KFW Bank aus Verantwortung

Der Sprung ins Next-Level-SOC: Modern, automatisiert, zukunftssicher

Udo Gross (KfW), Max Gerwens (CC)
Splunk Public Summit, Frankfurt, 16.03.2026

KFW
Bank aus Verantwortung

Next-Level-SOC

Team- und Projektvorstellung

Max Gerwens, Benjamin Gennermann Computacenter
Udo Gross, ITs2 SOC

Vorstellung Speaker

UDO GROSS

KfW

SOC Architect

ITs2 Security Operating Center SOC

MAX GERWENS

Computacenter

Technical Project-Lead

SIEM-Stream

BENJAMIN GENNERMANN

Computacenter

Technical Project-Lead

SOAR-Stream

UNSER TEAMLEAD FÜR EINE ERFOLGREICHE MIGRATION

Bedrohungslage

Angriffe auf Banken keine Seltenheit

Finanzsektor im Fokus der Hacker

Cyberangriffe auf Banken nehmen zu und moderne Abwehr ist gefragt

22.09.2025 · Ein Gastbeitrag von Thomas Gassenbauer · 5 min Lesedauer ·

Banken, Versicherer und IT-Dienst
im Visier von Cyberkriminellen. P
Ransomware-Gruppen und KI-ges
verursachen weltweit Schäden in
Sicherheitsarchitekturen wie SOA
helfen, Risiken frühzeitig zu erker

tagesschau Sendung verpasst?

Hacker-Angriff

Daten von Tausenden Bankkunden abgegriffen

Stand: 11.07.2023 14:00 Uhr

Ein Datenleck bei einem Dienstleister für den Kontowechsel trifft nicht nur Kunden der Deutschen Bank und Postbank. Wie jetzt bekannt wurde, zählen auch Kunden von zwei weiteren Geldinstituten zu den Opfern des Hackerangriffs.

Auch die Direktbank ING und die zur Commerzbank gehörende Comdirect sind von dem Hackerangriff auf einen Dienstleister für den Kontowechsel betroffen. Das haben beide Häuser heute bestätigt. Die Commerzbank stellte
enleck nicht

APT28 verantwortlich für großangelegte Cyberkampagne

Ab Ende Dezember 2022 kam es zu einem Cyberangriff von APT28 auf die Sozialdemokratische Partei Deutschlands (SPD). Der Angriff ist Teil einer größeren Kampagne, in der seit mindestens März 2022 eine Schwachstelle im Microsoft-Windows-Client von Outlook ausgenutzt wurde (CVE-2023-23397). Die Durchführung dieser Kampagne wurde durch die Bundesregierung nun öffentlich APT28 zugeschrieben.

Die SPD hatte den Angriff im Juni 2023 öffentlich gemacht. Die

Ausgangslage KfW

Motivation für Migration

SIEM (ArcSight)

- “in die Jahre gekommen”
- Bildet nicht mehr alle funktionalen Überwachungsanforderungen ab
- Spezielle Use Cases schwierig umzusetzen

Security Operation Center

SOAR (TheHive)

- End of Live angekündigt
- Bisher nur ein komplexer SOAR-Use Case umgesetzt (Phishing)
- Nicht zukunftssicher

umfassende Markterkundung

2023

EU-Ausschreibung im offenen Verfahren (Anfang 2024)
Migration von ArcSight Logger zu Splunk IDX Cluster
Zuschlag Computacenter (Ende 2024)

2024

Projektstart 10.12.2024
Erfolgreiches Ende für Migration zu Splunk ES und SOAR

Ende 2025

Projektzielbild

Projektauftrag

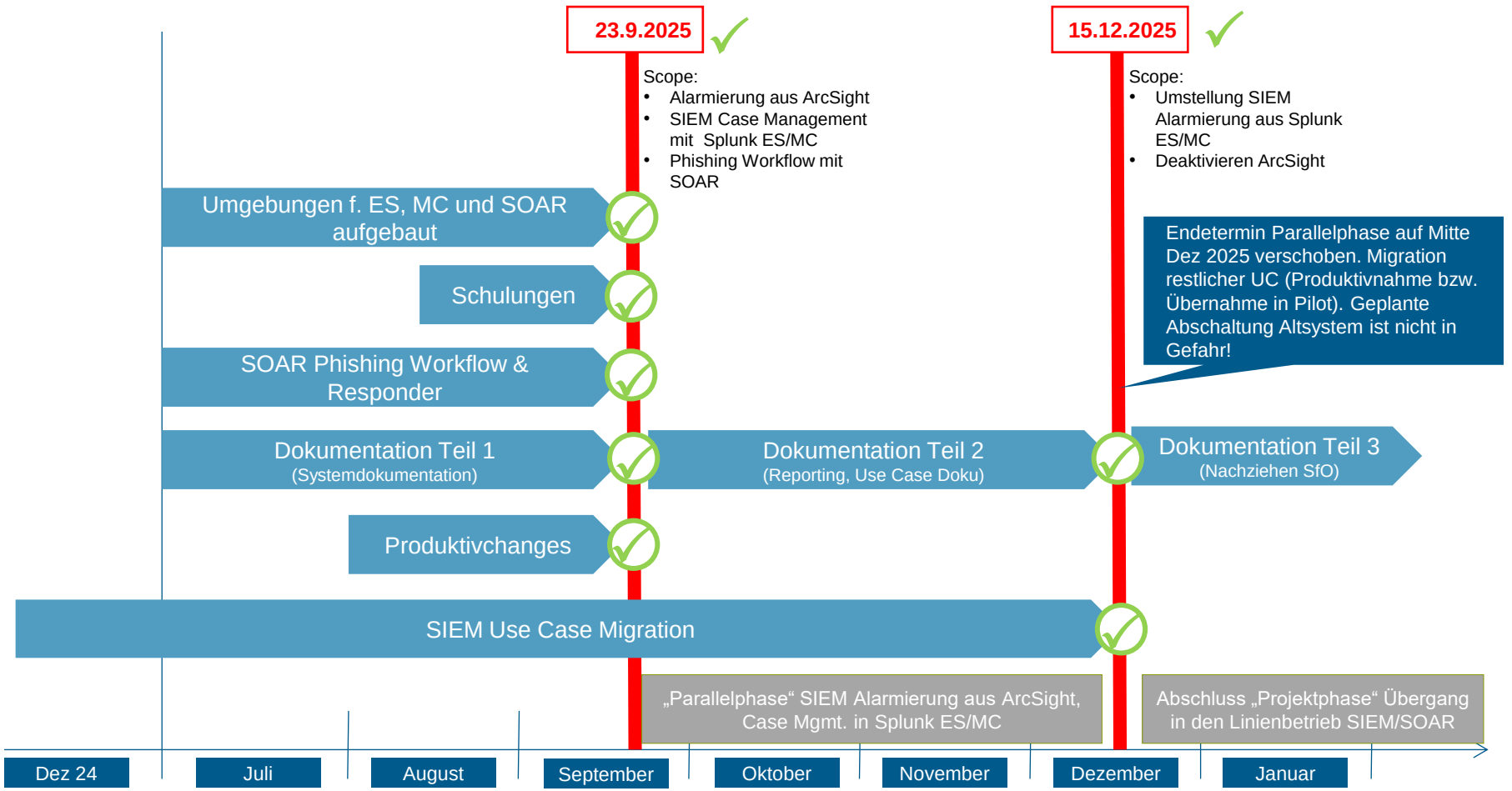
Austausch der bestehenden Security Systeme ArcSight SIEM und TheHive SOAR durch **Splunk Enterprise-Security (ES) und Splunk SOAR** in 2025

Projektziele

- **Migration des bestehenden Funktionsumfangs** von ArcSight SIEM und The Hive SOAR auf die neue Zielarchitektur
- **Aufbau** einer neuen/angepassten **Splunk Infrastruktur** für Splunk ES und für SOAR
- **Portierung** sämtlicher produktiver eingehender und ausgehender Schnittstellen und Datenlieferstrecken
- **Bereinigung und Optimierung** des SIEM Use Case Bestands
- Parallele Implementierung, aber mit Priorisierung:
  1. SOAR produktiv bis Mitte 2025 (Fehlender Support Altsystem TheHive 4.0)
  2. SIEM OnPrem bis Ende 2025 (Ablaufender Supportvertrag für ArcSight)
  3. SIEM/SOAR in der Cloud: Anbindung MS Sentinel an Splunk ES „as is“, Weiterentwicklung der Strategie und Umsetzung in 2026 (ggf. frühere Pilotierung falls sinnvoll/nötig)
- **Schulung** der Mitarbeiter (Admins, Analysten, Entwickler)
- **Cut Over von** Case Management **Migration** im Parallelbetrieb Alte/Neue Welt
- **Anpassung der Prozesse** und der SfO wo nötig sowie der Dienstvereinbarung SOC

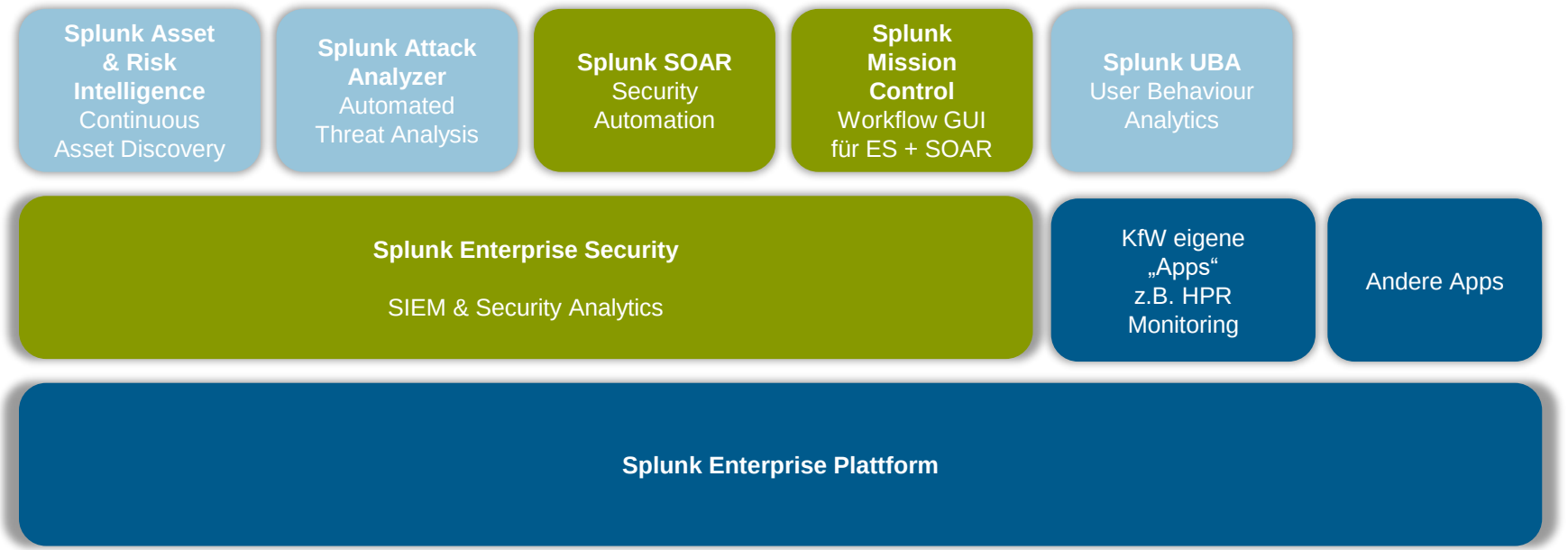
Projektphasen Next Level SOC

Kritische Projektphase – Crunchtime



Zielbild

High Level



KFW
Bank aus Verantwortung

Next-Level-SOC

Herausforderungen

Herausforderungen

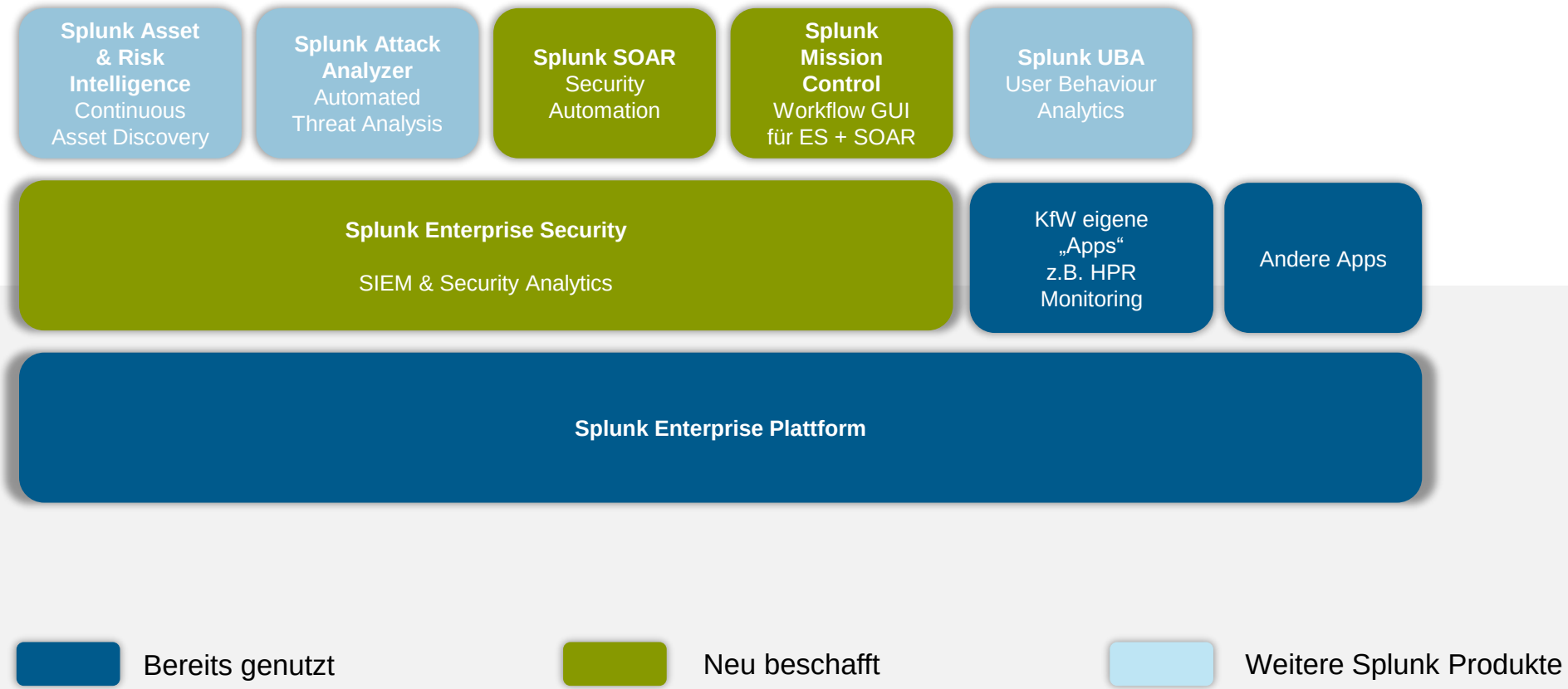
1. Architektur Design
2. Automatisierter Failover für Splunk SOAR
3. onPrem Pairing von Splunk ES + SOAR
4. Konsolidierung von Projekt Stakeholdern (Orange, KfW, CC, Freelancer, Splunk SE)
5. Use Case Migration und Konsolidierung inkl. Umstellung auf RBA
6. Verbesserungen von KPIs (MTTT, MTTR etc.)
7. SLAs und weitere regulatorische Rahmenbedingungen

Herausforderungen

1. Architektur Design
2. Automatisierter Failover für Splunk SOAR
3. onPrem Pairing von Splunk ES + SOAR
4. Konsolidierung von Stakeholdern (Orange, KfW, CC, Freelancer, Splunk SE)
5. Use Case Migration und Konsolidierung inkl. Umstellung auf RBA
6. Verbesserungen von KPIs (MTTT, MTTR etc.)
7. SLAs und weitere regulatorische Rahmenbedingungen

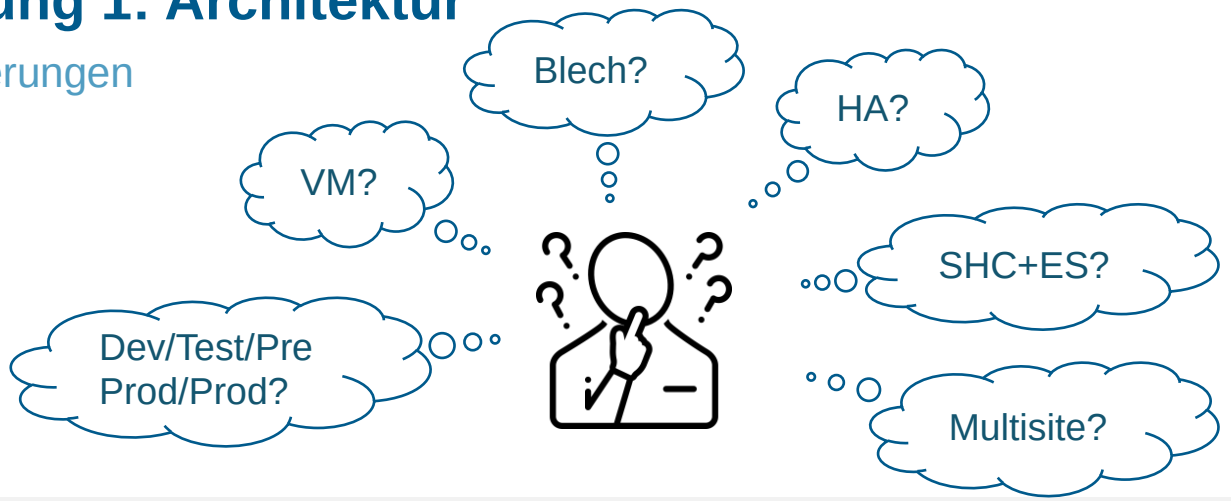
Herausforderung 1: Architektur

Design Herausforderungen



Herausforderung 1: Architektur

Design Herausforderungen



Splunk SOAR
Security Automation

Splunk Enterprise Security

SIEM & Security Analytics

Splunk Enterprise Plattform

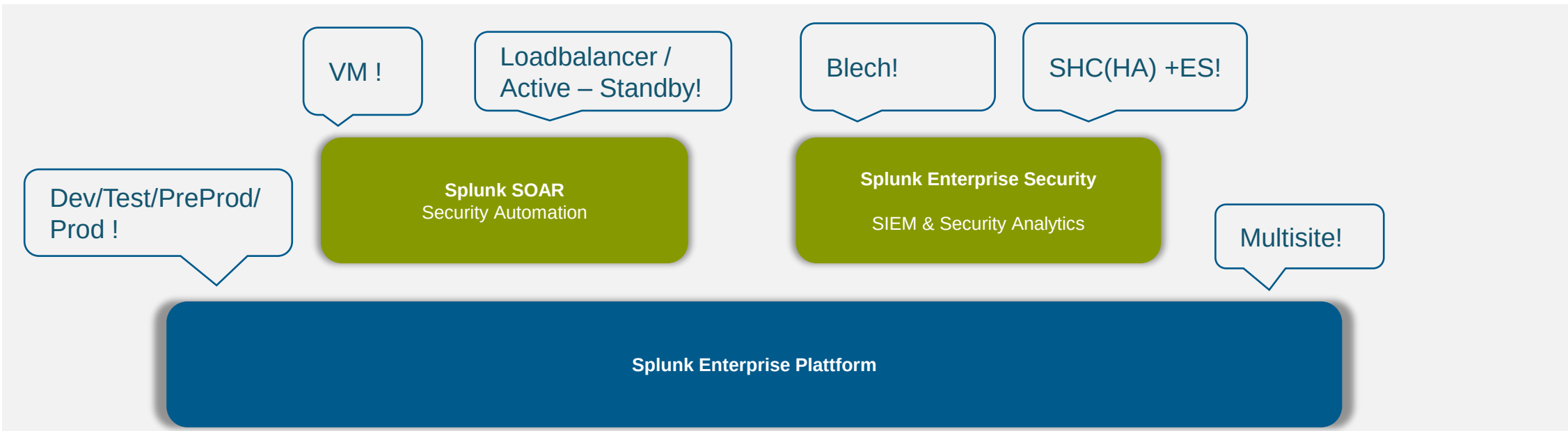
Herausforderung 1: Architektur

Design Herausforderungen

Entscheidungsgrundlagen

Aktuelle Daten - Performance, Ingest, Storage etc.

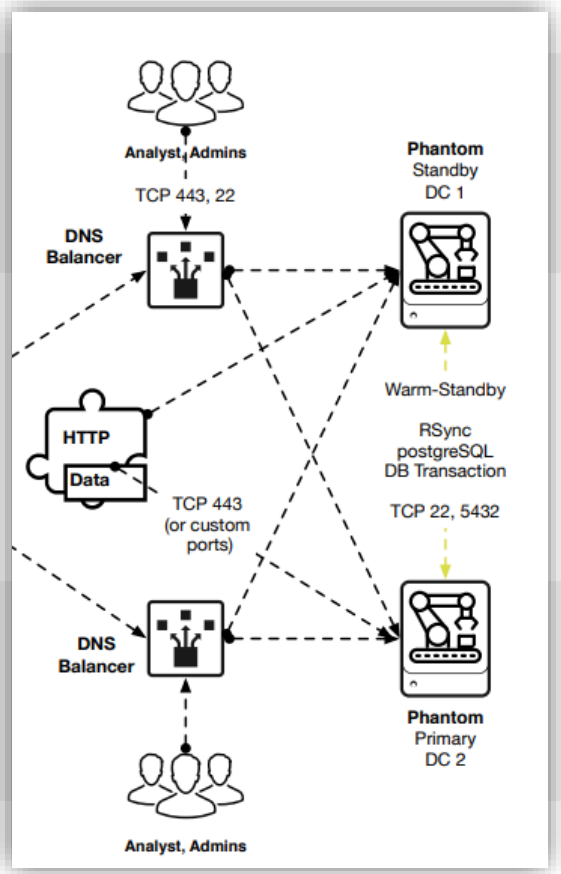
(Zukünftige) Anforderungen - Cloud, Automatisierung, Retention, SOC Services, Regularien etc.



Herausforderung 2: HA on Splunk SOAR

Design Überlegungen

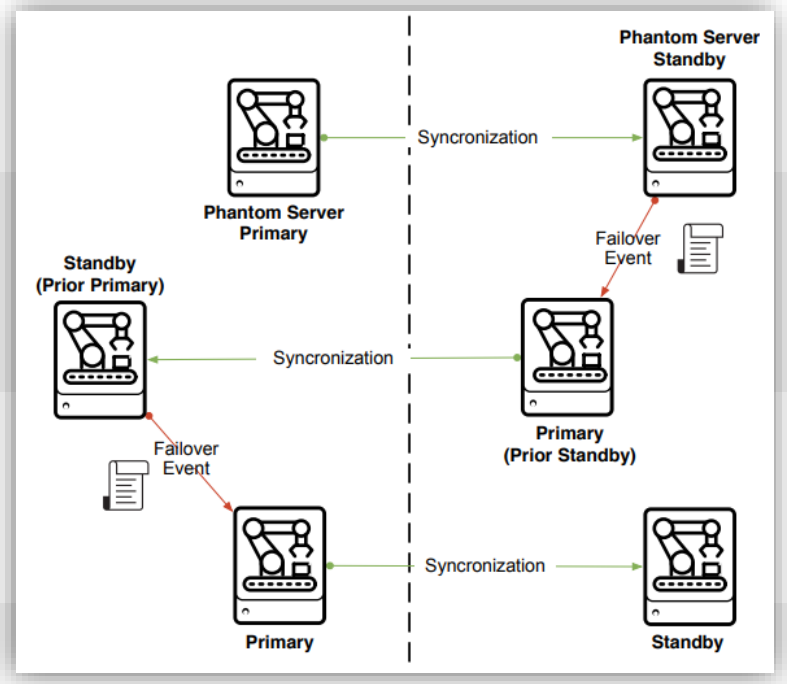
Herausforderung	HA-Ausfallzeit gewährleisten Automatisierter Failover
Input	Splunk SOAR Validated Architectures 2.0
Output	Virtuelle Single Instanzen Warm-Standby autom. Failover



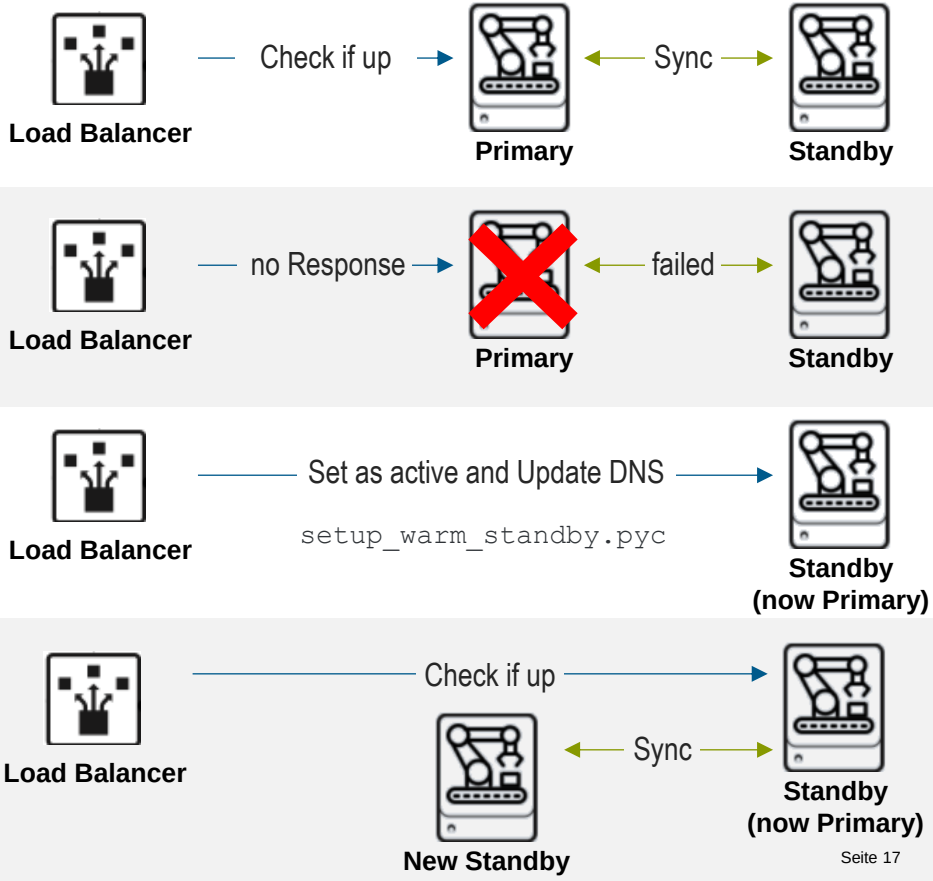
Herausforderung 2: HA on Splunk SOAR

Automatisierter Failover Prozess

Failover Prozess Detail



Scripted Failover (SSVA 2.0)



Herausforderung 3: Pairing von ES + SOAR

native Pairing von on Prem Splunk ES + on Prem SOAR

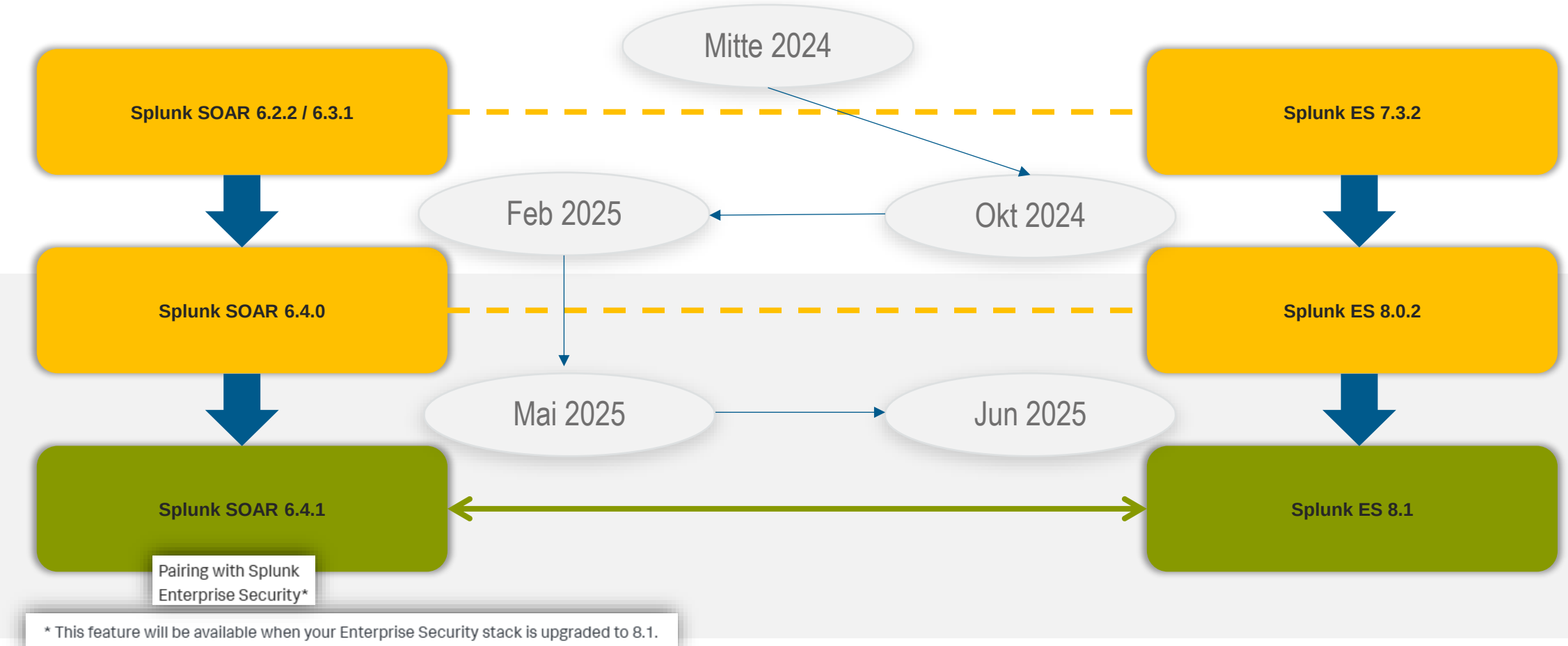
Splunk SOAR
Security Automation

Splunk Enterprise Security

SIEM & Security Analytics

Herausforderung 3: Pairing von ES + SOAR

native Pairing von on Prem Splunk ES + on Prem SOAR

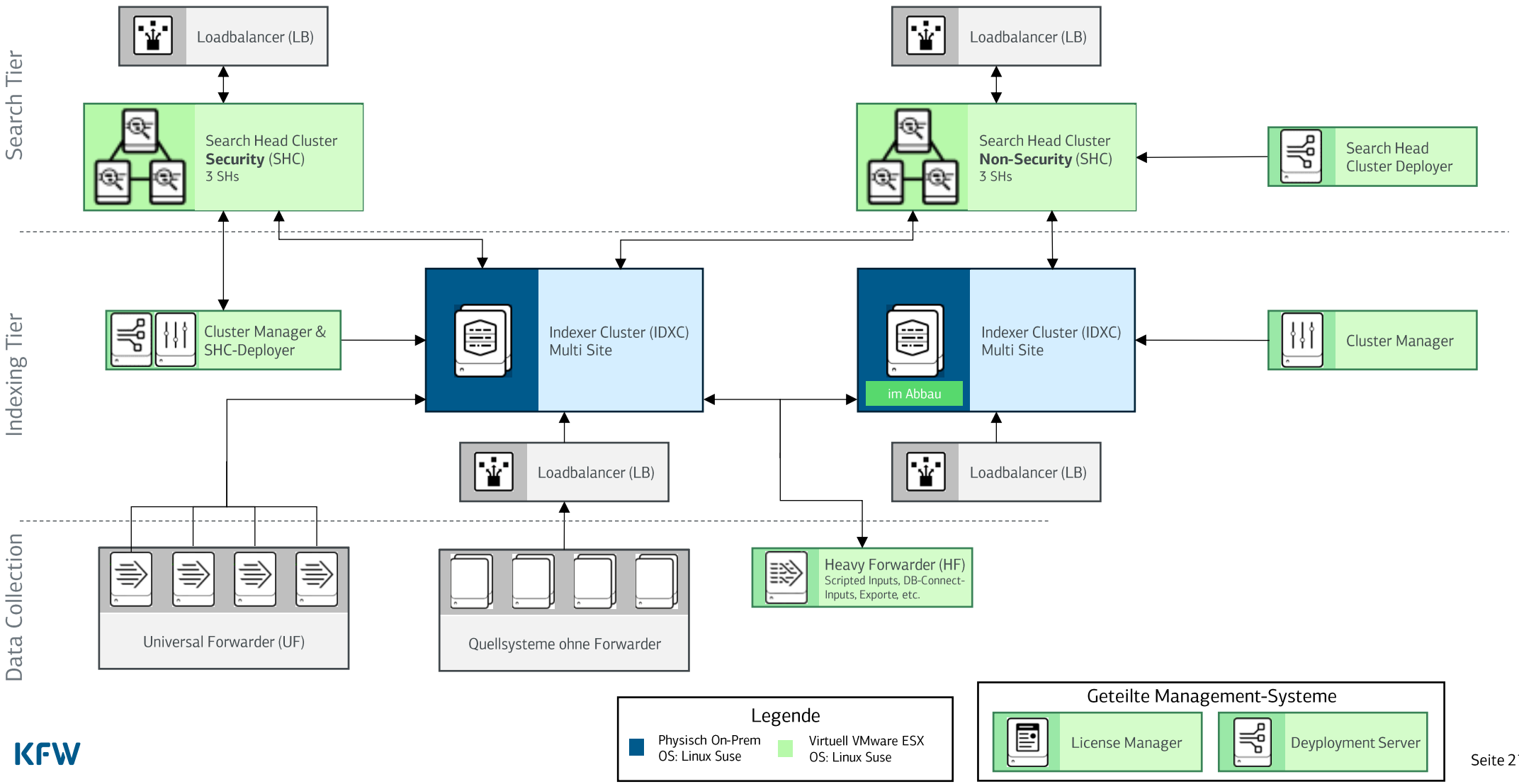


KFW
Bank aus Verantwortung

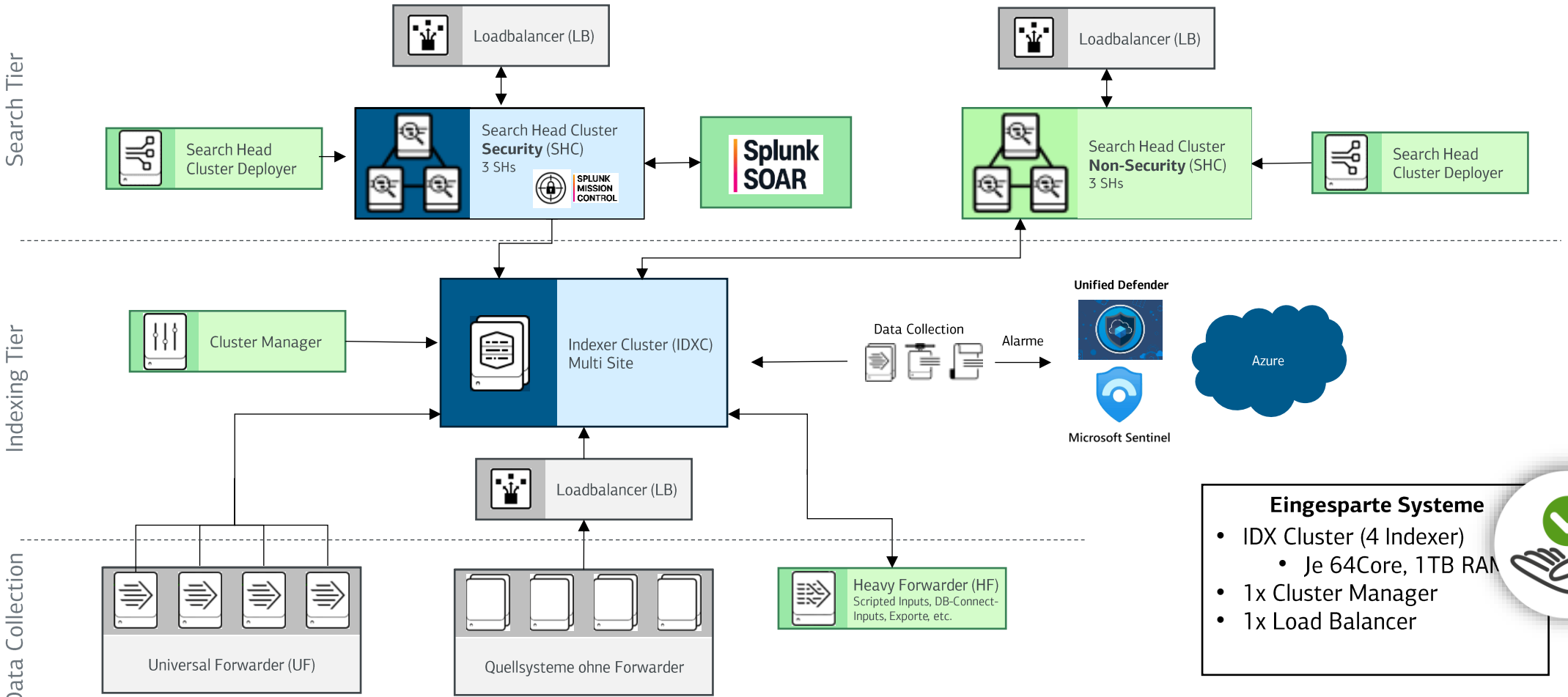
Next-Level-SOC

Architekturbeschreibung

PROD-Architektur Splunk IST-Zustand (vor Projektbeginn)



PROD-Architektur SOLL-Zustand (heutiger IST)



Eingesparte Systeme

- IDX Cluster (4 Indexer)
  - Je 64Core, 1TB RAM
- 1x Cluster Manager
- 1x Load Balancer

Legende

Physisch On-Prem
OS: Linux Suse

Virtuell VMware ESX
OS: Linux Suse

Geteilte Management-Systeme

License Manager

Deyployment Server

Zahlen Daten Fakten

PROD Umgebung

Dateninput	Server	Clients	Datenbanken	Netzwerkinfra.
~5 TB / Tag	3500+	8000+	450+	1000+

Indexer	Local Storage	Detections
30 (2x15)	~2 Petabyte	210+

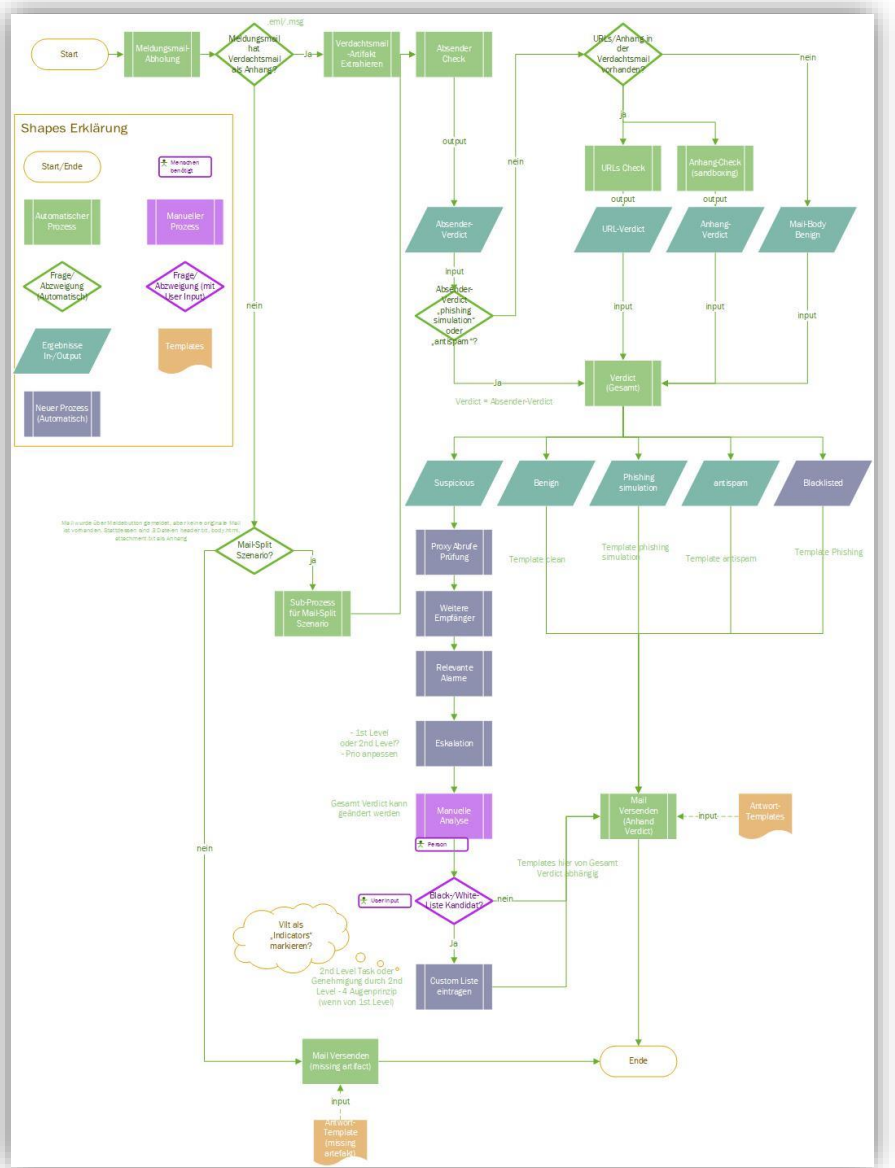
KFW
Bank aus Verantwortung

Next-Level-SOC

Workflow Beispiel

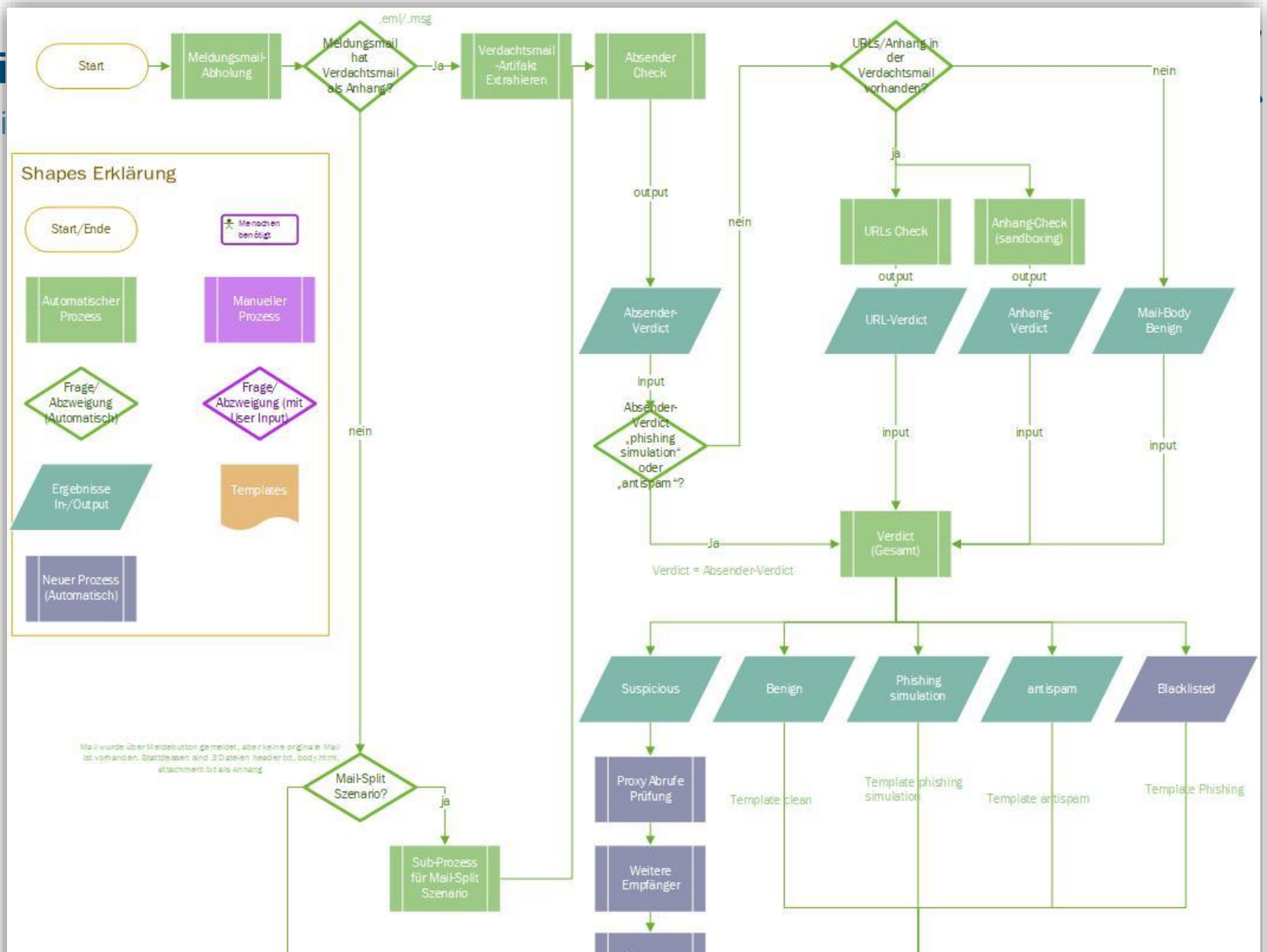
Der Phishing Workflow

High Level Visio

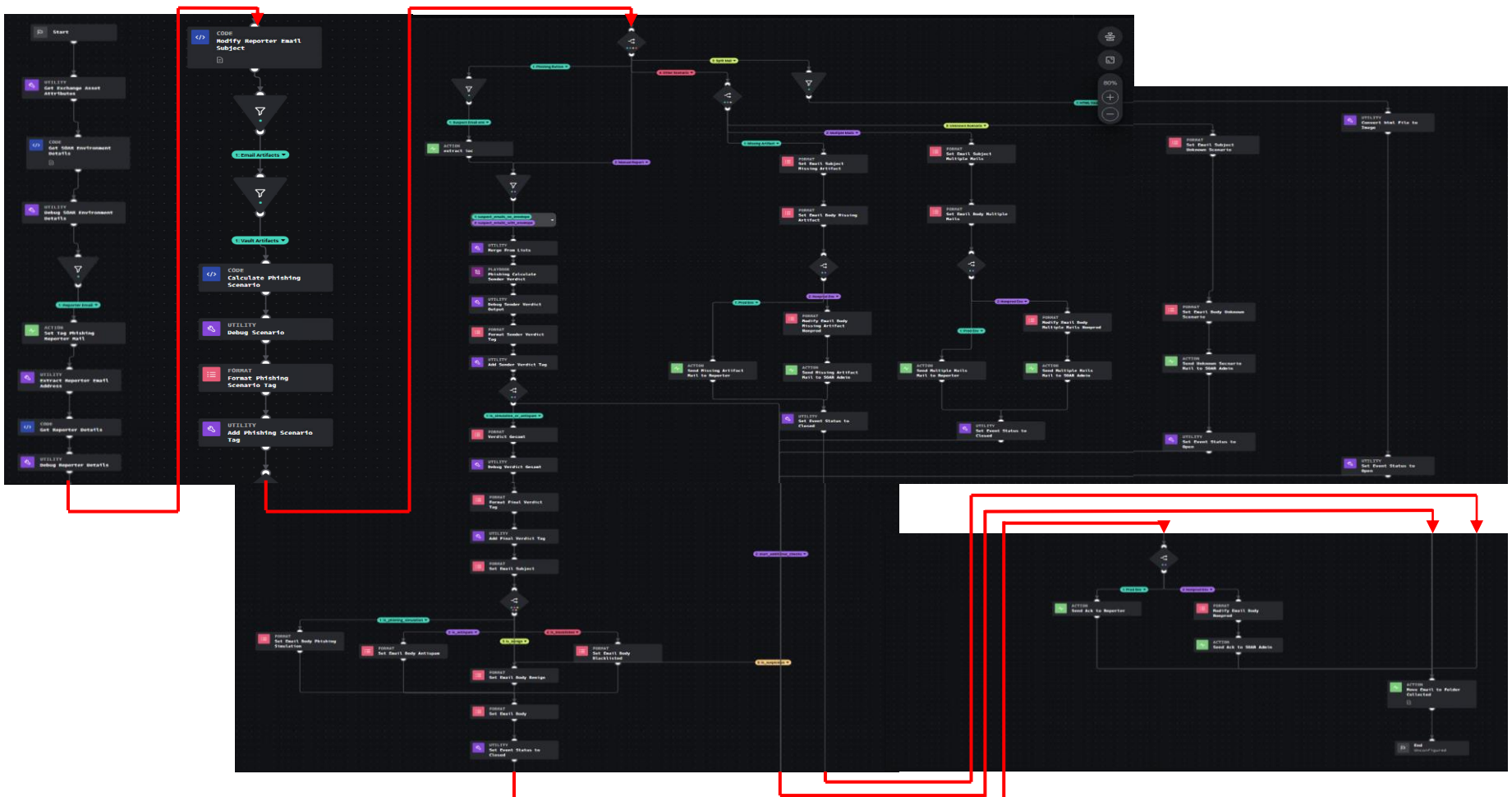


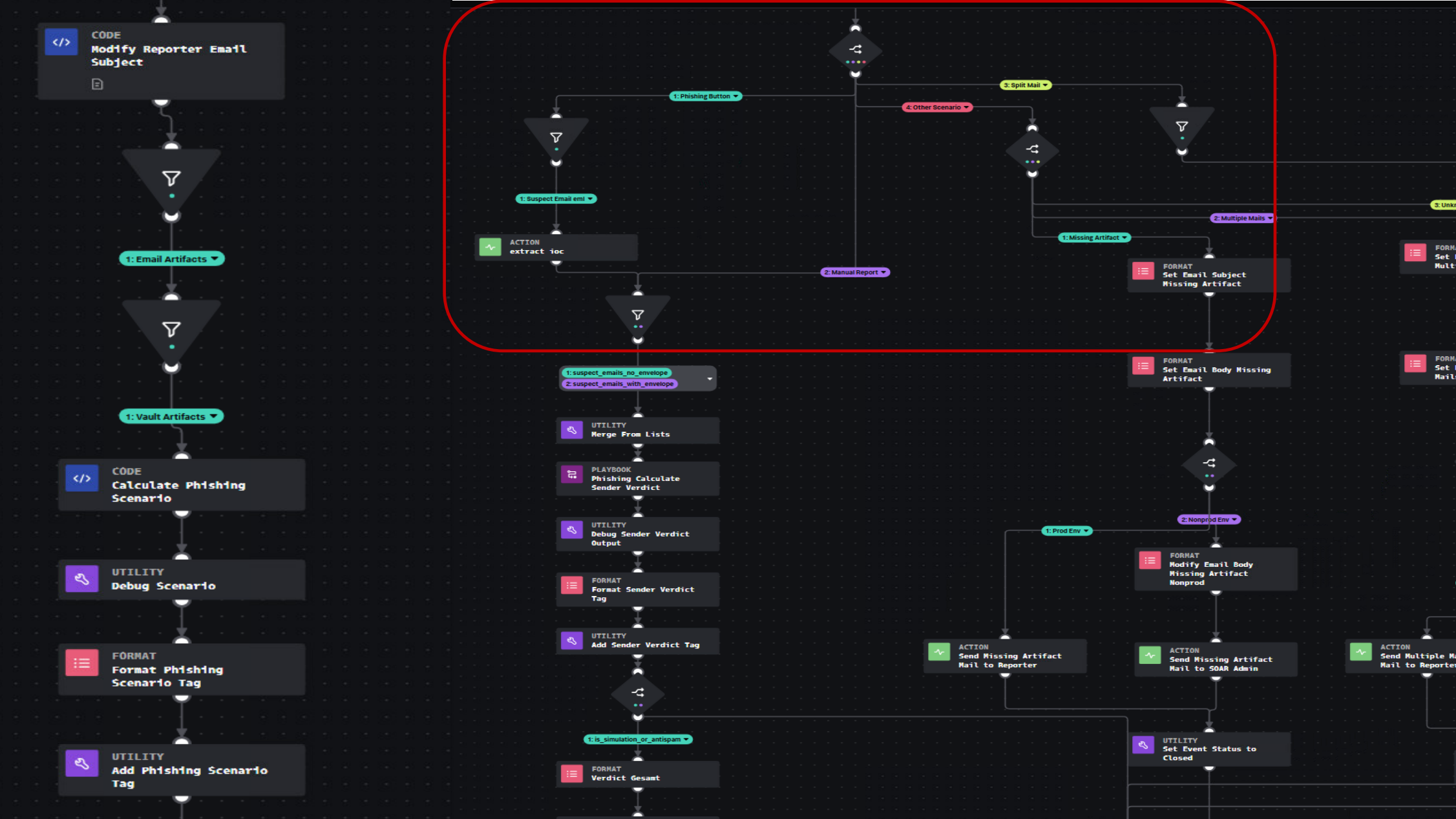
Der Phishi

High Level Visi



Splunk SOAR: Der Phishing Workflow




CODE
Modify Reporter Email Subject
1: Email Artifacts
1: Vault Artifacts
CODE
Calculate Phishing Scenario
UTILITY
Debug Scenario
FORMAT
Format Phishing Scenario Tag
UTILITY
Add Phishing Scenario Tag
1: Phishing Button
3: Split Mail
4: Other Scenario
1: Suspect Email eml
ACTION
extract ioc
2: Manual Report
2: Multiple Mails
1: Missing Artifact
FORMAT
Set Email Subject Missing Artifact
FORMAT
Set Email Body Missing Artifact
1: suspect_emails_no_envelope
2: suspect_emails_with_envelope
UTILITY
Merge From Lists
PLAYBOOK
Phishing Calculate Sender Verdict
UTILITY
Debug Sender Verdict Output
FORMAT
Format Sender Verdict Tag
UTILITY
Add Sender Verdict Tag
1: is_simulation_or_antispam
FORMAT
Verdict Gesamt
2: Nonprod Env
1: Prod Env
FORMAT
Modify Email Body Missing Artifact Nonprod
ACTION
Send Missing Artifact Mail to Reporter
ACTION
Send Missing Artifact Mail to SOAR Admin
UTILITY
Set Event Status to Closed

KFW
Bank aus Verantwortung

Next-Level-SOC

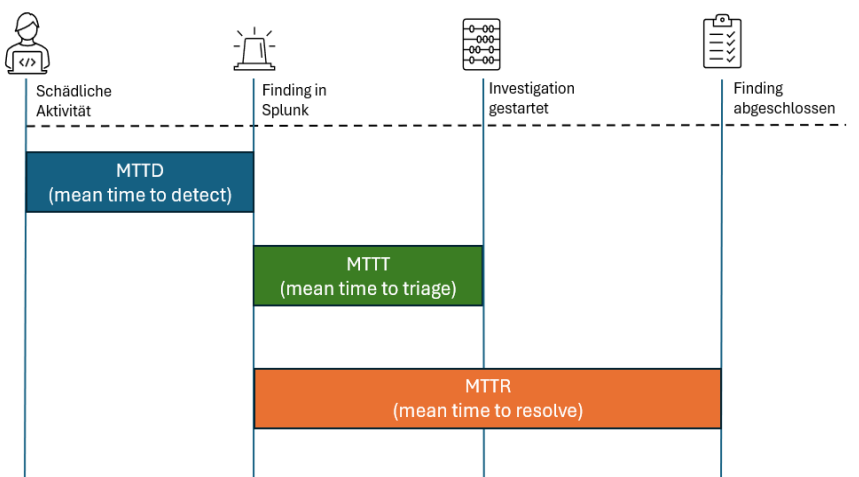
Ausblick

Ausblick

Cloudstrategie & Ausbau der Automatisierung

- Azure Sentinel Alarme und Unified Defender Alarme werden momentan via Splunk Azure Security App in die Splunk-Prod Umgebung gesendet und in Mission Control analysiert
- Verarbeitung findet im Kontext der Splunk ES im Mission Controll statt (wie bei anderen Usecases, über Detections und Findings).
- Mittelfristig ist die Multi SIEM Strategie zu prüfen. Abhängigkeit von der KfW Cloudstrategie

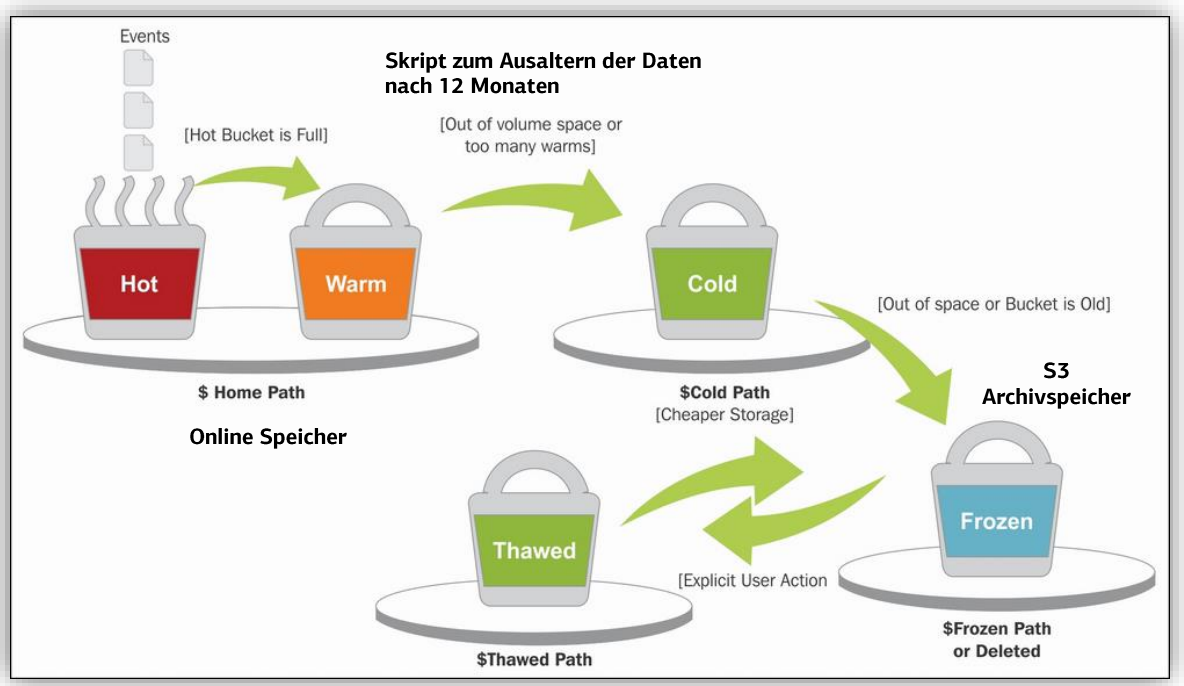
- SOAR Potential -> Mehr automatisierte SOAR Response Pläne / Automatisierungen auch für andere Use Cases / Detections!
- Überwachung von MTTD / MTTT/ MTTR Zeiten in Mission Control
- Automatisierte Eskalationen innerhalb des SOC und den beteiligten IT-Einheiten



Ausblick

Retention Erweiterung

- Erweiterung bei der Logaufbewahrung von **12 auf 24 Monate** für Security relevante Logs nach **BaFin** Hinweisen notwendig
- Abstimmung mit dem GPR erfolgt
- Technische Umsetzung erfolgt auf Basis von **Frozen Buckets**.
- Logs werden nach 12 Monaten von Cold in Frozen Buckets überführt
- Aufbewahrung in Frozen Buckets für insgesamt 24 Monate
- Analysten können bei Bedarf über einen Standard Change Frozen Logs wiederherstellen lassen (Thawed Buckets) um weitere Analysen durchführen zu können



KFW Bank aus Verantwortung

Vielen Dank.
Gerne Fragen.