KPMG

Praxisbericht SIEM

Erfahrungen beim Auf- und Ausbau von 24/7 verfügbaren Security Infomration und Event Management Systemen (SIEM) und Security Operations Centers (SOC)

—

Jan Stölting

22.11.2019

Agenda

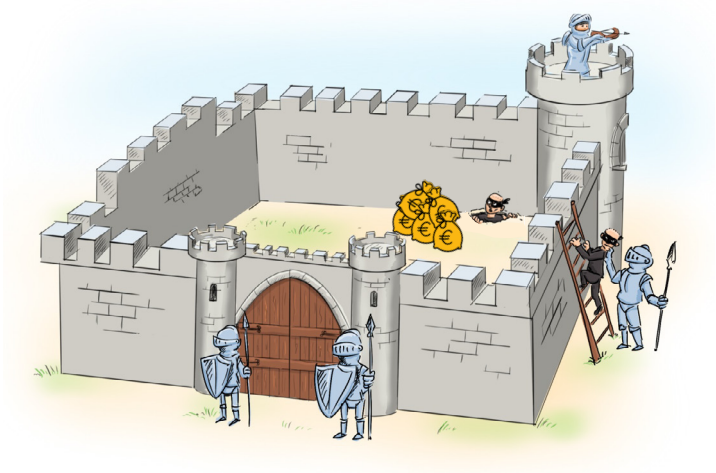
1	Hintergrund
2	Funktionsweise eines SIEM / SOCs
3	Erfahrungswerte: Herausforderungen, Aufwand und Nutzen eines SIEMs

KPMG

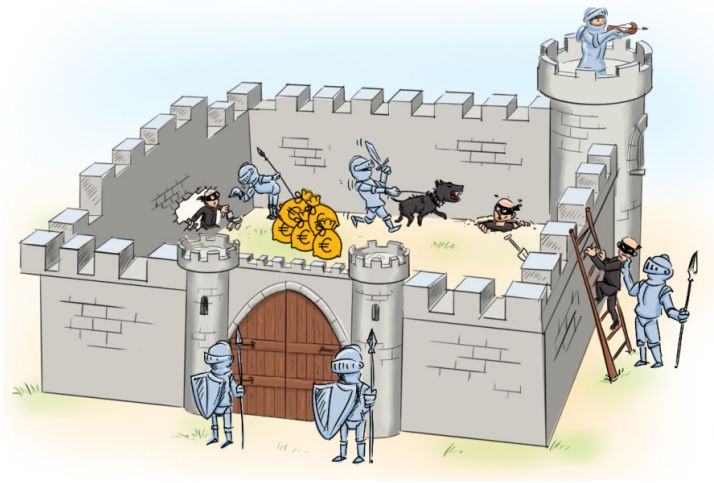
Hintergrund

Wozu brauche ich ein Security Information and Event Management (SIEM)?

Die Angreifer sind bereits im Netz



Cyber-Abwehr nur mit Perimeter (Firewall)-Schutz (rein präventiv)



Cyber-Abwehr mit Security-Monitoring (präventiv, detektiv und reaktiv)

Wesentliche Erkenntnis: Ein rein präventiver Ansatz der Cyber-Abwehr reicht nicht aus

Projekthintergrund

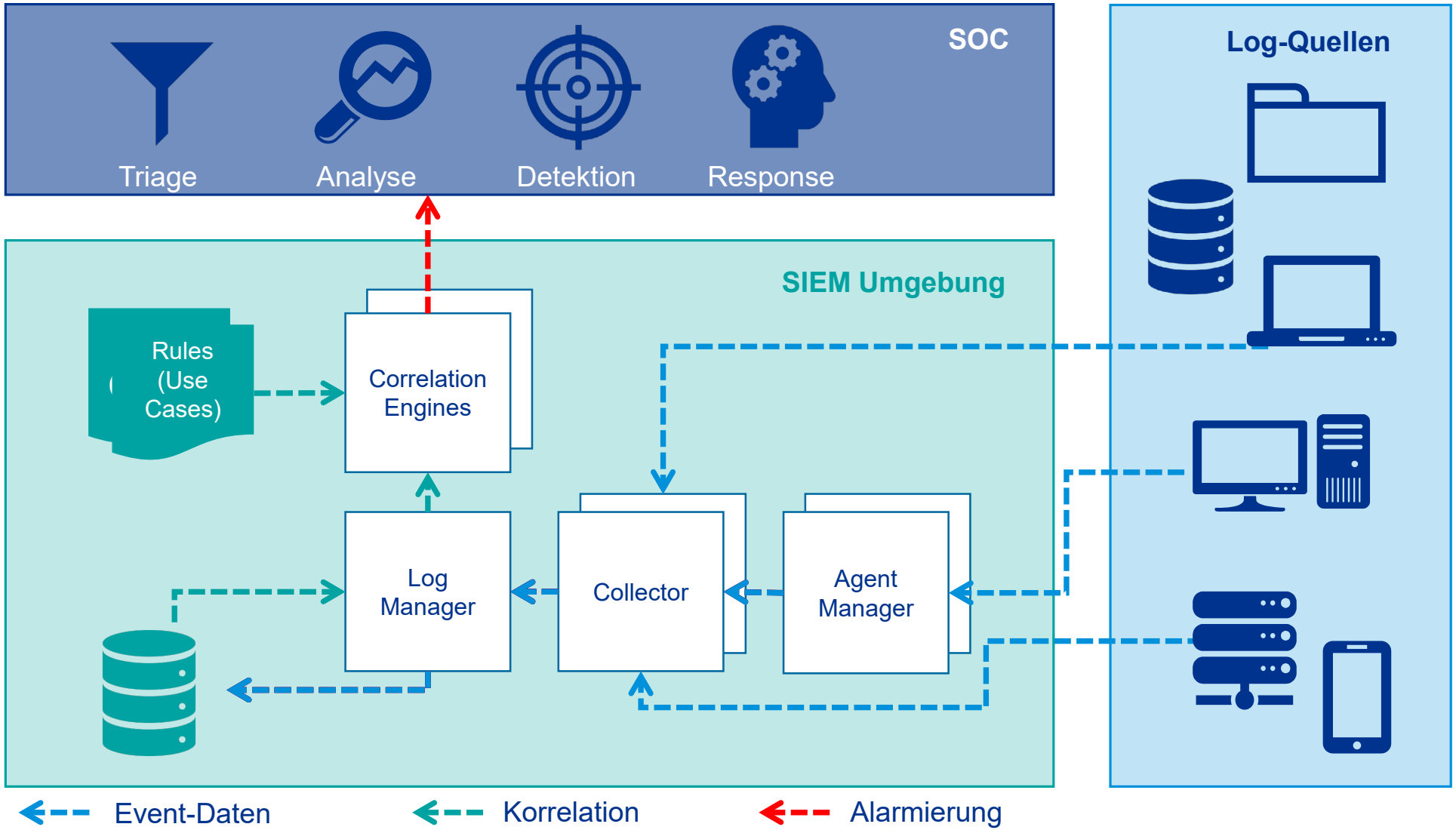
Projekt-hintergrund

- Projekt Teil eines Cyber Security Programms für ein **großes Finanzinstitut** in Deutschland
- Wesentliche Maßnahmen:
  - Definition und Umsetzung eines Betriebsmodells mit einer Teilauslagerung des Security Monitorings an einen SOC-Dienstleister zur 24/7 Überwachung
  - Ausbau der Breite und Tiefe der Überwachung der IT-Infrastruktur
  - Umsetzung einer Überwachung für fachspezifische Szenarien besonders relevanter Systeme
- Das Programm hat bis **Ende 2020** eine geplante Laufzeit von 3 1/2 Jahren
- Diese Präsentation basiert im Wesentlichen auf den konkreten Praxis-Erfahrung aus diesem Projekt sowie weiteren Aspekte aus 10 Jahren Erfahrungen in diesem Bereich

KPMG

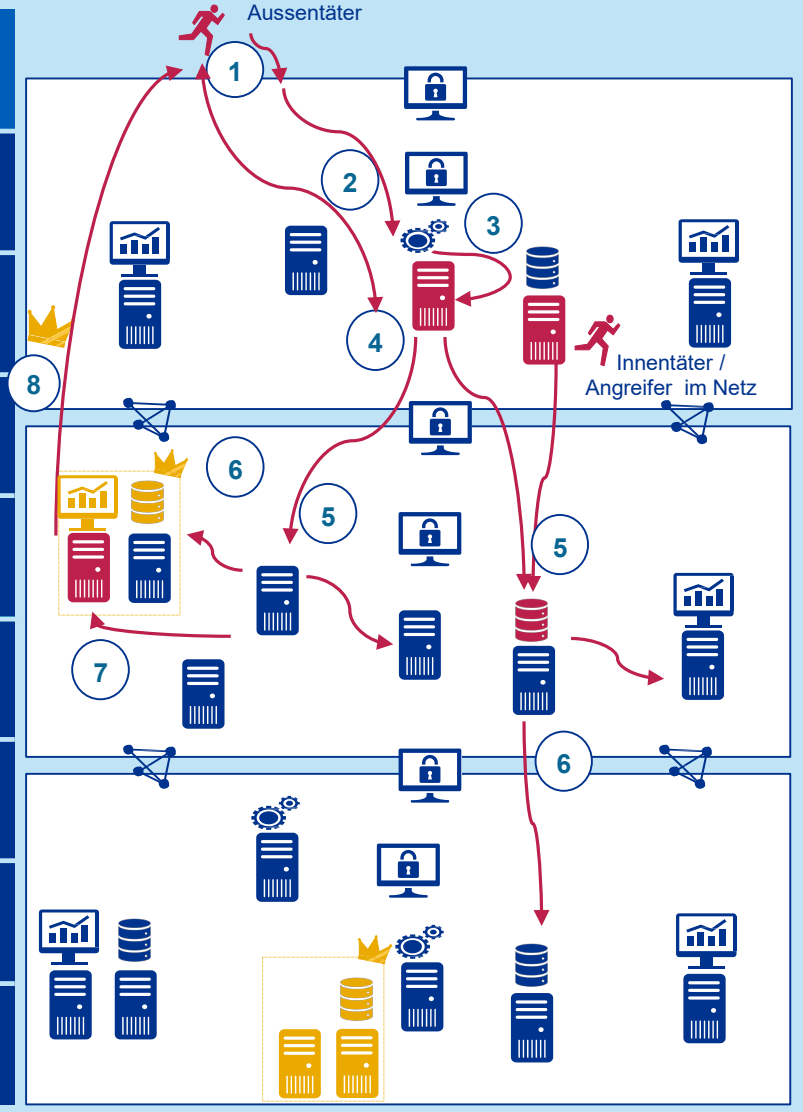
Funktionsweise eines SIEMs

Abgrenzung SIEM / SOC: Technische Sicht



Cyber Kill Chain zur Systematisierung und Ableitung von Detektionsszenarien

		Exemplarische Darstellung Detektionsszenarien
1	**External Reconnaissance**	Port Scans from External Source Scan Detected by IDS …
2	**Attack Delivery**	Attacks against Webservices Mail related Attack Delivery …
3	**Exploit & Installation**	Malware Detection Remote Code Execution …
4	**Command & Control**	Suspicious Outbound Traffic Command and Control Traffic …
5	**Local Compromise**	Suspicious Activity on Windows Suspicious Activity on Linux …
6	**Internal Recon**	Internal SNMP Scans Internal TCP Scans …
7	**Lateral Movement**	Suspicious Remote Logins Unusual Login Attempts & Account activity …
8	**Exfiltration/Manipulation**	Suspicious Outbound Data Transfer …



KPMG

Erfahrungswerte: Aufwand, Nutzen und Grenzen eines SIEMs

Erfolgsfaktoren bei der SIEM Anwendung

- Definition eines risikoorientierten Vorgehens zur Überwachung
- SIEM als Orchestrator von sicherheitsgebenden Technologien
- Dauerhafte Bearbeitung von Use Cases im Betrieb zur Reduktion von false positives
- Standardisierung im IT-Betrieb für Log / Sensor Onboarding
- Angemessene Balance zwischen Security und Compliance Überwachung
- Früher Einbezug von Datenschutz & Mitbestimmung
- Analysten im Security Operations Center (SOC)

Erfahrungswerte aus dem Projekt

Erfahrungswerte

- SIEM Implementierung erfordert relativ hohe Aufwendungen
- Notwendige Skills sind in der Regel nicht (vollständig) im Unternehmen vorhanden
- Implementierung und Betrieb des SIEM erfordert regelmäßige Abstimmungen und Unterstützung von anderen Teilen des Unternehmens (Fachbereiche, IT) sowie von Dienstleistern
- Benötigte Infrastruktur ist relativ komplex (abhängig von Art und Umfang der Überwachung und der Datenaufbewahrungsfristen)
- Zeitliche Dauer des Implementierungsprojektes großzügig wählen, um die Vorgehensweise an gewonnene Erfahrungen anpassen zu können

Aufwand für ein SIEM-System

Mit folgenden quantitativen Aufwands-Faktoren kann gerechnet werden (Angaben jeweils pro 1.000 Anwender):

- 1.000 EPS (Events per Second)
- 10 TB Plattenspeicher (netto)
- 1 Mio. EUR laufende Kosten p.a.

Personalbedarf (im eingeschwungenen Betrieb)

- 1 SIEM Koordinator
- 2 SIEM Regelentwickler
- 1 SIEM Asset Anbindungsexperte
- 2 SOC-Analysten je 1.000 Anwender (24x7-Abdeckung nicht berücksichtigt)

Disclaimer:

Die Angaben sind sehr grobe Schätzungen, die als Orientierung dienen sollen. Es wird von einer hohen IT mit hoher Komplexität ausgegangen. Es wird von überdurchschnitllich hohen Überwachungsanforderungen ausgegangen. Erkenntnisse aus mehreren Projekten wurden gemittelt.

Wesentlicher Nutzen eines SIEM-Systems

Zentrale Aspekte

- Zeitnahe Erkennung von Security Incidents durch automatisierte Korrelationen und manuelle Analysen
- Erhöhter Aufwand für Angreifer unentdeckt zu bleiben
- Automatische Erfassung, Überwachung und Speicherung von Logdaten bildet gute Grundlage für die nachfolgende Reaktion auf Security Incidents

Des Weiteren…

- Kenntnisse von und Verständnis über den Aufbau der eigenen IT werden signifikant gesteigert
- Kenntnisse von und Verständnis über Geschäftsprozesse und „Kronjuwelen des Unternehmens“ werden im Rahmen der Entwicklung fachlicher Use Cases gesteigert.
- Einsatz eines SIEM Systems sorgt in der Regel auch für eine Hygiene und Verbesserung der Prozesse insgesamt und insbesondere bei Dienstleistern bspw. root Anmeldung, scannen, etc.

Jan Stölting
Senior Manager, Cyber Security
T +49 69 9587-6273
jstoelting@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
The Squaire
60549 Frankfurt