SWS COMPUTERSYSTEME
Member of ACP Group

Healthcare for innovators.

Hans-Martin Kuhn

T.I.S.P. TeleTrustInformationSecurtiyProfessional

SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

- Historischer Abriss
- Cyberangriffe
- Logmanagement
- SIEM
- UseCases
- §§
- Fragen

Angriffe anno 70 bis heute

IT-IoT-OT

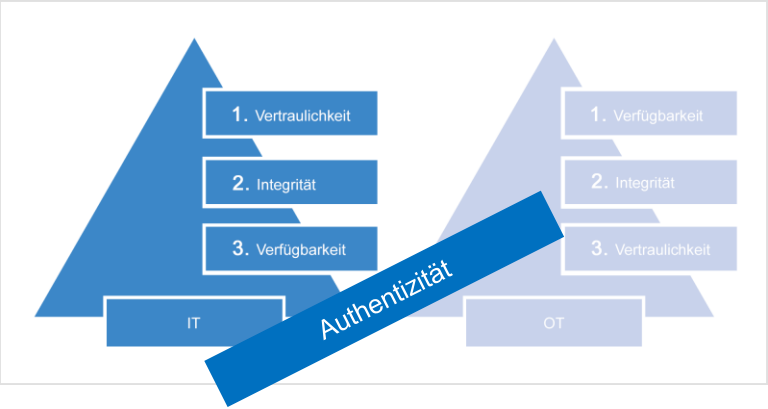
70er | 90er | 2000 | 2008 | 2010 | 2017 | **Heute**

Mafiaboy Denial-of-Service-Angriff im Jahr 2000

Emotet, Trickbot, Ryuk – ein explosiver Malware-Cocktail
Quelle: Heise-Online

Hintergründe

Aktive Cyberangriffe sind politisch oder kriminell motiviert und zielen auf….



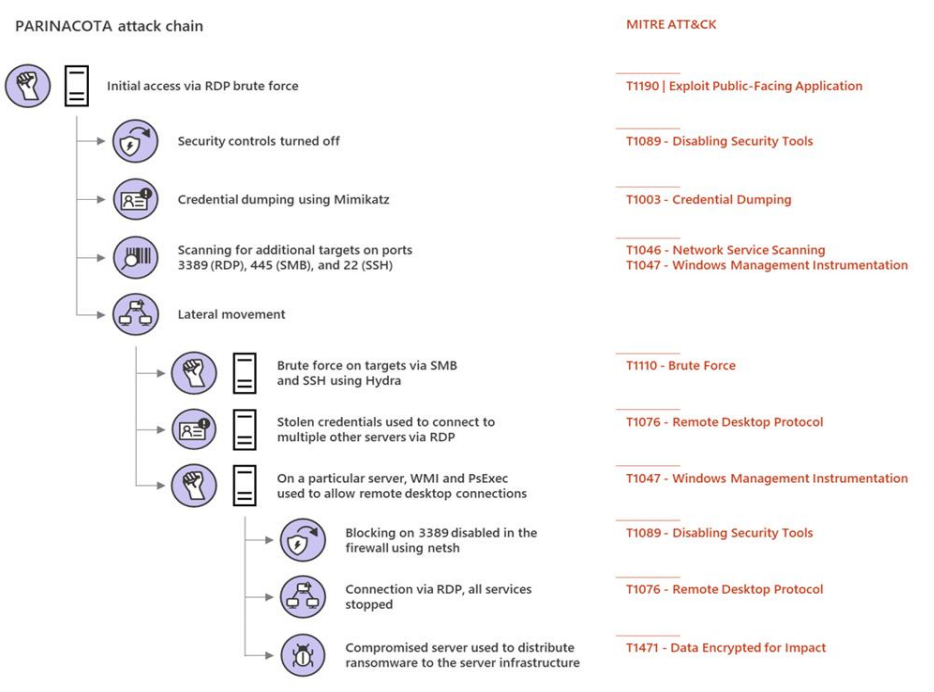
….ab!

HealthCare Security – Hausaufgaben gemacht?

Wenn ja, dann Security Check zum Review

Wenn nein, dann Security Check zum Reifegrad

Beispielhafter Ablauf eines Cyberangriffs



Quelle:https://www.heise.de/hintergrund/Cybercrime-Erpressung-auf-neuem-Niveau-4867430.html

Bedrohungen auch in der Medizintechnik

- Einschleusen von Schadsoftware über externe Geräte
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- (D)DoS Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Klinikumfeld

Was setzt man Cyberangriffen entgegen?

Zero Trust im Trend? (auch im medizinischen Bereich)

- Abschaffung von implizitem Vertrauen in einem Netzwerkbereich unter der Annahme, es könnte alles kompromittiert sein…
- …die Umsetzung ist allerdings ein Prozess…
- … daraus folgt, dass es umso wichtiger ist, ungewöhnliche Aktivitäten zu erkennen

Logdaten

- **Zentrale Sammlung ermöglicht:**
  - Compliance Dokumentation
  - Sicherung von Protokollinformationen
  - Traffic Monitoring
  - Anomalieerkennung
  - Bereitstellung von forensischem Material
  - Stärkung der Cybersicherheit
  - Effiziente IT
  - …

Healthcare for innovators.

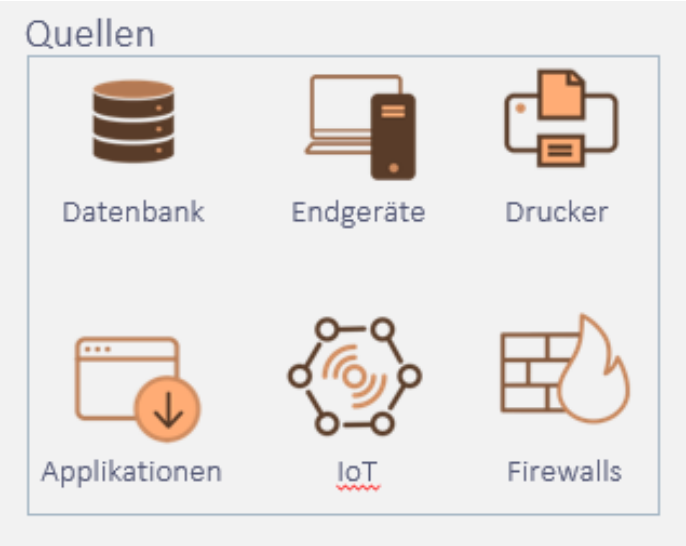
Was ist SIEM?

Security Information and Event Management (SIEM)

- Speichert Log-Daten und ermöglicht Netzwerküberwachung.
- Gesammelte Meldungen oder Log-Files werden korreliert, strukturiert und ausgewertet.
- Nutzt in der Regel Künstliche Intelligenz (KI) und Maschinelles Lernen.
- **Benötigt aber zusätzlich Regeln und Modelle, damit im Unternehmen einzelne Daten zueinander in Bezug gesetzt werden können.**

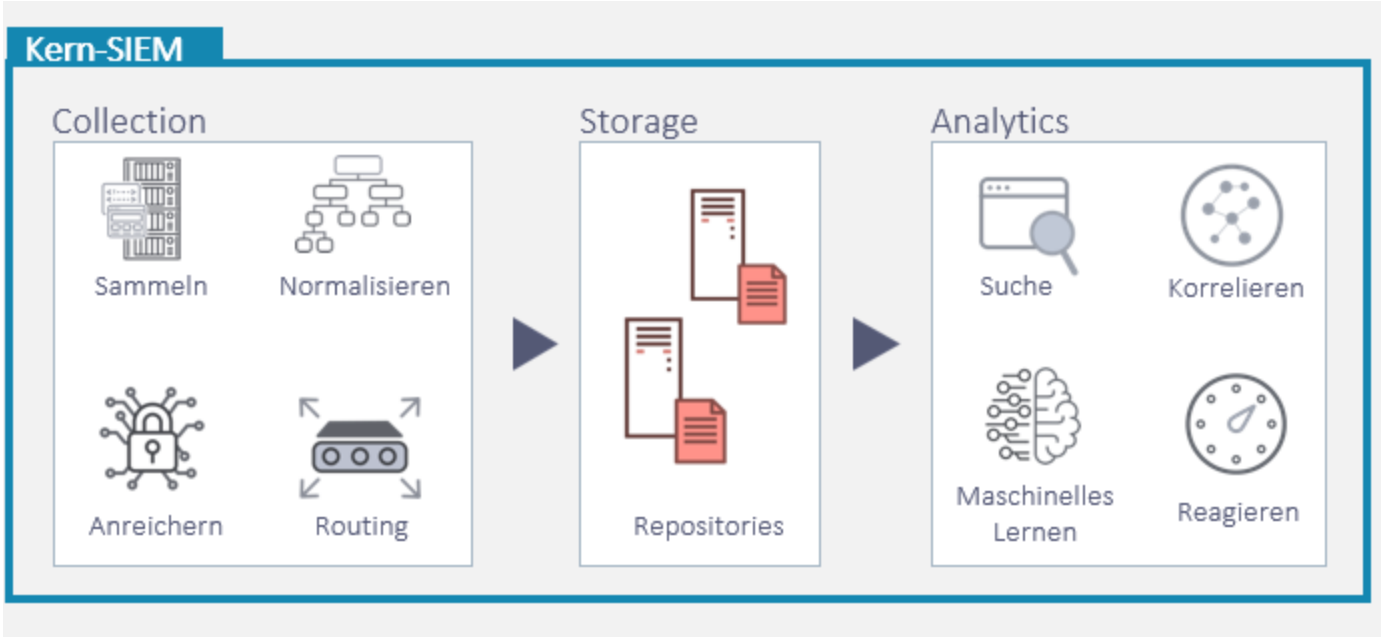
Log-Daten und Log-Management

Sammeln von Logs



Log-Daten und Log-Management

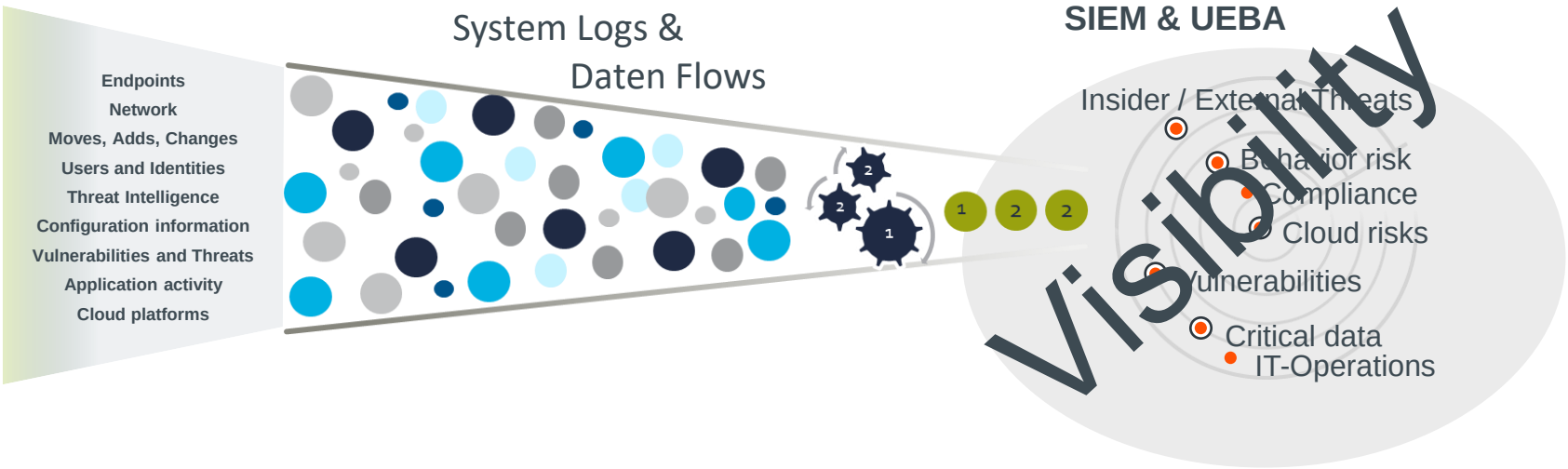
Normalisieren und Korrelieren



Healthcare for innovators.

Log-Daten und Log-Management

Sammeln von Logs und deren Auswertung



Use Cases Beispiele

- Unerlaubter Dateizugriff (Intellectual Property etc.)
- Ungewöhnliche Aktionen im Log
- Weniger Logs als üblich
- Neuer, unbekannter Windows Service angemeldet
- Start von nicht üblichen Diensten und Prozessen
- Server zu Internet Kommunikation
- Malware auf Server erkannt
- Neue lokale Benutzer / Administratoren sind erschaffen worden
- Web Applikationen (Logins)
- User Password Spraying
- Brute Force Erkennung
- …

Zusammengefasst

Zitat eines Kunden: „ich möchte wissen, wenn in meinem Netzwerk irgend etwas komisch ist“

Healthcare for innovators.

UEBA* – KI und Machine Learning

- Dynamische Unterstützung eines regelbasierten SIEM
- Hochverdächtige Aktivitäten
- Eingrenzung von Anomalien
- Deutlichere (automatisierte) Reduktion von false positives
- Ableiten von Risikoprofilen
- …

*User and Entity Behaviour Analysis

Compliance Reports auf Knopfdruck

- Policy Reports
- Network Access Reports
- Data Loss Reports
- Mobile Device Activities Reports
- Network Security Reports

Änderung gesetzlicher Rahmenbedingungen

- IT-Sicherheitsgesetz 2.0
- **§ 75c SGB V: IT-Sicherheit in Krankenhäusern**

Healthcare
for innovators.

Fazit

- IT-Security Check
- Pentest
- Awareness
- Technik
- Organisatorische Maßnahmen
- Compliance/Richtlinien
- Effektives Management

Healthcare
for innovators.

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

IT for
innovators.
Member of ACP Group