Forensische Analyse eines SAP-Systems nach einem Sicherheitsvorfall unter Einbeziehung verschiedener Untersuchungszeitpunkte

Kolloquium

02. November 2021

Fakultät für Ingenieurwissenschaften \ Bereich Elektrotechnik und Informatik

Gliederung

1. Motivation
2. Versuchsaufbau und -ablauf
3. Ergebnisse
4. Evaluierung und Konfiguration der Protokolle
5. Security Information and Event Management (SIEM)
6. Ausblick

Motivation

- **SAP Weltmarktführer in mehreren Business-Software Bereichen**
- **SAP-Systeme häufig zentrale IT-Komponente von Unternehmen**
- **Angriff kann gravierende Auswirkungen haben**

Problemstellungen

Welche Daten können extrahiert werden?
Welche Protokollfunktionen generieren die Daten?
Wie müssen diese für ein optimales Ergebnis konfiguriert werden?

Motivation

Nortel hacking attack went unnoticed for almost 10 years

Hackers broke into Nortel's computer networks more than a decade ago and over the years downloaded technical papers, research-and-development reports, business plans, employee emails and other documents.

By Ryan Naraine for Zero Day | February 14, 2012 |

Sophisticated iPhone hacking went unnoticed for over two years

30 AUG 2019 4

e, Security threats, Vulnerability

Solarwinds lässt grüssen

Codecov-Hack bleibt zwei Monate lang unbemerkt

Fr 23.04.2021 - 14:56 Uhr
von Yannick Chavanne und Übersetzung: Niara Sakho

Operation Layover Malware Campaign Targeted Aviation Industry For Five Years

written by Abeerah Hashim | September 20, 2021

Quellen:
https://www.it-markt.ch/cybersecurity/2021-04-23/codecov-hack-bleibt-zwei-monate-lang-unbemerkt
https://latesthackingnews.com/2021/09/20/operation-layover-malware-campaign-targeted-aviation-industry-for-five-years/
https://www.zdnet.com/article/nortel-hacking-attack-went-unnoticed-for-almost-10-years/
https://nakedsecurity.sophos.com/2019/08/30/sophisticated-iphone-hacking-went-unnoticed-for-over-two-years/

Motivation

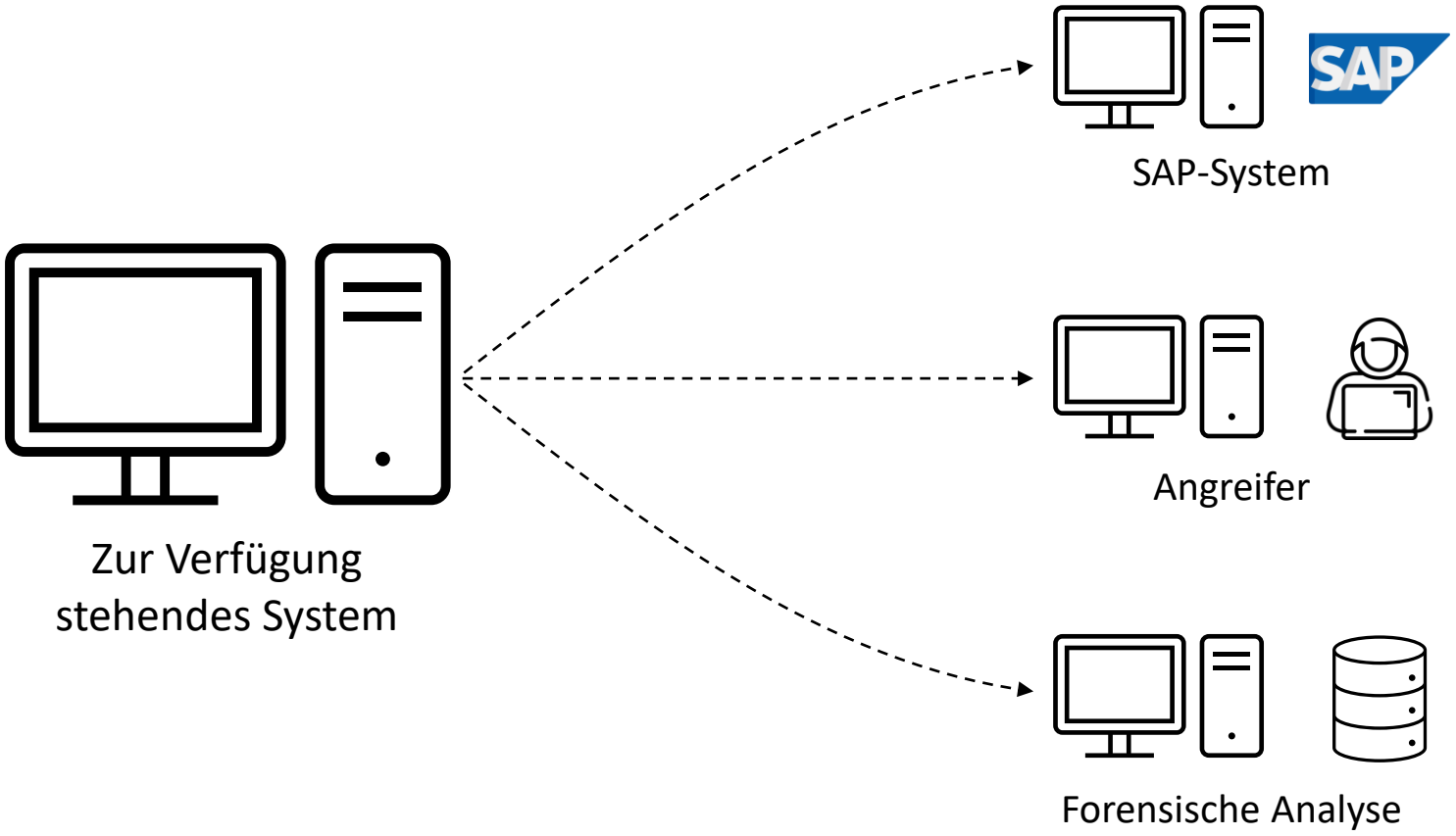
- **Durchschnittliche Reaktionszeit auf einen Angriff: 54 Tage (Stand 2019)**
- **Nur 40% aller Angriffe werden innerhalb der ersten 30 Tage bemerkt**

Problemstellungen

Welche Auswirkungen hat eine verzögerte Reaktionszeit auf die zur Verfügung stehenden Daten?

Quelle: https://www.fireeye.com/content/dam/collateral/en/mtrends-2020.pdf

Versuchsaufbau und -ablauf

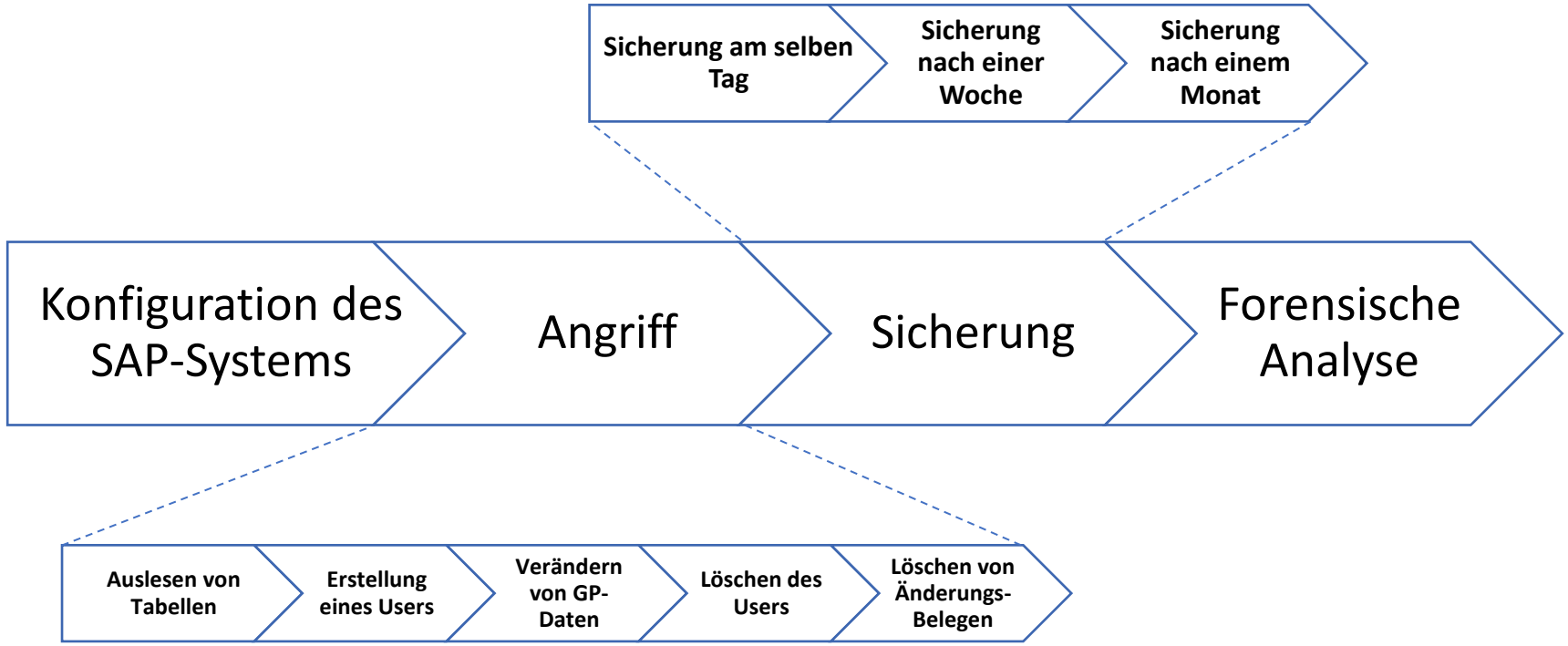


- IDES ERP 6.0 inkl. EHP8
- Innerhalb VirtualBox

- Benutzer mit Zugriff auf das SAP-System
- Verwendete Tools: Excel, Hashcat

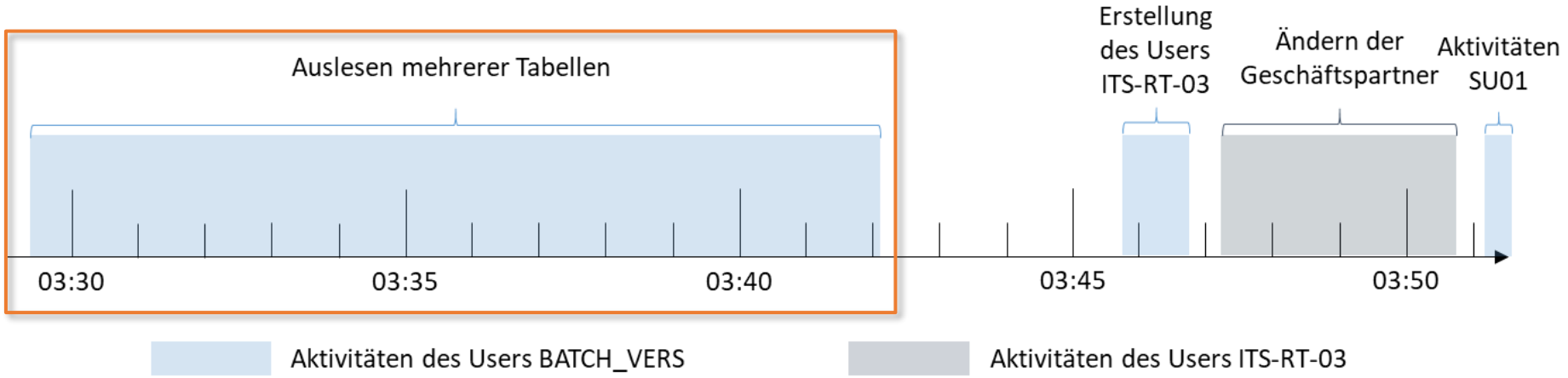
- Sicherung der Images auf einer externen Festplatte
- Verwendete Tools: FTK Imager, Autopsy

Versuchsaufbau und -ablauf



Ergebnisse - Überblick

Mit Hilfe der forensischen Analyse konnten die folgenden Tätigkeiten des Angreifers rekonstruiert werden:



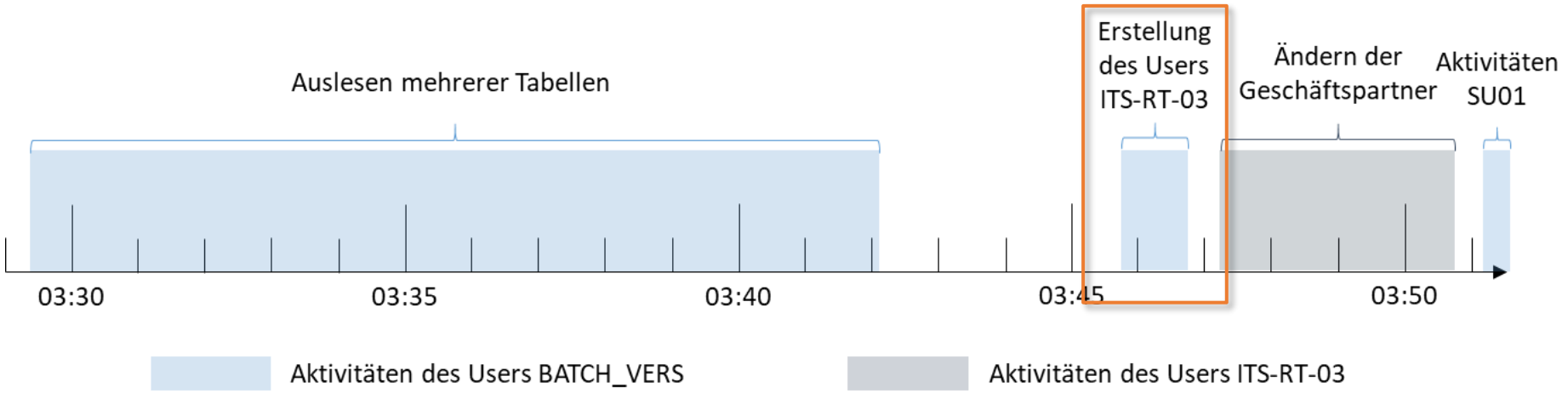
Ergebnisse – Auslesen mehrerer Tabellen

- **Ausschlaggebendes Protokoll: Security Audit Log**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
ID	SAL-Code	Jahr	Monat	Tag	Stunde	Minute	Sekunde	String	Terminal	User	Transaction	Report	Mandant	Beschreibung	Terminal lang
2	AUK	2021	6	20	3	29	26	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	29	26	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1KNA1&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	29	44	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	29	44	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1KNA1&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	30	18	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	30	18	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1KNBK&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	32	45	000552000007D7	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	32	45	000552000007D7	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT_ADRC_ACT&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	33	6	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	33	6	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT_ADRC_ACT&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	33	40	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	33	40	000534800005D5	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT000&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	34	13	000269600003D3	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	34	13	000269600003D3	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT0BK&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	35	24	000269600003D3	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	35	24	000269600003D3	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1LFA1&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	36	13	000329200001D1	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	36	13	000329200001D1	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1LFBK&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	36	22	000329200001D1	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	36	22	000329200001D1	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1LFBK&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	40	4	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	40	4	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT000&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	40	41	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	40	41	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1BUT000&03	WIN-IDES01.fritz.box
2	AUK	2021	6	20	3	42	11	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1SDTX&&RFC_READ_TABLE	WIN-IDES01.fritz.box
2	CUZ	2021	6	20	3	42	12	000388000000D0	WIN-IDES	BATCH_VERS	S000	SAPMSSY1	800	1USR02&03	WIN-IDES01.fritz.box

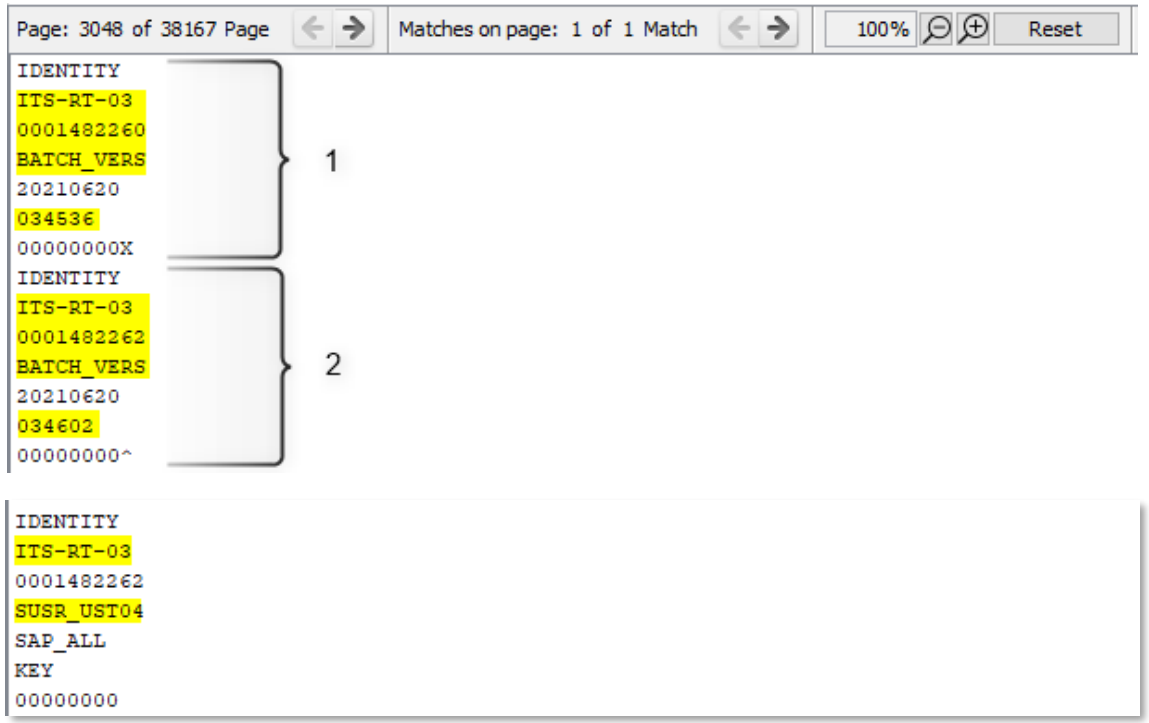
Ergebnisse - Überblick

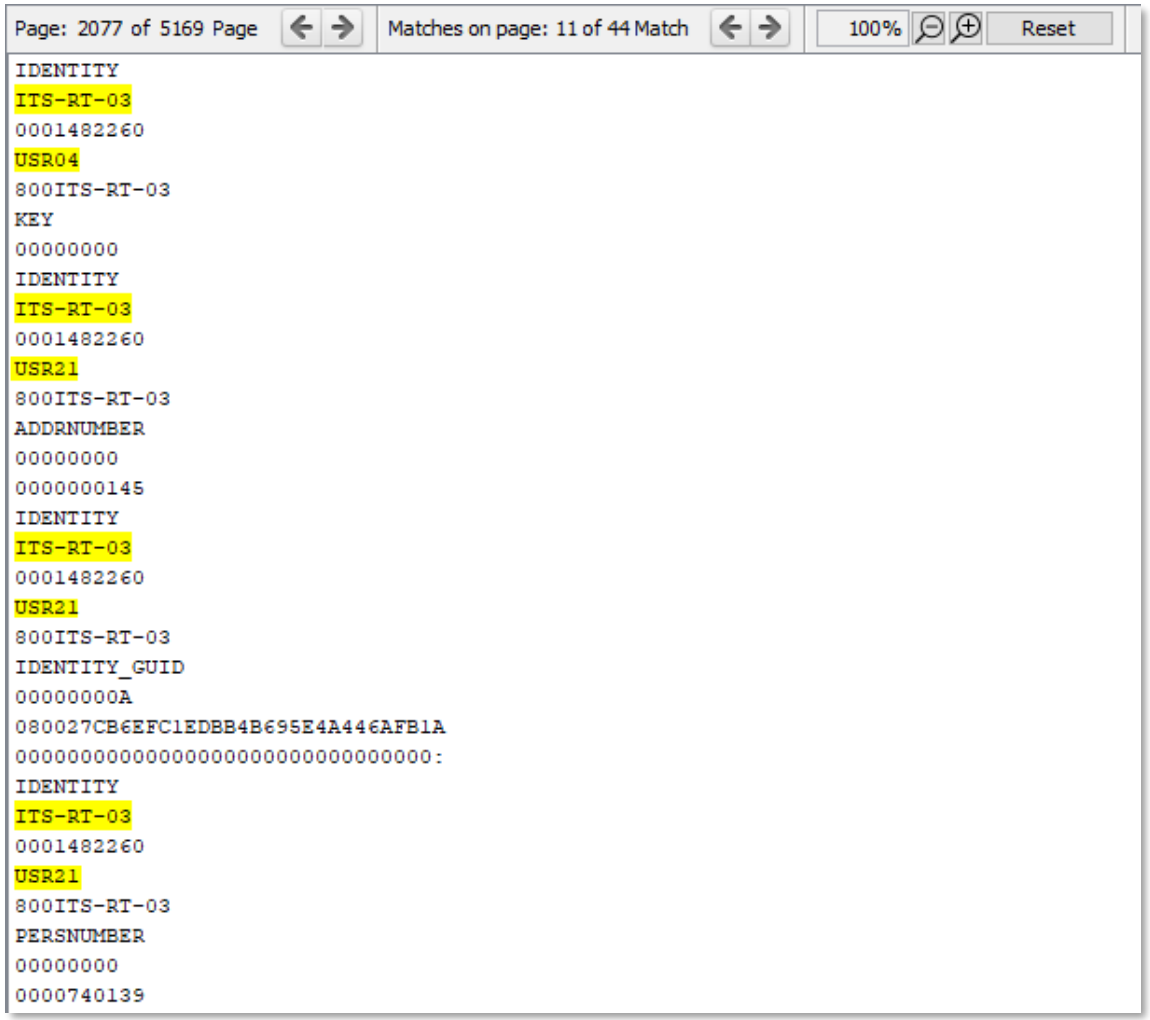
Mit Hilfe der forensischen Analyse konnten die folgenden Tätigkeiten des Angreifers rekonstruiert werden:



Ergebnisse – Erstellung des Users ITS-RT-03

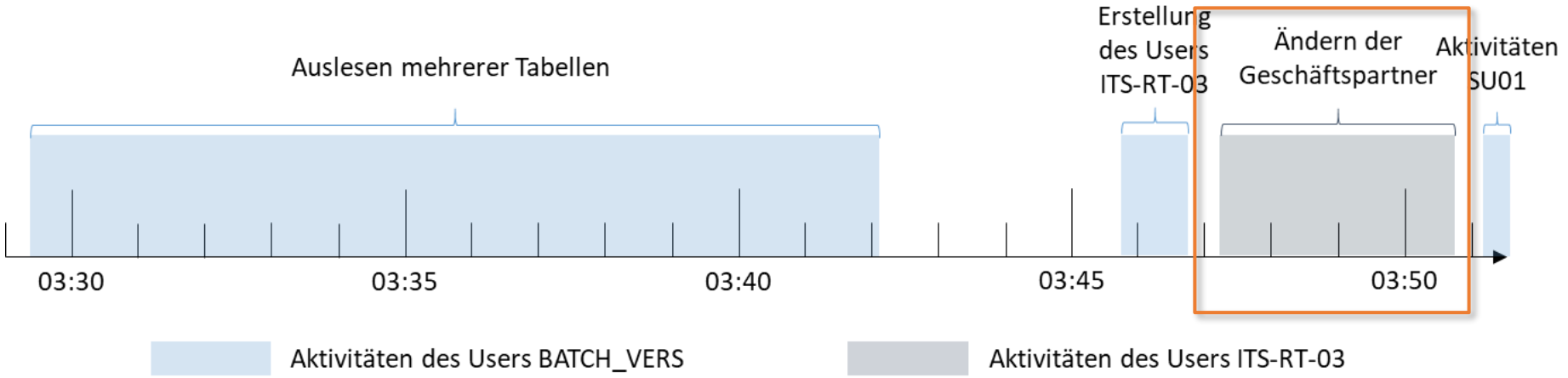
- **Ausschlaggebendes Protokoll: Database Dump, Disk- und Log-Volumes**





Ergebnisse - Überblick

Mit Hilfe der forensischen Analyse konnten die folgenden Tätigkeiten des Angreifers rekonstruiert werden:



Ergebnisse – Ändern der Geschäftspartnerdaten

- **Ausschlaggebendes Protokoll: Database Dump, Disk- und Log-Volumes**

Geschäftspartner	Kreditor
0000609131	GTS_0002

Neue Bankverbindung

DE 10033000 888888888

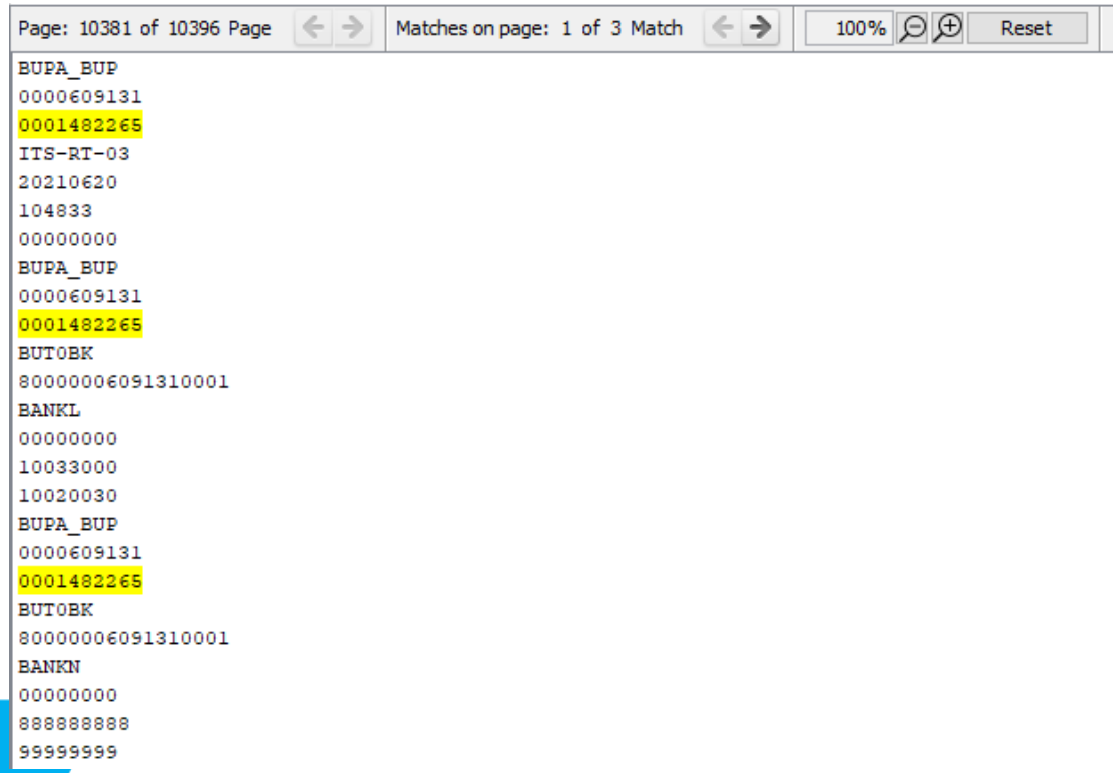
Geschäftspartner	Kreditor
0000611432	0000003200

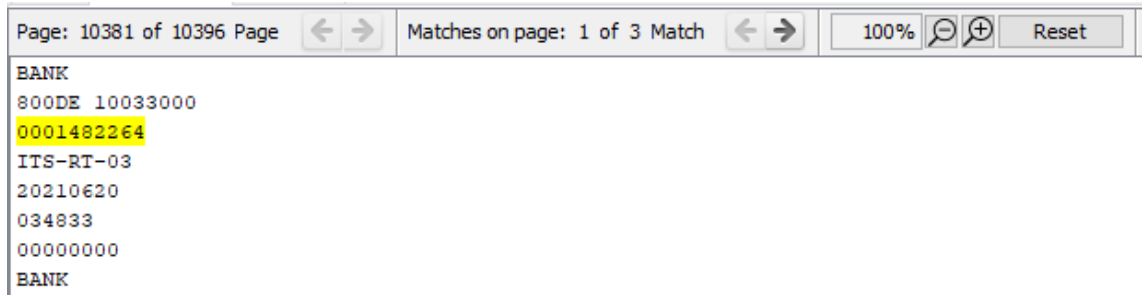
Neue Bankverbindung

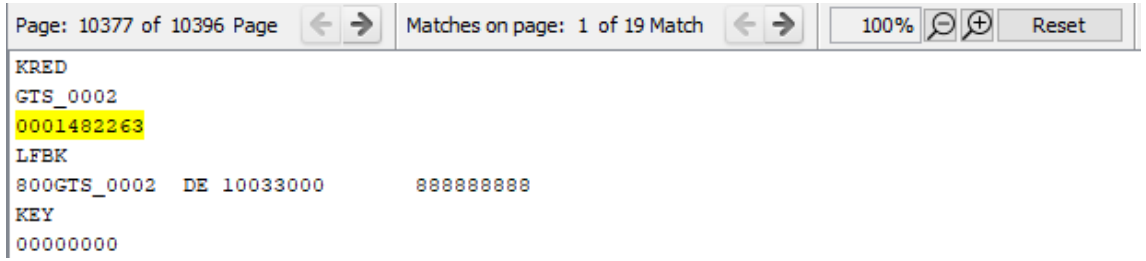
US 443235555 44444444

Ergebnisse – Ändern der Geschäftspartnerdaten

1. Anpassung des Kreditors *GTS_0002*
2. Erstellung der Bank *Bank Forensik*
3. Anpassung des Geschäftspartners 0000609131

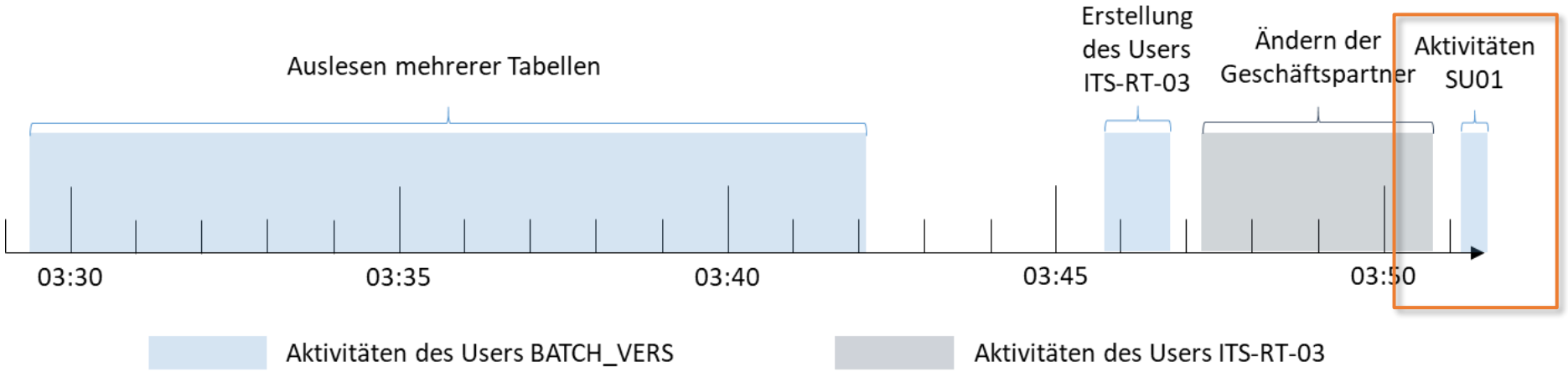






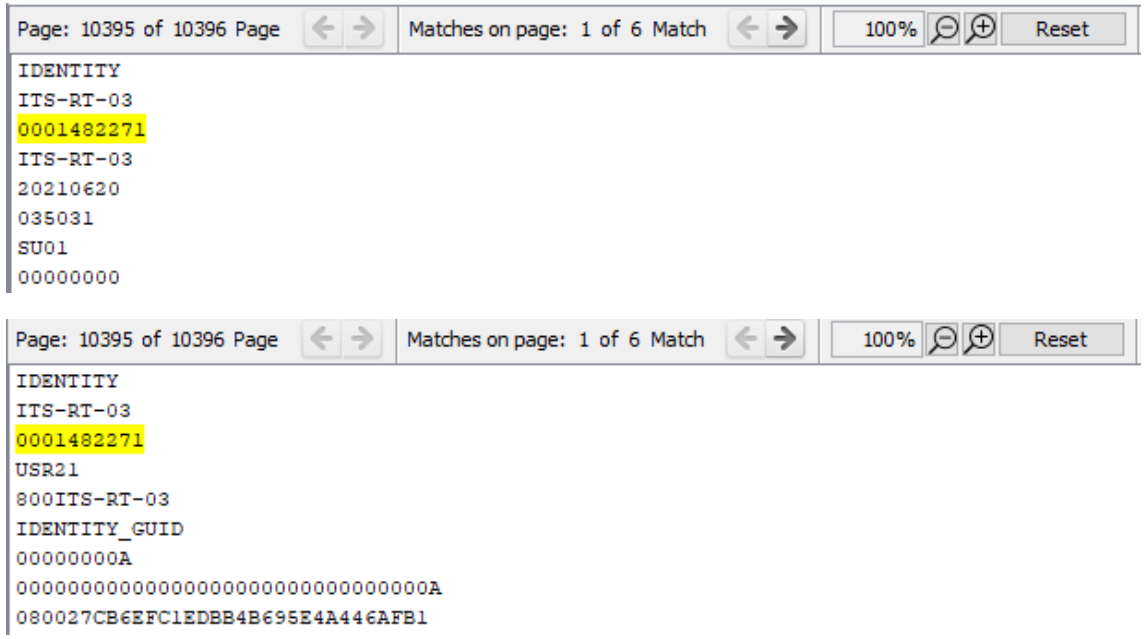
Ergebnisse - Überblick

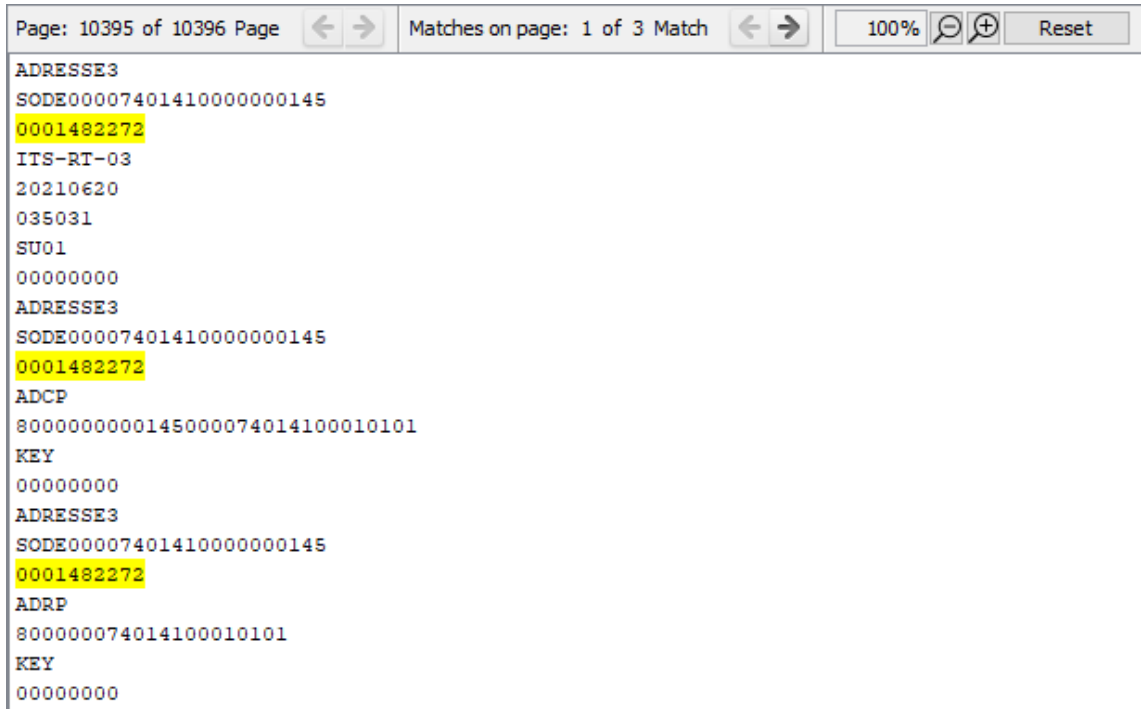
Mit Hilfe der forensischen Analyse konnten die folgenden Tätigkeiten des Angreifers rekonstruiert werden:



Ergebnisse – Aktivitäten in der SU01

- **Ausschlaggebendes Protokoll: Disk- und Log-Volumes, Statistikdatensätze**





Ergebnisse – Report Z_READ_TABLE

Evaluierung und Konfiguration der Protokolle

Security Audit Log

- Zentrales Protokoll
- Je nach Filtereinstellungen umfangreiche Protokollierung
- Zeigt lesende RFC-Aufrufe des Batchusers

- Manuelle Aktivierung notwendig
- Konfiguration der Speicherparameter entscheidend

Statistikdatensätze

- Zeichnet einen „roten Faden“ der erfolgten Aktivitäten
- Alle Report, Transaktions- und RFC-Aufrufe werden aufgezeichnet

---

- Einplanung eines Standard-Jobs notwendig
- Anpassung des Parameters stat/max_files empfohlen

Dateien der Datenbank

- Großteil der erfolgten Änderungen nachvollziehbar
- Änderungsbelegtabellen CDHDR und CDPOS ausschlaggebend

- Aktivierung der Dateien nicht notwendig
- Overwrite-Modus sollte vermieden werden

Evaluierung und Konfiguration der Protokolle

Gateway Log

- Nutzen für durchgeführten Angriff gering
- Für Analyse externer Zugriff dennoch nützlich

- Konfiguration in der SMGW bietet mehrere Filter
- Zu detaillierte Einstellungen können zu stark an-wachsenden Dateien führen

Entwickler Traces

- Nutzen für durchgeführten Angriff gering
- Fokus liegt auf der temporären Fehleranalyse

- Ab dem Trace-Level 2 ist das Protokoll sehr detailliert
- Wächst rasant in der Größe an

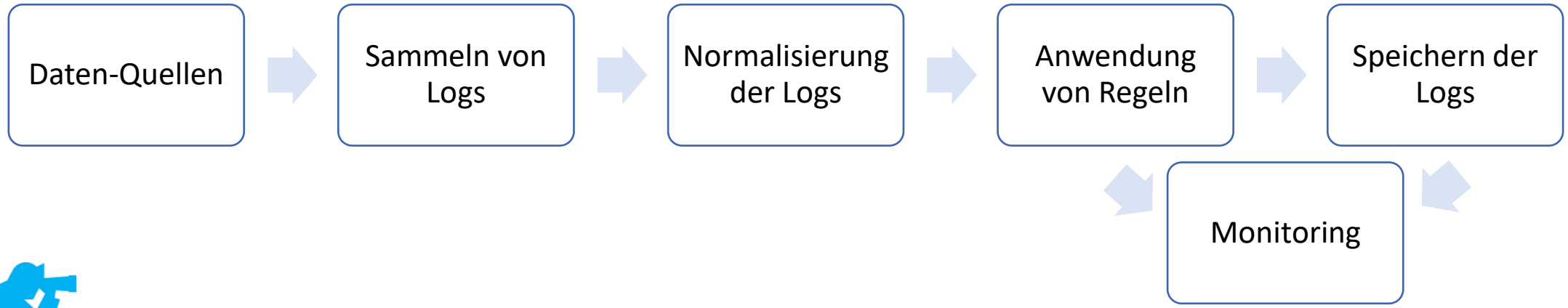
Weitere Logs

- Systemlog mit nur geringem Nutzen für Analyse
- CCMS-Alerts bieten eine Absicherung des SAL und STAT

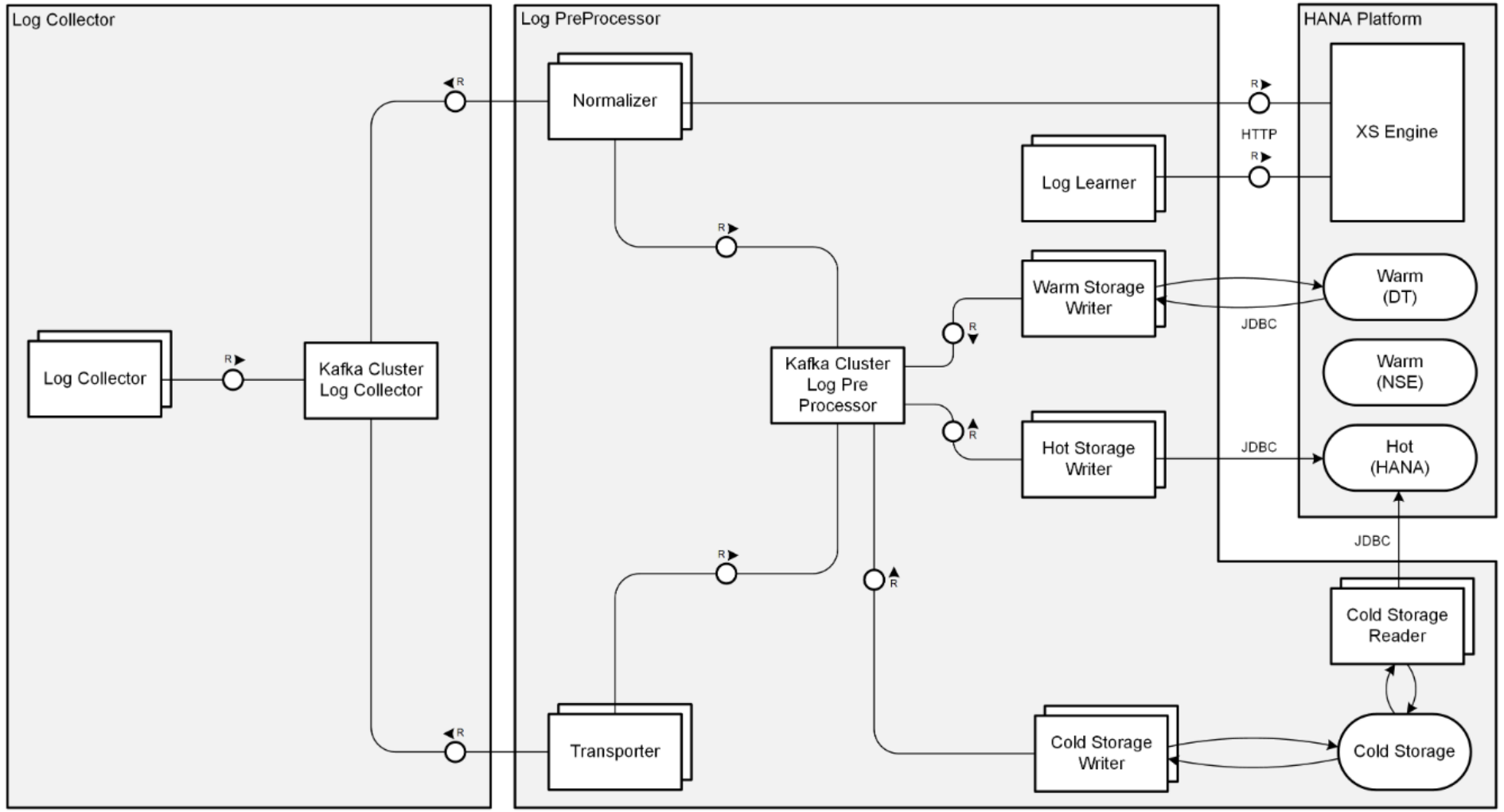
- Aufbewahrungsfrist des Systemlogs bei Bedarf anpassbar
- Anpassung des Umfangs der Alert-Dateien sollte im System beobachtet werden

Security Information and Event Management (SIEM)

- Sammeln Log-Dateien aus verschiedenen Quellen an einem zentralen Punkt
- Analyse der Logs anhand von definierten Regeln
- Automatische Generierung von Meldungen
- Überwachung der Meldungen in Echtzeit



SAP Enterprise Thread Detection



Security Information and Event Management (SIEM)

Vorteile:

- Automatische Analyse großer Datenmengen
- Automatische Erkennung von Sicherheitsvorfällen möglich
- Zentraler Speicherort für verschiedene Logdateien
- Speicherdauer unabhängig vom SAP Standardwert

Nachteile:

- Konfiguration von Regeln sehr komplex
- Je nach Log-Dateien große Speicherkapazitäten notwendig
- Keine 100% Abdeckung möglich – Gefahr des „blinden Vertrauens“

Ausblick

- **Neue Technologien in SAP:**
  - Fiori (Web-Oberfläche)
  - HANA (Datenbank)
- **HANA Datenbank**
  - Bestehende Logs können größtenteils weiterverwendet werden
  - Zusätzliche Audit-Möglichkeiten
- **Fiori**
  - Weboberfläche bietet Angriffsmöglichkeiten für „klassische“ Webangriffe
  - Neue Logfunktionen für Auswertung relevant