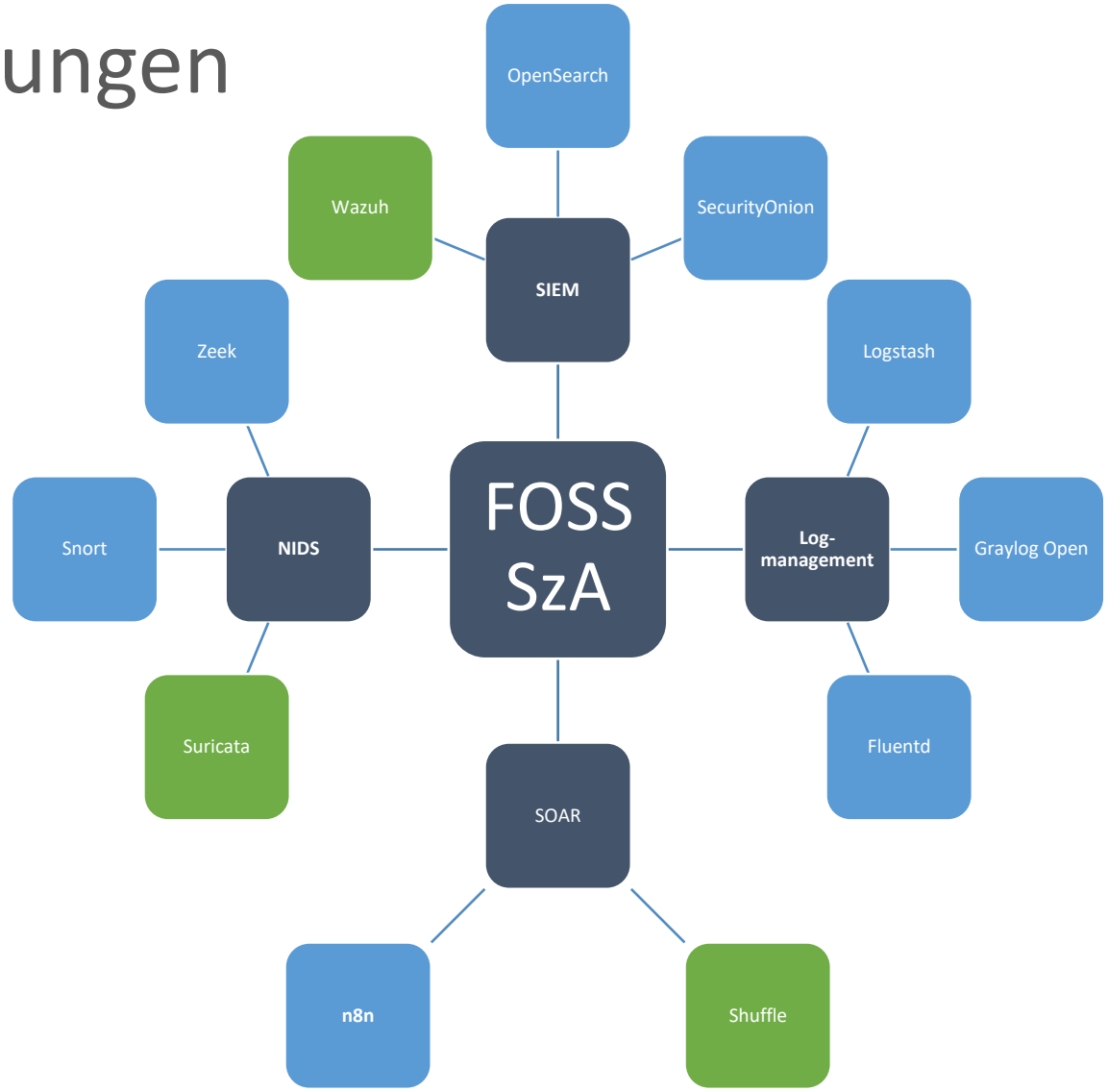
- ISO27001 / ISO27002
  - Definiert Rahmen für Informationssicherheits-Managementsysteme in Einführung, Betrieb und kontinuierlicher Verbesserung
  - Für Unternehmen aller Größen und Sektoren universell konzipiert
  - Zertifizierung nach ISO 27001 ist möglich
- BSI IT-Grundschutz
  - Methode und Anleitung zur Absicherung von Informationen und Systemen von Organisationen
  - Gestaffelt in die Absicherungsstufen Basis-, Standard- und Kern-Absicherung
  - An ISO 27001 ausgerichtet, dadurch ist ISO 27001 zertifizierbar auf Basis des IT-Grundschutz
- NIST Cybersecurity Framework
  - Leitfaden für das Management von Cybersicherheitsrisiken für beliebige Organisationen
  - Geteilt in verschiedene Funktionen, darunter auch „Detect“ und „Respond“ als integrale Bestandteile des Cybersecurity Managements

Auswahl von Systemtypen

- „Protokollierung“ fordert möglichst zentrale Speicherung aller Protokolle
  - Logmanagement-System erforderlich, das Protokolldaten weiterleitet und zentral speichert
  - Unterstützt idealerweise selbst die Protokollierung (Windows Event Forwarding, Syslog, …)
- „Detektion“ fordert Angriffserkennung vorrangig durch Korrelation von Protokollen
  - SIEM erforderlich, das Protokolldaten korreliert und auf Anomalien überwacht
  - NIDS wird ohne spezielle Anforderungen gefordert
- „Reaktion“ fordert automatisierte Reaktion auf Sicherheitsvorfälle
  - Breit interpretierbar: Bereits durch übliche Antivirusfunktionen abgedeckt?
  - Möglichst umfassende Lösung zur automatisierten Reaktion gesucht → SOAR

Auswahl von Open Source Lösungen

- Auswahlkriterien
  - Quellcode muss öffentlich sein
  - Aktive Entwicklung (6 Monate seit letzter Änderung)
  - Lizenz muss kommerzielle Nutzung erlauben
  - Kostenfreies Preismodell darf keinen Einschränkungen zu Zeit, Volumen oder Lizenzschlüssel-Zwang unterliegen
- Nur kostenfreie Funktionen berücksichtigt
- Dienstleistungen werden nicht betrachtet
- Maximal drei Vergleichskandidaten



Auswahl von Open Source Lösungen: Wazuh

- Open Source XDR-Lösung [9]
  - Bietet Funktionen in Endpoint-Sicherheit, Threat Intelligence, SIEM und Cloud Security
- Über 100.000 Enterprise Kunden und 20 Millionen jährliche Downloads
- Vollständig kostenfrei, professioneller Support, Consulting und Trainings angeboten
- Selbst installierbar oder als SaaS beziehbar
- Besteht aus Wazuh Server, Indexer und Agent
- **Stärken:** Als SIEM, Logmanagement und EDR geeignet → Umfassendes XDR
- **Schwächen:** Keine einfache Möglichkeit zur Ausführung von Suchen auf bereits analysierten Protokolldaten dokumentiert
- **Anforderungserfüllung:** 9/11 (Protokollierung), 19/21 (Detektion) 4/4 (Reaktion)

Auswahl von Open Source Lösungen: Shuffle

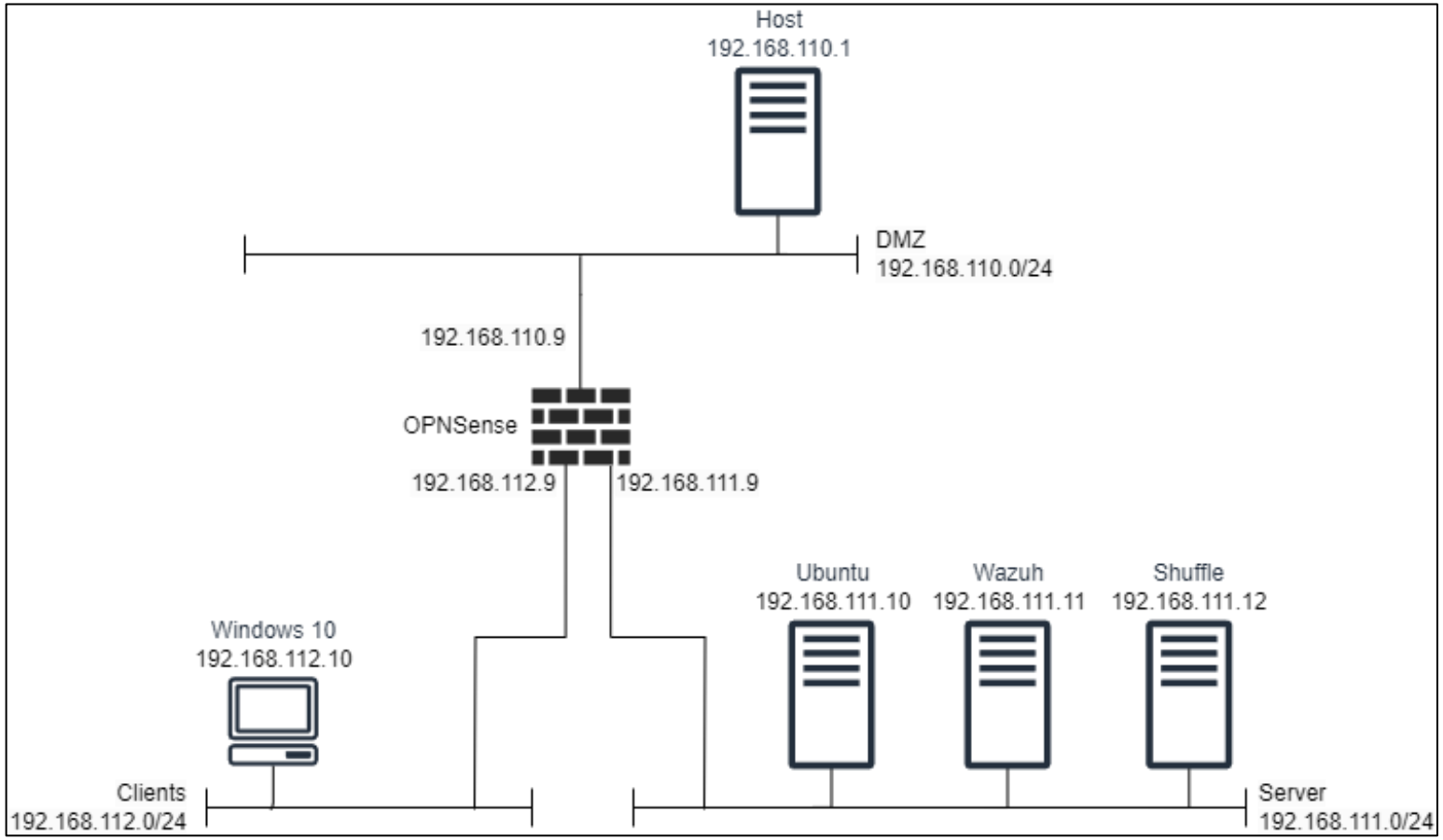
- Automatisierungslösung für Security-Workflows (SOAR) mit grafischem Editor [10]
- Beinhaltet fertige Vorlagen für Automatisierungen
- Über 2000 fertige Apps bzw. Integrationen
  - No-Code App Ersteller für die Erstellung eigener Integrationen eingebaut
- Selbst installierbar oder als SaaS beziehbar
  - Selbst installiert funktional vollständig kostenfrei, „Speed & Scale“ für Skalierfähigkeit zu kaufen
- **Stärken:** Voller Funktionsumfang kostenfrei
- **Schwächen:** Nichtfunktionale Einschränkungen in kostenfreier Version
- **Anforderungserfüllung:** 4/4 (Reaktion)

Konzept des Prototyps

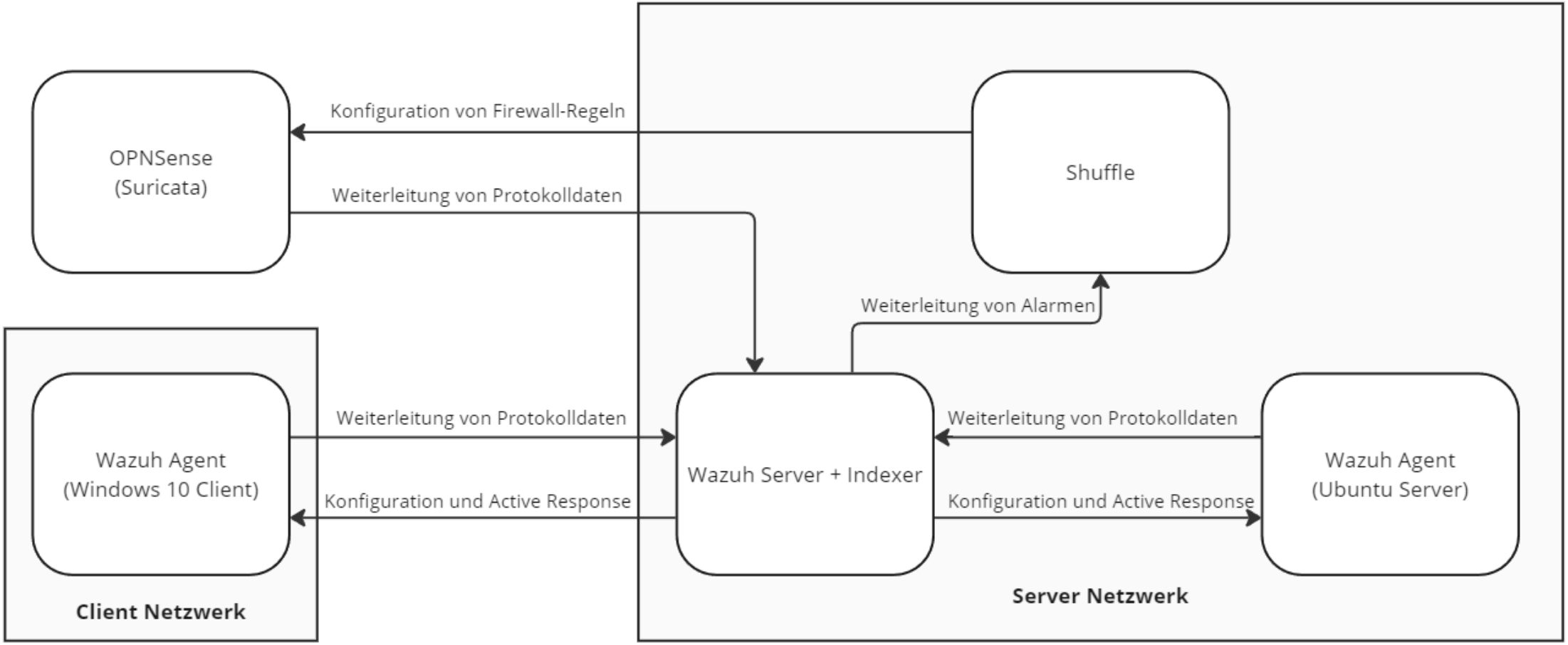
- Grundlage für den Entwurf des Prototyps ist die RECPLAST GmbH [11] des BSI
- Beschreibung, bestehende Richtlinien, Strukturanalyse und Netzplan vorhanden
- Einsatz von theoretisch evaluierten Open Source Lösungen:
  - Wazuh als SIEM und Logmanagement
  - Shuffle als SOAR
  - Suricata als NIDS, integriert in Open Source Firewall OPNsense
    - Firewall zur Nachempfindung des Netzplans der RECPLAST GmbH erforderlich

Aufbau des Prototyps: Netzplan

- Zentrale Firewall mit NIDS verbindet alle Netze
- DMZ mit Virtualisierungs-Host als Proxy ins Internet
- Client-Netz mit Windows 10 Client
- Server-Netz mit Ubuntu-Server, SIEM und SOAR



Aufbau des Prototyps: Interaktion der Systeme



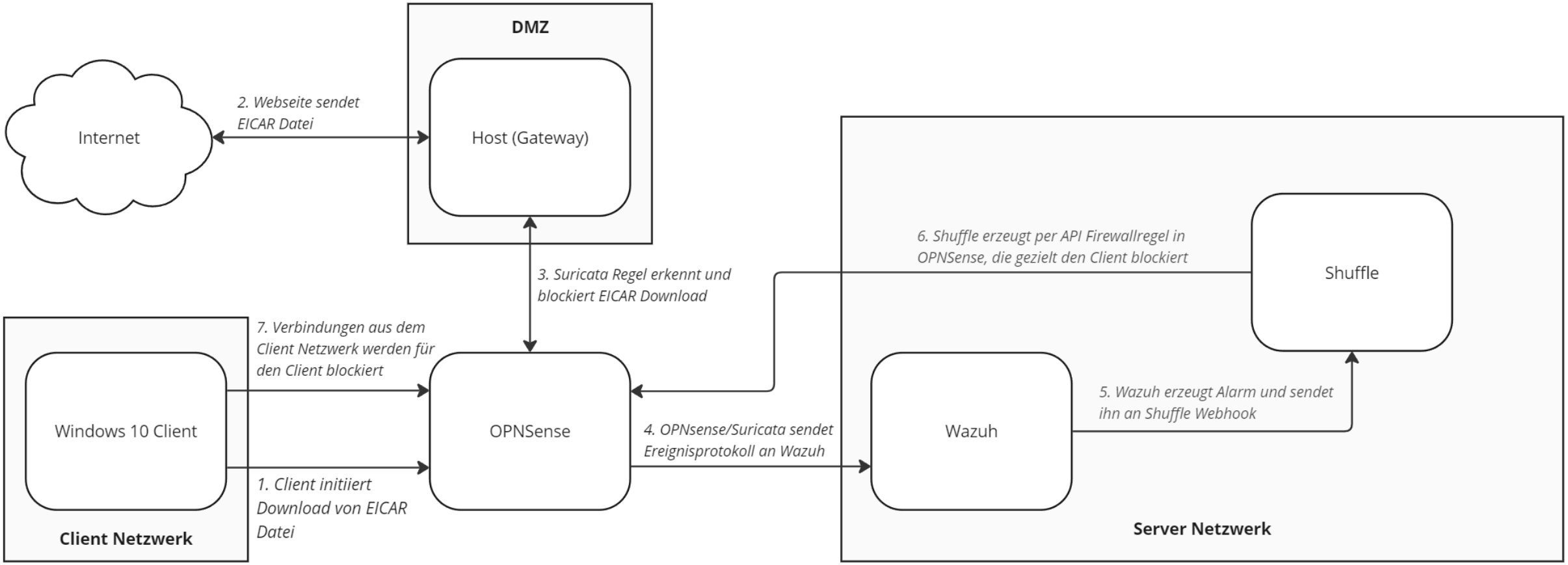
Organisatorische Maßnahmen

- Etablierung eines kontinuierlichen Verbesserungsprozesses
- Aufnahme der SzA in den IT-Betrieb
- Erstellung einer Richtlinie zur Protokollierung
- Synchronisation der Systemzeit der Protokolldatenquellen
- Einführungsprojekt zur Protokollierung
- Anpassung der IT-Betriebsprozesse
- Festlegung der Protokollierungsinfrastruktur
- Erstellung einer Richtlinie zur Detektion
- Etablierung eines Melde- und Alarmierungsprozesses
- Schulung der Mitarbeitenden
- Konfiguration der Detektion auf eingesetzten IT-Systemen
- Etablierung eines Security Operations Centers
- Einholen und Auswerten von Threat Intelligence
- Etablierung eines Schwachstellenmanagements
- Einsatz zusätzlicher Detektionssysteme
- Kalibrierung der Detektionsmechanismen
- Bedrohungs- und Risikoanalyse
- Erstellung einer Richtlinie zur Reaktion
- Definition eines Prozesses zur Reaktion
- Definition einer Kommunikations- und Kontaktstrategie
- Definition einer Eskalationsstrategie
- Automatisierte Reaktion

Test-Workflow des Prototyps

- Idee: Ablauf für möglichst umfassenden Nachweis der geforderten Funktionen
- Demonstration von…
  - NIDS
    → erkennt Anomalie
  - Protokollierung
    → NIDS protokolliert Anomalie
  - Detektion von Sicherheitsvorfällen auf Basis von Protokolldateien
    → SIEM detektiert Sicherheitsvorfall in Anomalie
  - automatisierter Reaktion
    → SOAR reagiert automatisch auf Sicherheitsvorfall

Test-Workflow des Prototyps



Protokolldatei | Einbruchserkennu | Discover - Wazuh | Shuffle - Workflows

Nicht sicher | 192.168.112.9/ui/diagnostics/log/core/suricata

OPNsense | root@opnsense-fw.recplast.lan

- Lobby
- Berichterstattung
- System
- Schnittstellen
- Firewall
- VPN
- Dienste
  - Captive Portal
  - DHCRelay
  - Dnsmasq-DNS
  - Einbruchserkennung
    - Verwaltung
    - Richtlinie
    - Protokolldatei
- Energie
- Hilfe

Dienste: Einbruchserkennung: Protokolldatei

Suche | Hinweis | 20

Datum	Gewichtung	Prozess	Zeile
2024-09-04T11:25:35	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:63566
2024-09-04T11:18:44	Notice	suricata	[100216] <Notice> -- Threads created -> W: 4 FM: 1 FR: 1 Engine started.
2024-09-04T11:18:34	Notice	suricata	[100326] <Notice> -- This is Suricata version 7.0.6 RELEASE running in SYSTEM mode
2024-07-14T18:04:28	Notice	suricata	[100327] <Notice> -- Signal Received. Stopping engine.
2024-07-14T17:50:35	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:64703
2024-07-14T17:18:58	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:64300
2024-07-14T15:02:53	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:61679
			virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:61663
			virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:61641
			virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.112.10:61284
			: 4 FM: 1 FR: 1 Engine started.
			on 7.0.6 RELEASE running in SYSTEM mode
			pping engine.
2024-07-14T14:19:29	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:29397
2024-07-14T14:13:37	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:23578
2024-07-14T12:46:46	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:48055
2024-07-14T12:35:46	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:22697
2024-07-14T12:17:14	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:1566
2024-07-14T11:59:54	Notice	suricata	[Drop] [1:7999999:1] OPNsense test eicar virus [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 89.149.222.99:80 -> 192.168.110.9:20311

Windows PowerShell

```
PS C:\Users\recplast> Invoke-WebRequest -Uri "http://pkg.opnsense.org/test/eicar.com.txt" -OutFile .\notavirus.txt
```

13:10
04.09.2024

Protokolldatei | Einbruchserkennu | Discover - Wazuh | Shuffle - Workflows

Nicht sicher | https://192.168.111.11/app/data-explorer/discover#?_a=(discover:(columns:!(_source),isDirty:!f,sort:!()),metadata:(indexPattern:'wazuh-*',view:discover))&_g=(filters:!(),re...

Discover | New Discover | New | Save | Open | Share | Reporting | Inspect | a

wazuh-* | test | DQL | Today | Show dates | Refresh

+ Add filter

Search field names | Filter by type 3

Selected fields

_source

Available fields

_index
agent.id
agent.ip
agent.name
analysisd.alerts_queue_size
analysisd.alerts_queue_usage
analysisd.alerts_written
analysisd.archives_queue_size
analysisd.archives_queue_usage
analysisd.dbsync_messages_dispatched
analysisd.dbsync_queue_size
analysisd.dbsync_queue_usage

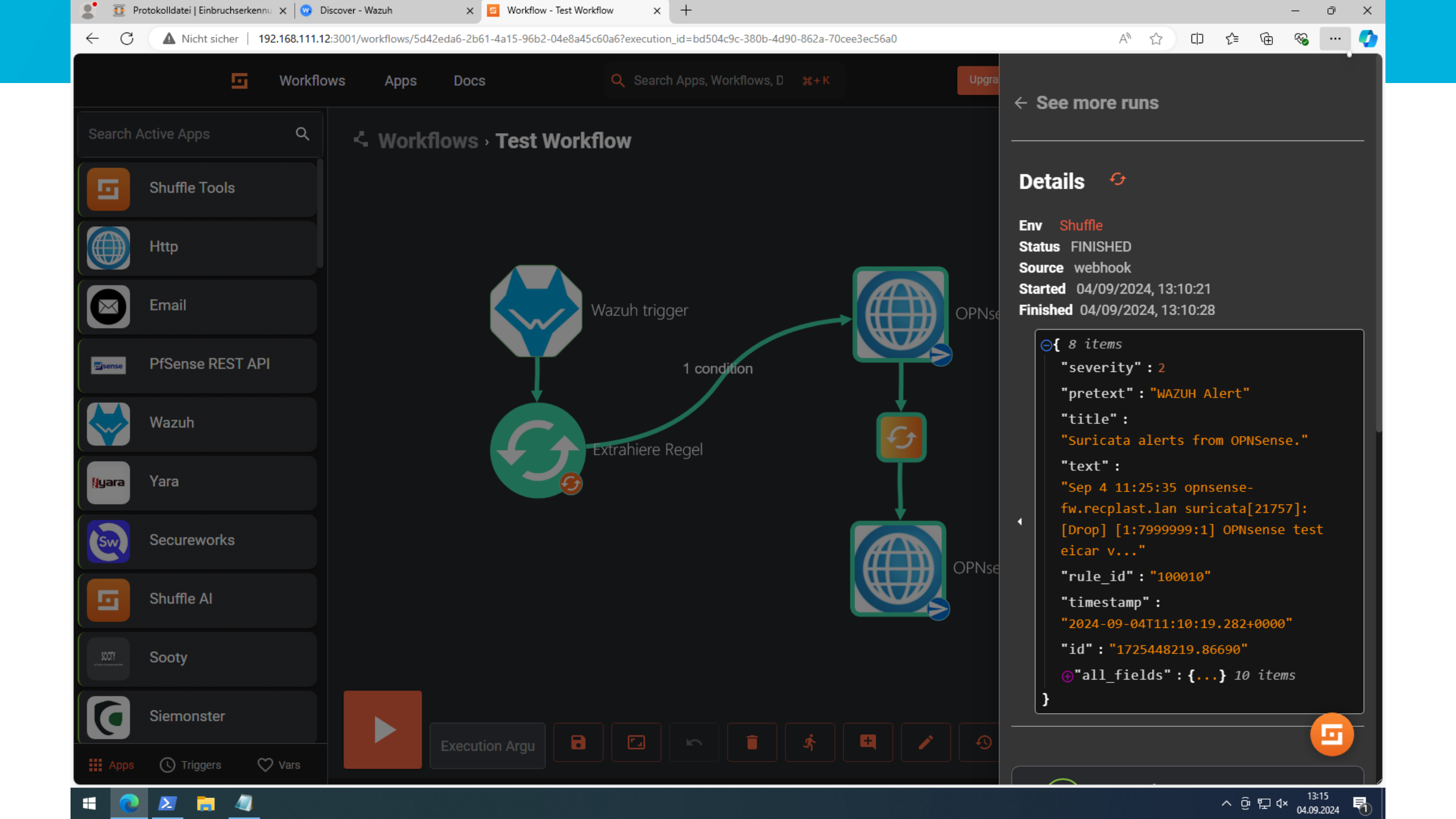
2 hits

Sep 4, 2024 @ 00:00:00.000 - Sep 4, 2024 @ 23:59:59.999 per Auto

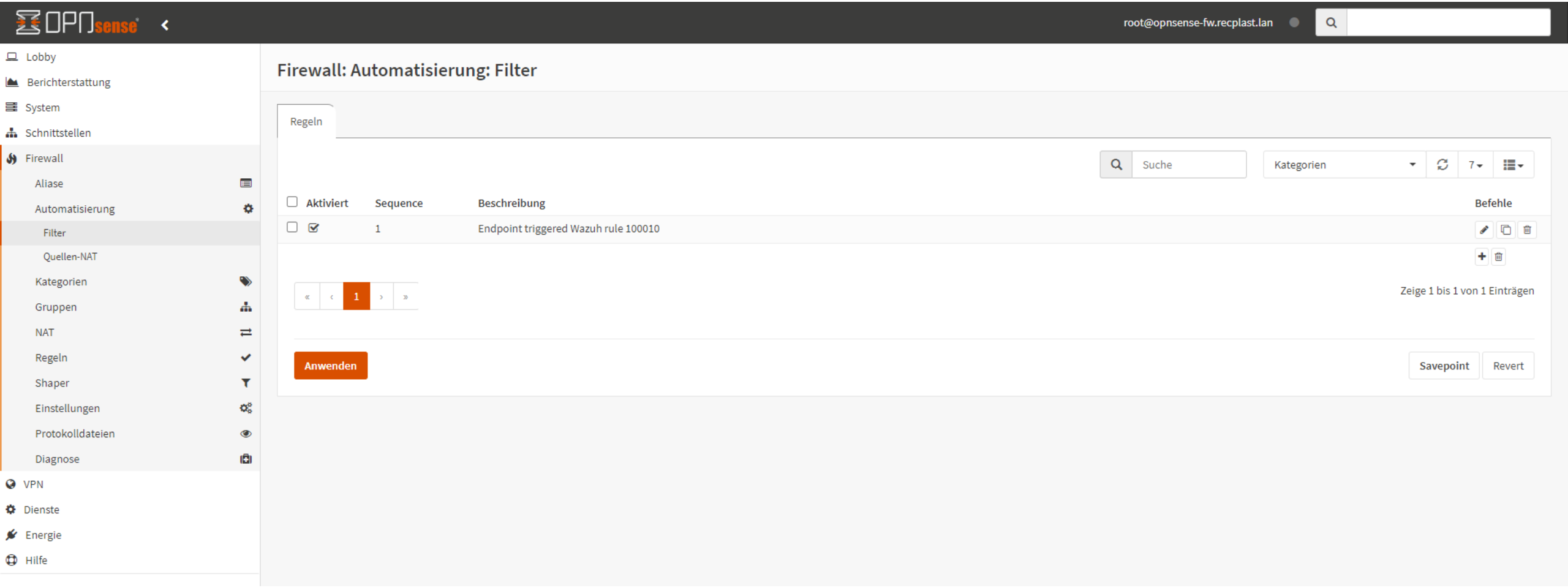
Columns | Sort fields

Time (timestamp)	Source
Sep 4, 2024 @ 13:02:17.734	predecoder.hostname opnsense-fw.recplast.lan predecoder.program_name suricata predecoder.timestamp Sep 4 13:02:17 input.type log agent.name wazuh agent.id 000 manager.name wazuh data.ids_classification Potentially Bad Traffic data.src_ip 89.149.222.99 data.src_port 80 data.protocol TCP data.ids_prio 2 data.dst_port 52625 data.ids_rule OPNsense test eicar virus data.dst_ip 192.168.112.10 rule.firedtimes 1 rule.mail fals...
Sep 4, 2024 @ 13:02:17.734	predecoder.hostname opnsense-fw.recplast.lan predecoder.program_name suricata predecoder.timestamp Sep 4 13:02:17 input.type log agent.name wazuh agent.id 000 manager.name wazuh data.ids_classification Potentially Bad Traffic data.src_ip 89.149.222.99 data.src_port 80 data.protocol TCP data.ids_prio 2 data.dst_port 52625 data.ids_rule OPNsense test eicar virus data.dst_ip 192.168.112.10 rule.firedtimes 1 rule.mail fals...

Netzwerk Internetzugriff


Protokolldatei | Einbruchserkennu
Discover - Wazuh
Workflow - Test Workflow
Nicht sicher
192.168.111.12:3001/workflows/5d42eda6-2b61-4a15-96b2-04e8a45c60a6?execution_id=bd504c9c-380b-4d90-862a-70cee3ec56a0
Workflows
Apps
Docs
Search Apps, Workflows, D
⌘+K
Upgra
Search Active Apps
Shuffle Tools
Http
Email
PfSense REST API
Wazuh
Yara
Secureworks
Shuffle AI
Sooty
Siemonster
Apps
Triggers
Vars
Workflows › Test Workflow
Wazuh trigger
1 condition
Extrahiere Regel
OPNse
OPNse
Execution Argu
See more runs
Details
Env Shuffle
Status FINISHED
Source webhook
Started 04/09/2024, 13:10:21
Finished 04/09/2024, 13:10:28
{ 8 items
"severity" : 2
"pretext" : "WAZUH Alert"
"title" :
"Suricata alerts from OPNSense."
"text" :
"Sep 4 11:25:35 opnsense-
fw.recplast.lan suricata[21757]:
[Drop] [1:7999999:1] OPNsense test
eicar v..."
"rule_id" : "100010"
"timestamp" :
"2024-09-04T11:10:19.282+0000"
"id" : "1725448219.86690"
"all_fields" : {...} 10 items
}
13:15
04.09.2024

Umsetzbarkeit der OH-SzA des BSI mittels Open Source Lösungen

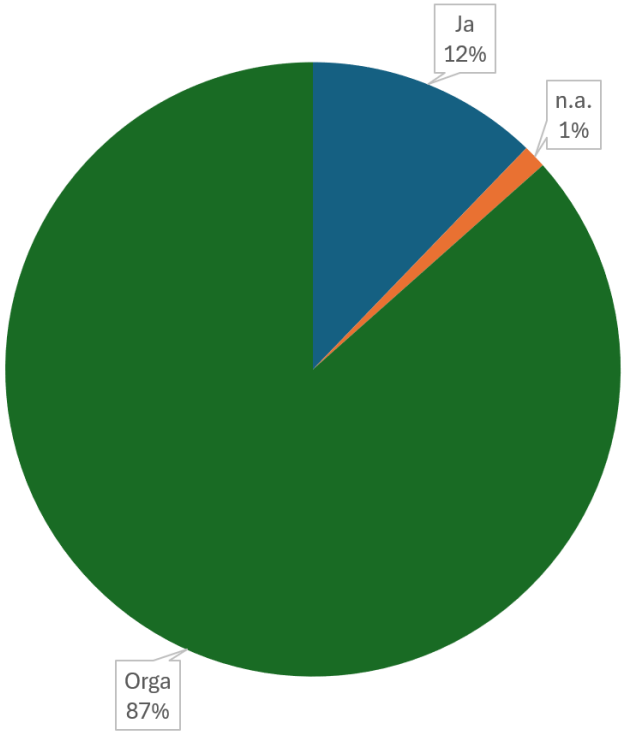


Bewertung des Prototyps

- Zielwert der OH-SzA: Umsetzungsgrad Stufe 4
- Erfüllt in Verbindung mit den organisatorischen Maßnahmen sämtliche Anforderungen
- „Nicht anwendbare“ Anforderungen sind durch Erfüllung der anderen automatisch erfüllt
- Über die OH-SzA hinaus sind keine Maßnahmen geplant

→**Der Prototyp erreicht Umsetzungsgrad Stufe 4**

→**Bietet gute Basis zur Erreichung von Stufe 5**



Ausbaumöglichkeiten des Prototyps

- Der Prototyp bietet Erweiterungs- und Verbesserungspotenzial
- Erweiterung um weitere Workflows
  - Alarmierung bei identifizierten Schwachstellen, automatisches Löschen von Malware auf Endpunkten, ...
- Integration weiterer Systeme
  - Mailserver oder andere Kommunikationsplattformen zur verlässlicheren Benachrichtigung bei Vorfällen

Empfehlungen für KMU: Kernfragen

FOSS oder kommerzielle Lösungen?

- **Faktoren:** Dokumentation, Support, Kosten und Verfügbarkeit von Dienstleistern.
- **Mehraufwand bei FOSS-Lösungen:** Geringere Dokumentation, umfangreiche Tests notwendig.
- **Verfügbarkeit von SaaS:** Für kommerzielle SzA verbreiteter als bei FOSS.

Betrieb: Intern oder extern?

- **Interner Betrieb:** Höhere Kontrolle, aber auch höhere interne Aufwände.
- **SaaS:** Geringere Aufwände, aber Abhängigkeit von externer oder Cloud-Infrastruktur.
- Entscheidung von Risikoappetit, intern verfügbaren Ressourcen und IT-Strategie abhängig

SOC: Intern oder extern?

- **Internes SOC:** Erfordert Fachpersonal und Expertise.
- **Externes SOC / MSSP:** Ohne interne Aufwände, aber externe Kosten.
- **Hybrides SOC:** Kombination aus internem und externem SOC möglich.
- Entscheidung maßgeblich von IT-Strategie und Unternehmensfokus abhängig

Empfehlungen für KMU: Vorgehen

- Umfassende Analyse
  - Bewertung von Support- und Dienstleister-Verfügbarkeit
  - Prüfung der Dokumentation auf hinreichende Qualität
  - Vollkostenbetrachtung (Lizenzen, Betriebsaufwände, Nutzungsaufwände, …)
- Berücksichtigung der Unternehmensstrategie
  - Internalisierung oder Externalisierung bevorzugt?
  - Fokus auf Aufbau interner IT-Sicherheits-Kompetenzen?
- Hinterfragen der Motivation
  - IT-Sicherheit oder Compliance im Fokus?

Die Wahl der richtigen Lösung für den Einsatz von SzA hängt von diversen Faktoren ab. Eine gründliche Analyse der relevanten Betrachtungsaspekte und Abwägung der Vor- und Nachteile ist essenziell.

Quellen

[1] 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: 2. September 2024. [Online]. Verfügbar unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

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

[3] Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“. 26. September 2022. Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=15

[4] Microsoft, „Was ist SIEM?“ Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.microsoft.com/de-de/security/business/security-101/what-is-siem

[5] IBM, „Was ist ein Intrusion Detection System (IDS)?“ Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/intrusion-detection-system

[6] IBM, „Was ist Endpoint Detection and Response (EDR)?“ Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/edr

[7] IBM, „Was ist SOAR (Security, Orchestration, Automation and Response)?“ Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/security-orchestration-automation-response

[8] IBM, „Was ist ein Security Operations Center (SOC)?“ Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://www.ibm.com/de-de/topics/security-operations-center

[9] Wazuh, „Wazuh - Open Source XDR. Open Source SIEM.“, Wazuh. Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://wazuh.com/

[10] Shuffle, „The Open Source SOAR for all purposes“. Zugegriffen: 2. September 2024. [Online]. Verfügbar unter: https://shuffler.io

[11] Bundesamt für Sicherheit in der Informationstechnik, „Arbeitsbeispiel RECPLAST GmbH“. Zugegriffen: 2. September 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