Vom SIEM zur Erkennung von APTs

Die Evolution des Security Monitorings

Agenda

Kurzvorstellung KPMG Cybersecurity

Die Grundlagen

- SIEM
- Advanced Persistant Threats

Advanced Persistant Threats

- Definition
- Ablauf
- Erkennung und Maßnahmen
- Herausforderungen und Lösungsansätze

Die Evolution des Security Monitorings

- 3.1 SIEM 1.0: Sammlung von System Logs
- 3.2 SIEM 2.0: Korrelation von Daten
- 3.3 SIEM 3.0: Security Intelligence

KPMG Cyber Security

KPMG Cyber Security

IHR VORTEIL

Netzwerk
Unsere Spezialisten haben im Hintergrund Zugriff auf ein internationales Netzwerk von Fach-, IT- und Security-Spezialisten

Unabhängig
Wir sind an keinen Technologieanbieter gebunden – unsere Empfehlungen basieren auf dem, was für Sie am besten geeignet ist

DAX 30
KPMG berät zahlreiche DAX 30-Unternehmen zu Sicherheits-Themenstellungen – wir sind mit den Anforderungen von Großunternehmen bestens vertraut

Anerkannte Zertifizierungsstelle
KPMG zertifiziert Unternehmen nach ISO 27001 mit Zusatz ISO 27034 (application security)

Vertrauen
Um den vertrauensvolle Umgang mit Kundendaten nachweisen zu können, haben wir unsere Services nach ISO 27001 zertifizieren lassen.

IT-Compliance
KPMG hat umfassende Fach-Kenntnisse und Projekterfahrung im Bereich IT-Compliance (z.B. IT-Sicherheitsgesetz. BDSG)

Unsere Dienstleistungen

Wir begleiten unsere Kunden in allen Phasen ihrer Cyber Security Initiativen und Projekte

Wir haben Spezialisten für alle Cyber Security-Bereiche – von Security-Prozess- und Organisation-Beratung, über IT- und Industrieanlagen-Sicherheit bis hin zu Prüfungsexperten. Gerne stellen wir Ihnen unsere weiteren Dienstleistungen im Detail vor.

- Cyber resilience/BCM
- Cyber governance
- Cyber strategy & roadmap
- Privacy & data protection
- Cyber risk management

Strategy & governance

Security transformation

- Cloud/digital/mobile/social
- Industry 4.0/ICS
- Education & awareness
- Security transformation & architecture
- Identity & access management

- CERT/SOC/SIEM
- Penetration testing
- Advanced Cyber Defence (Center)
- Incident response & cyber forensic
- Application security

Cyber defence services

Assessments & assurance

- ISO 27001 certification
- “KRITIS”/“IT-Sicherheitsgesetz”
- Cyber maturity assessments
- Privacy assessments
- 3rd party risk management

Security Information and Event Management

Grundschema

Event → Protokollierung → Sammlung → Analyse → Bewertung → Reaktion

Analyse und Bewertung im Detail

Analyse → Bewertung → Reaktion

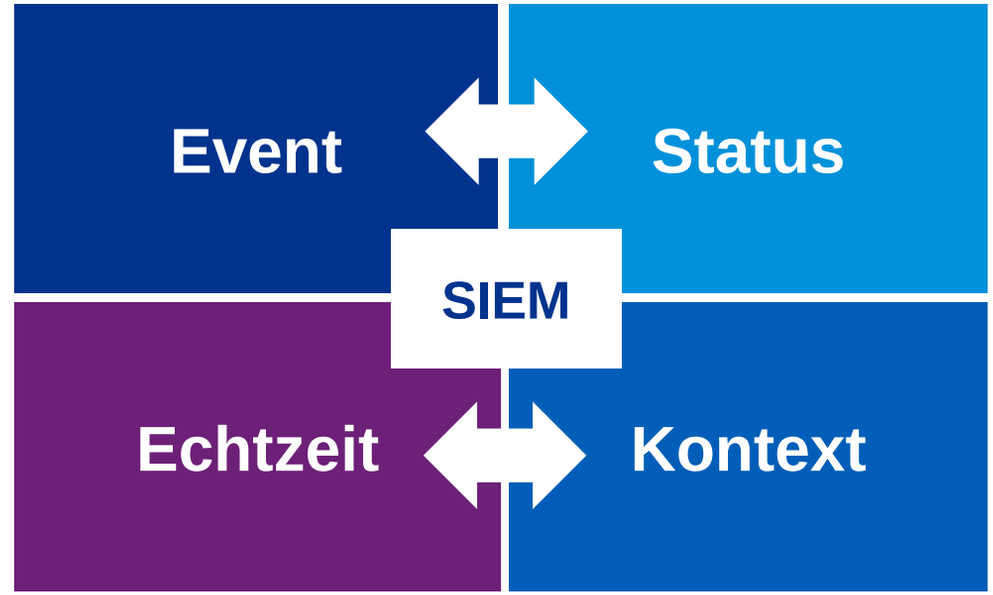
Analyse	Bewertung	Reaktion
Anzahl Events gesamt	Nicht relevant	Verwerfen/ Archivieren
	Kritisch	Alarmierung
	Unklar	Weitere Analyse

REDUKTION!

KOSTEN!

Security Information and Event Management

- Event: Kritische (System-) Ereignisse werden protokolliert
- Status: Änderungen an Konfigurationen werden erkannt
- Echtzeit: Kritische Ereignisse können zum Zeitpunkt des Entstehens entdeckt werden
- Kontext: Ereignisse können zeitlich mit anderen korreliert werden

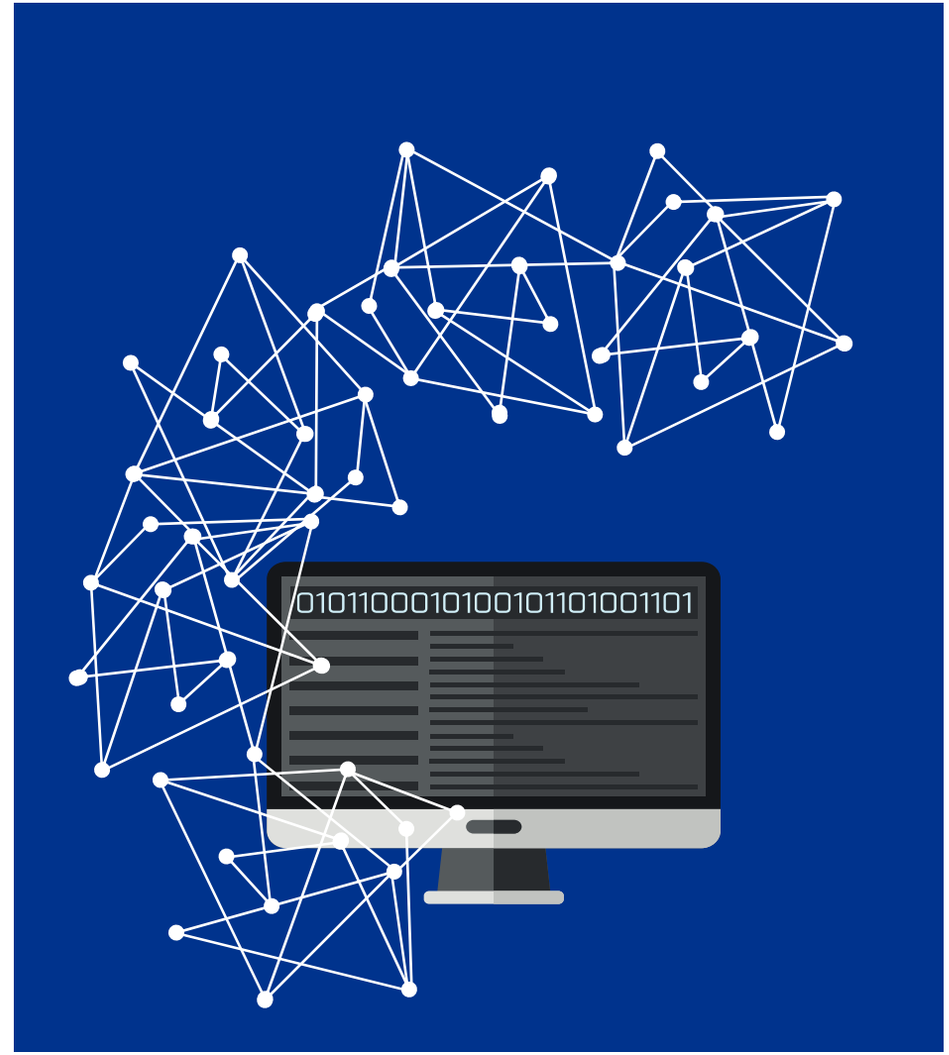


Ein vollständiges SIEM adressiert alle vier Aspekte!

Advanced Persistant Threats - Definition

Merkmale:

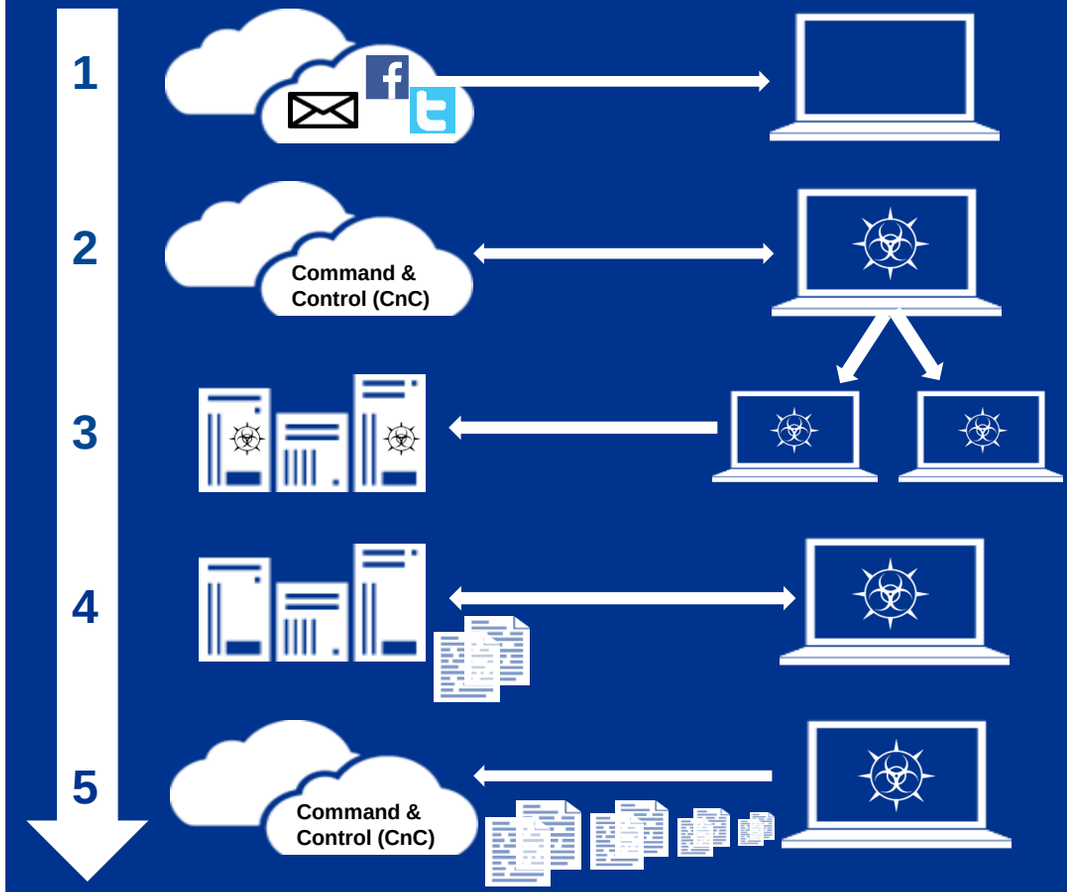
- Verwendet mehrere Kanäle (auch Social Media, Phishing, Spear Phishing, …)
- Verdeckte Vorgehensweise
- Lange Zeiträume
- Technisch ausgefeilt
- Auf das Ziel individualisiert
- Angreifer häufig hoch qualifiziert und gut budgetiert



Advanced Persistant Threats - Ablauf

Typisches Angriffsmuster

“Schwachstelle in Anwendung ausnutzen”, “Phishing” oder **“Remote-Exploits”,** um Zugriff zu erlangen



Zugang verschaffen

“Schwachstelle in Anwendung ausnutzen”, “Phishing” oder **“Remote-Exploits”,** um Zugriff zu erlangen

Festsetzen

Schadsoftware und “Hintertüren” werden installiert

Sichten

Ausspähung und Ausbreitung um Präsenz zu erhöhen

Sammeln

Beschaffung und Aggregation von wertvollen Daten

Herausbefördern

Datenübertragung nach Extern

Advanced Persistant Threats - Erkennung und Maßnahmen

Indizien für ein APT	Gegenmaßnahmen
Neu angelegte Administrator Konten	Regelmäßige Rezertifizierung
Anmeldungen aus ungewöhnlichen Ländern	Analyse und Auswertung der Source IP
Anmeldungen zu ungewöhnlichen Uhrzeiten	Definition/Anomalie Erkennung
Anmeldungen im Urlaub	Abgleich Personalinformationen
Ungewöhnliche Benutzer auf vertraulichen Daten	Datenklassifikation Einführung von Dateneigentümern Analyse der Zugriffe

APTs – Herausforderungen und Ansätze

Erkennung erfordert hohen Reifegrad

— Anbindung unterschiedlicher Systeme (HR, Zugangskontrolle, etc.)
— Daten müssen intelligent korreliert werden
— Große Datenmengen erfordern zielgerichteten Ansatz
— Entsprechend qualifizierte Mitarbeiter sind knappe Ressource
— Erkennung muss 24/7 aktiv sein
— Viele wertvolle Informationen sind in unstrukturierten Daten verborgen

Erfolgreiche Ansätze bei der Umsetzung

— Identifikation der schützenswerten Informationsgüter
— Erstellung von Use Cases im Top-Down Ansatz
— Risikoorientierte Vorgehensweise
— Zugriff auf externe Erfahrung
— Entscheidung über Sourcing (make or buy)

Die Evolution des Security Monitorings

Weiterentwicklung SIEM		
SIEM 1.0	**Herausforderungen:**	Anbindung von Systemen Interpretation von Einzelevents
	Ziel:	Einfache Angriffe („Elefant“)
	Struktur:	Netzwerkperimeter
SIEM 2.0	**Herausforderung:**	Korrelierung der Daten Sourcing/Ressourcen Management
	Ziel:	Einfache APTs („Tiger“)
	Struktur:	Tiefe Integration von Kunden und Dienstleistern
SIEM 3.0	**Herausforderung:**	Optimierung der Korrelation Anwendung von Security Analytics
	Ziel:	Komplexe APTs („Maus“)
	Struktur:	Komplette Integration („Identität als Perimeter“)

Technische Umsetzung der Anforderungen

Erfolgreich durch Teamarbeit

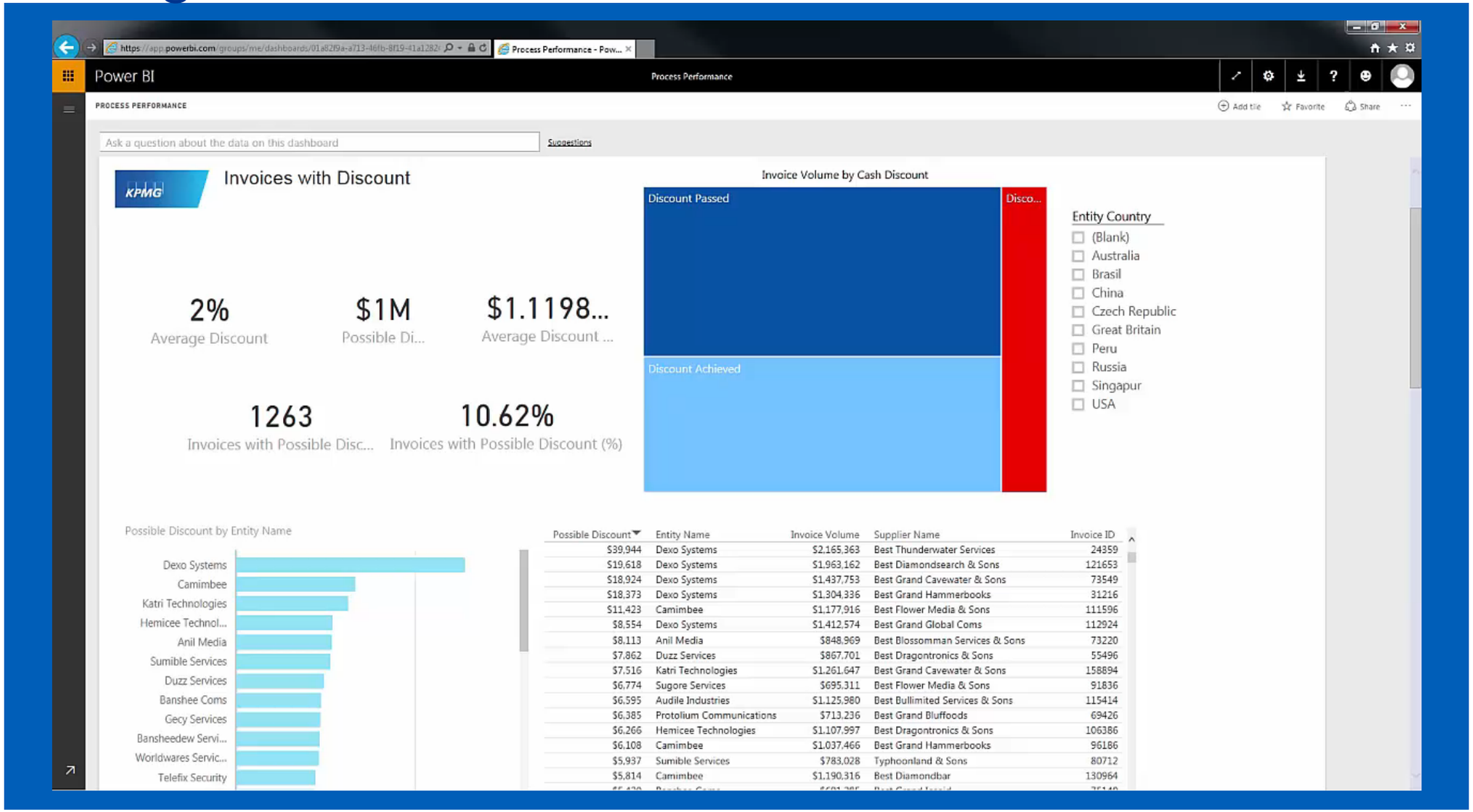
Entwicklung einer SIEM Strategie
Optimierung bestehender SIEM Installationen
Erstellung fachlicher Use Cases
Ableitung in technische Parameter
Umsetzung der Use Cases im SIEM
Umstellung auf SIEM als Managed Service

PROFI Innovative IT-Lösungen

Data Classification auf Regelbasis
Überwachung von unstrukturierten Daten
Identifizierung von Dateneigentümern
Erkennung von Anomalien im Dateizugriff

SailPoint™

Ein Ausblick: SIEM 3.0 und Cognitive Security Intelligence



Ihre Ansprechpartner

Hans-Peter Fischer
Partner, Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
Am Flughafen
60549 Frankfurt am Main

Sascha Schäffer
Manager, Cyber Security
T +49 69 9587-4850
sschaeffer@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
Am Flughafen
60549 Frankfurt am Main

www.kpmg.de/socialmedia

www.kpmg.de