

ENDLICH DURCHBLICK BEI DER IT-SECURITY

SIEM 2.0 – WICHTIGER BAUSTEIN FÜR WIRKSAME CYBER DEFENCE

Die Digitalisierung der Wirtschaft erhöht das Risiko für Unternehmen, Opfer von Cyber-Angriffen zu werden. Zu 100% kann sich niemand davor schützen. Deshalb werden Detektions- und Reaktionsmöglichkeiten immer wichtiger – das geht allerdings nur, wenn man seine Systeme permanent überwacht und sämtliche Daten analysiert. Zum Beispiel mit Security Information & Event Management (SIEM).

HÖCHSTE ZEIT, LICHT INS DUNKEL ZU BRINGEN

SIEM 1.0

SIEM 2.0



SIEM 1.0

ist Standard in vielen Unternehmen
zentralisiert Logdaten
detektiert per Tunnelblick
primär vorhergesehene Ereignisse
ist bei manueller Suche nach
Ungewöhnlichem nicht performant

ABER

Angriffsvektoren verändern sich
Angriffe werden gezielter,
langfristiger, unauffälliger
Social Engineering und Spear Phishing*
ist über Social-Media-Daten sehr einfach
Unternehmen werden durch
Digitalisierung** verwundbarer

**SIEM 1.0 reicht nicht mehr!
Genauer hinschauen!**

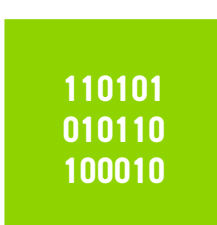
HERAUSFORDERUNG



Unzählige
Formate



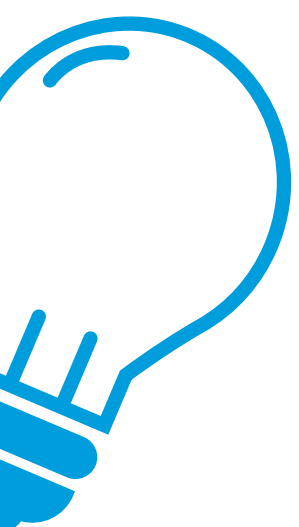
Enormes
Datenvolumen



Neue Such-
algorithmen



Fehlendes
Personal für die
Analyse



LÖSUNG

SIEM 2.0 – BIG DATA MACHT'S MÖGLICH

Unauffällige Angriffe erkennen durch:

1

Analyse aller
Datenformate

2

Speicherung
und Auswertung
großer Daten-
massen

3

proaktive
Angriffssuche
nach neuen
Angriffsmustern
– unabhängig
vorgegebener
Suchalgorithmen

4

Korrelation
weit auseinander-
liegender Events

5

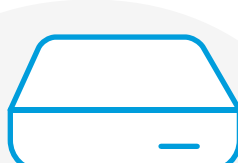
Spezifisches
Know-how von
IT-Security-Analysten

DIE BASIS SCHAFFEN IN 3 SCHRITTEN



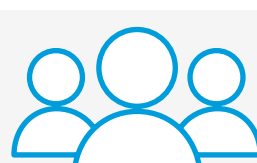
Big-Data-Technologien für Security aufbauen

- ✓ Big-Data-Initiativen bündeln
- ✓ Big-Data-Lösungen aufbauen
- ✓ hohe Datensicherheit herstellen



Speicherkapazitäten schaffen

- ✓ Enormes Datenvolumen aus SIEM 2.0 bewältigen
- ✓ Risikobewertung vornehmen – in kritischsten Geschäftsprozessen mit Pilotprojekt starten



Security-Analysten einstellen

- ✓ Dynamische Suchen entwickeln, Analyse und Hunting betreiben
- ✓ Beratung von außen dazu holen, eventuell outsourcen

Quellen

* Symantec Internet Security Threat Report (ISTR) 2016

** Bundesamt für Sicherheit in der Informationstechnik (BSI): Cyber-Sicherheits-Umfrage 2015

