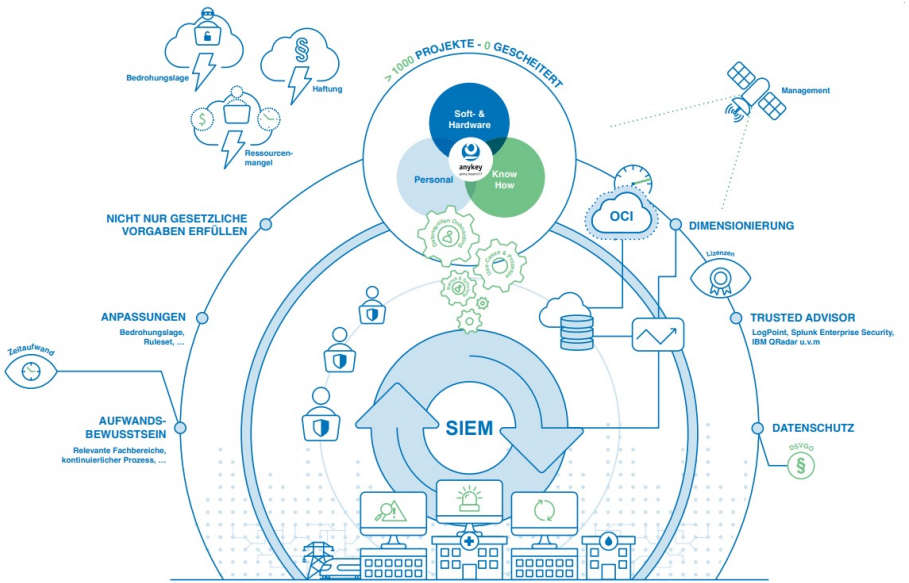
Sicherheitsarchitekturen mittels SIEM und XDR

Thomas Schwert

Berlin 19.10.2022

77. DFN-Betriebstagung



anykey
going beyond IT

anykey Expertise

- Seit 1999 spezialisiert auf Rechenzentrumsnahe Dienstleistungen
- 20+ Jahre Erfahrung in der Informationssicherheit
- Partner des BSI
- Gründungsmitglied im Cyber-Security-Cluster Bonn

Die Bedrohungslage

- COVID 19 ? Ukraine Krieg?
- Unsichere Betriebssysteme und Applikationen
- Unsicherheitsfaktor Anwender
- Abhängigkeit von komplexen IT Infrastrukturen
- Ständig steigendes Schadenspotential
- Fehlende Ressourcen in der IT / Fachkräftemangel

Regulatorische Vorgaben

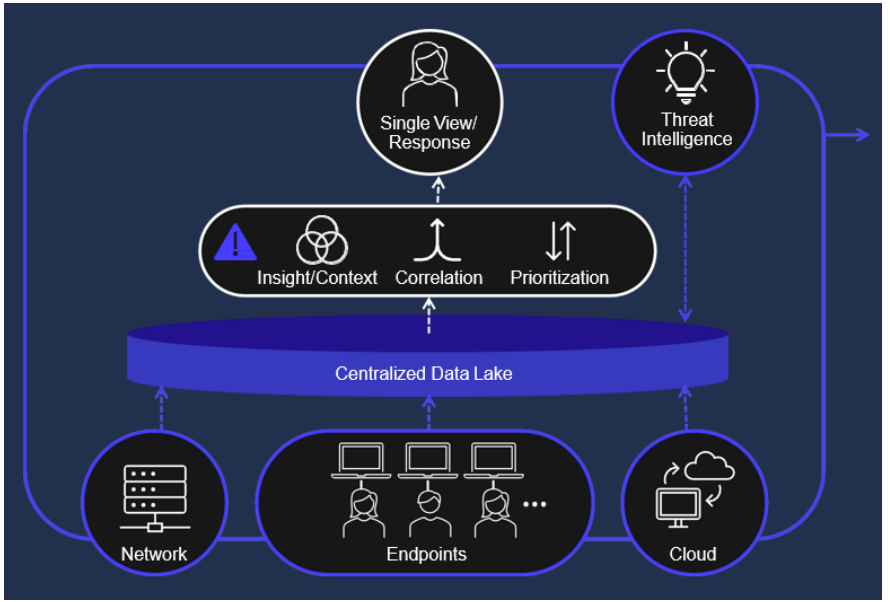
- Der Gesetzgeber reagiert auf die Risikolage mit regulatorischen Vorgaben

§


SOC?

XDR – Extended Detection and Response – SOC lite?

- Basiert i.d.R. auf EDR
- Erweitert um weitere Logs
- Data Lake in der Cloud
- Automatisierte Reaktion



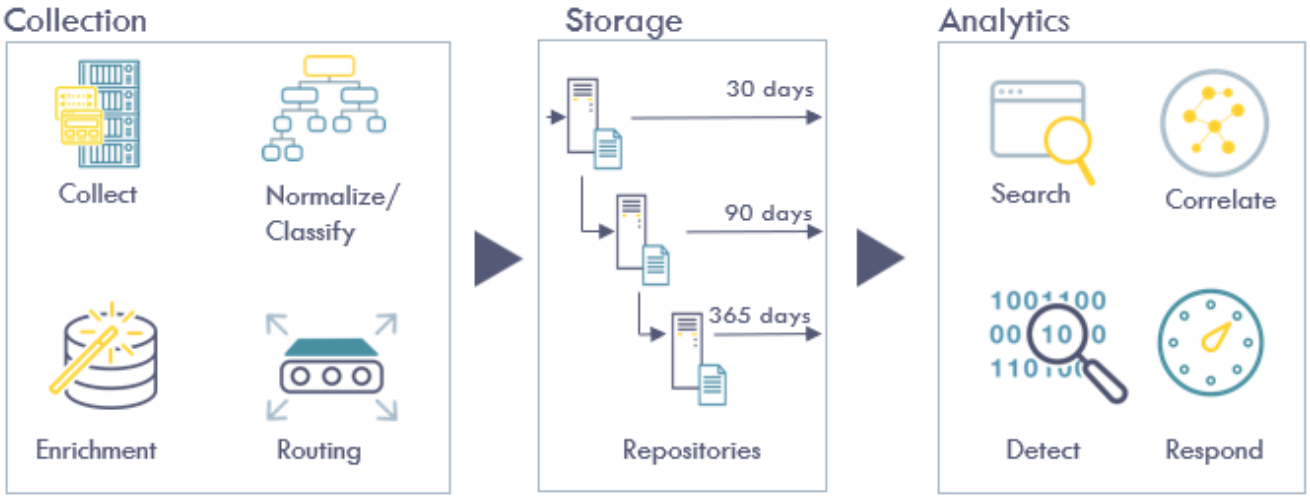
Die Zwickmühle CLOUD bei XDR Lösungen

+ Zusätzlicher Nutzen
+ geringer Aufwand

- Herausforderung Datenschutz
- Abhängigkeit vom Anbieter

SIEM – Security Information and Event Management

- **Etablierte Plattform im SOC (Security Operation Center)**



Warum SIEM?

- Silo- und Systemübergreifendes Logmanagement
- Einfaches handling der Logfiles
- Flexibel
- Erweiterbar
- Machine learning (UEBA)

SIEM sinnvoll einführen und betreiben

- Ziele definieren
- Interne Ressourcen prüfen
- Konzeption (Betriebsmodell, Datenquellen, Usecases, Plattform….)
- Erfahrene Spezialisten einbinden

→ Sicherheitsniveau gezielt und kontinuierlich verbessern

XDR als Ergänzung zu SIEM

- XDR und SIEM können wichtige Bausteine einer IT Sicherheitsstrategie sein
- Mehr Spielraum für Prävention einräumen
- SIEM als Chance

Vielen Dank für Ihre Aufmerksamkeit!

Für Fragen und Anregungen stehen wir gerne an unserem Stand zur Verfügung

Thomas Schwert

anykey GmbH

t.schwert@anykey.de

01511 4315182