Cyber Defence Konzepte für den Mittelstand

Christian Grusemann

Business Manager Security,
Bechtle Managed Service AG

Agenda.

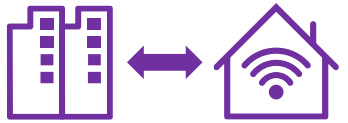
- Herausforderungen
- Lösungsansätze
- Zusammenfassung

Herausforderungen

IT Trends

Stellen Herausforderungen dar

Zunehmende Digitalisierung



Möglichkeit von überall aus zu arbeiten

IT-TRENDS

Corporate Social Responsibility

Eine sich weiterentwickelnde Bedrohungslandschaft

Fragestellungen im Angriffsfall

Zur Abwehr eines Angriffs

Wie groß ist das Ausmaß des Angriffs?

Wie kann ich die Systeme bereinigen?

Auf welchem Weg kam die Infektion ins Unternehmen?

Wie lange sind die Angreifer bereits im Netz?

Wurden Daten entwendet oder beschädigt?

Wer steckt dahinter - mit welcher Motivation?

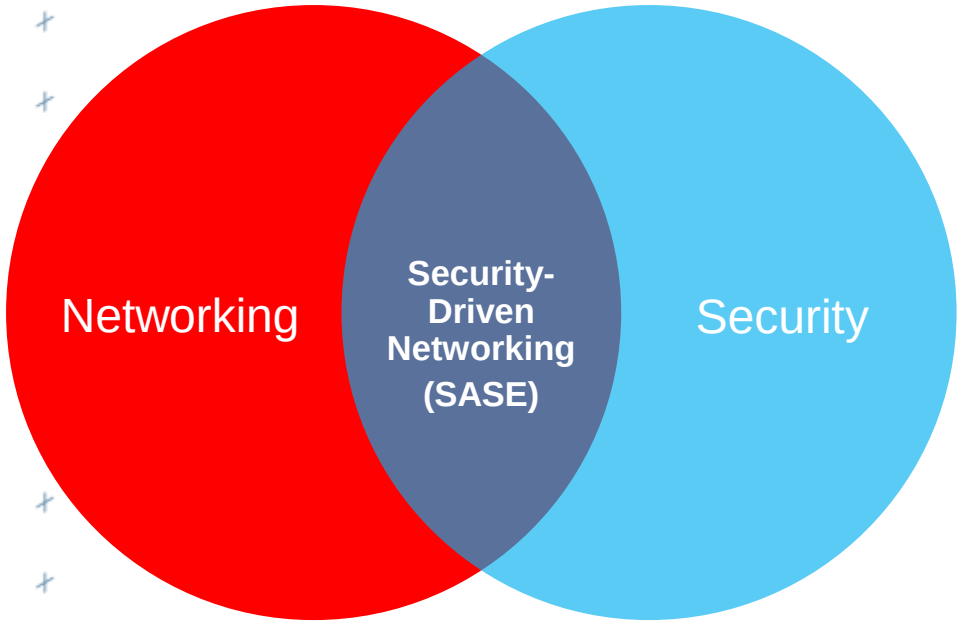
Können Sie mit 100%iger Sicherheit sagen, dass sich kein Angreifer in Ihrem Netz befindet?

Lösungsansätze

Trends und Technologien

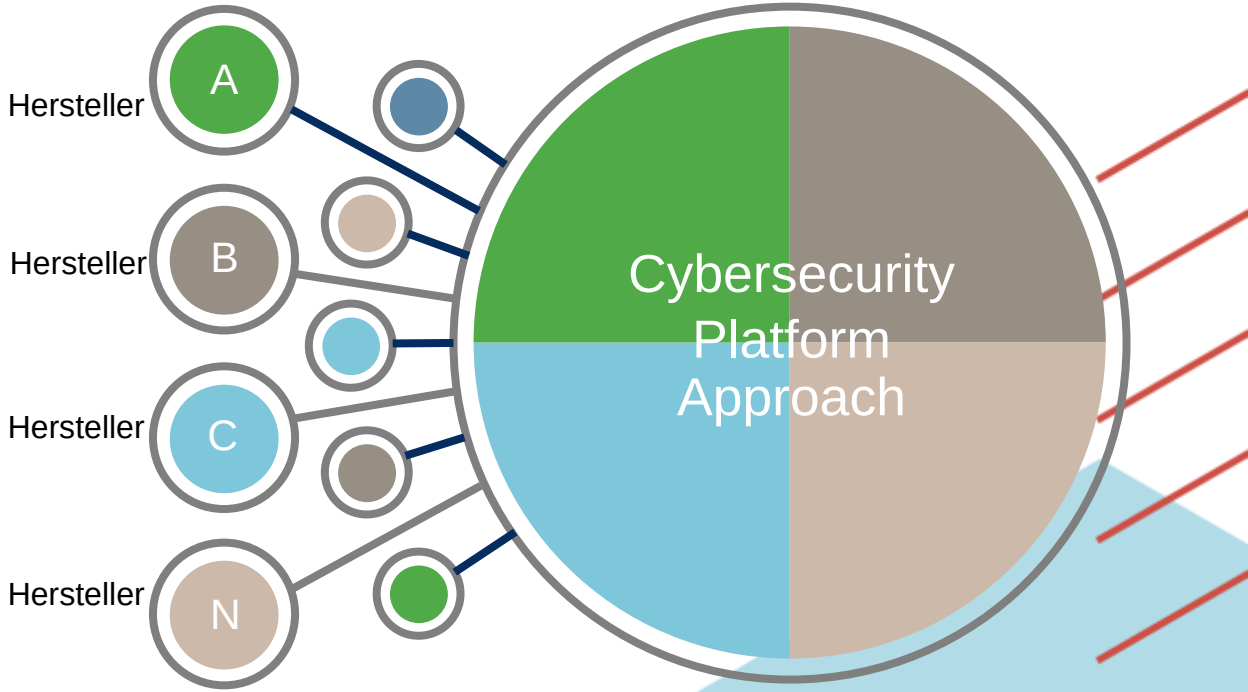
Zusammenführung und Konsolidierung

Zusammenführung von Networking und Security



Proof points: Gartner Enterprise Networking Market Forecast

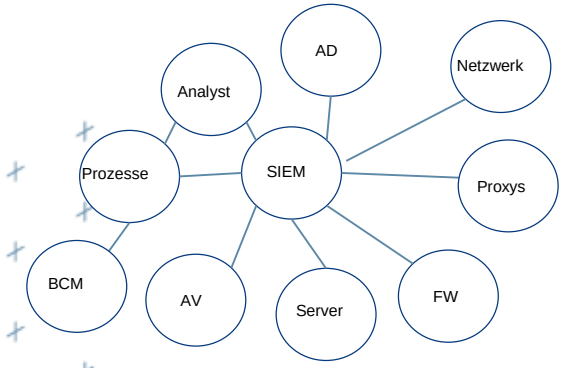
Konsolidierung von Security Point-Produktanbietern



Proof point: Gartner Cybersecurity MESH Architecture

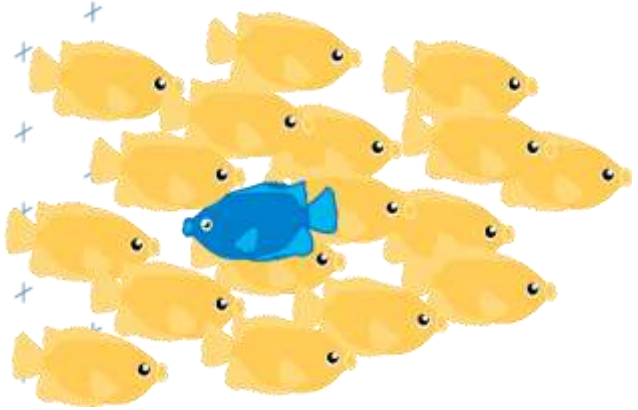
Ganzheitliche Betrachtung

SOC Ansätze im Vergleich



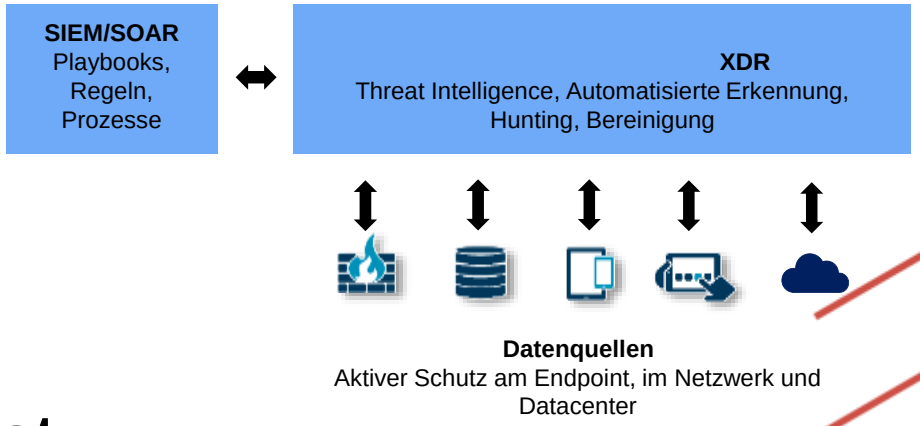
Klassischer Ansatz

- Spotbetrachtung
- Punktuelle Lösungen
- Vielzahl an Herstellern



User & Entity Behavior Ansatz

- Betrachtung der Geschäftsprozesse
- Automatisiertes Erkennen von Anomalien
- Erhöhung des Sicherheitsniveaus durch kontinuierliches Monitoring



Mischform

- Ein Hersteller
- Dienstleister Multivendor

Cyber Defence Konzept

Ohne ein SOC zu kaufen

- Security Awareness etablieren
- Security in der Infrastruktur auf den aktuellen Stand der Technik bringen.
  - EDR, NDR
  - FWs, IPS
  - Cloud
  - etc.
- Regelmäßiges Schwachstellen Management
- Regelmäßige Penetrationstests
- Notfall Maßnahmen etablieren
- Incident Response Dienstleister etablieren

Bechtle Kontaktdaten APT Hotline
Telefonnummer: +49 7132 981 2783
E-Mail-Adresse: help.sirt@bechtle.com

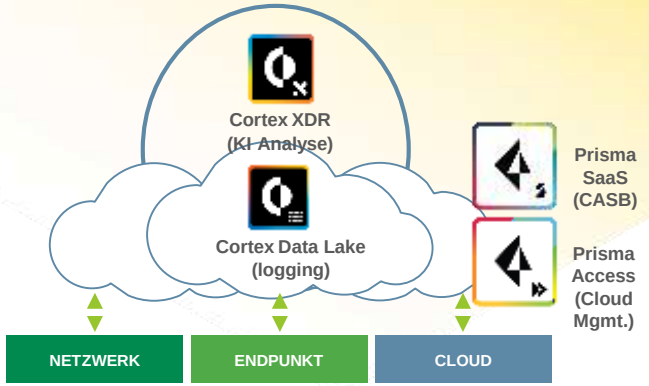
Bundesamt
für Sicherheit in der
Informationstechnik

Ganzheitlicher XDR Ansatz

Am Beispiel Sophos, Microsoft, Check Point, Palo Alto Networks

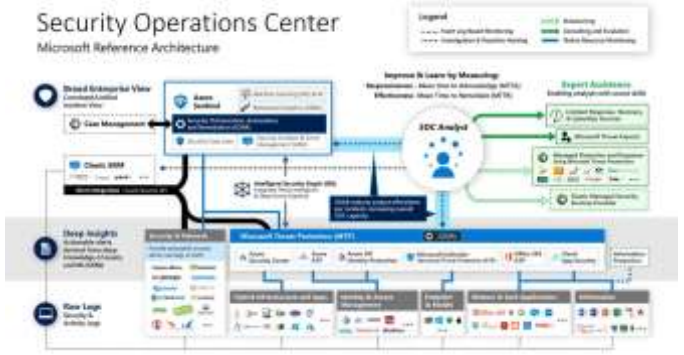
- Best-of-Breed wird ersetzt durch Security als System
- Erkennung und Eindämmung von Hacker-Aktivitäten
- Automatische Reaktion auf Vorfälle
- Analyse der Infektions- und Verbreitungswege
- Risk Profiling und Automatisierung
- Kommunikation von Netzwerk-, Endpoint-, Server und Verschlüsselungslösungen

Sophos Intercept X Architektur



Palo Alto Networks Cortex Architektur mit Demisto

Check Point Infinity Architektur

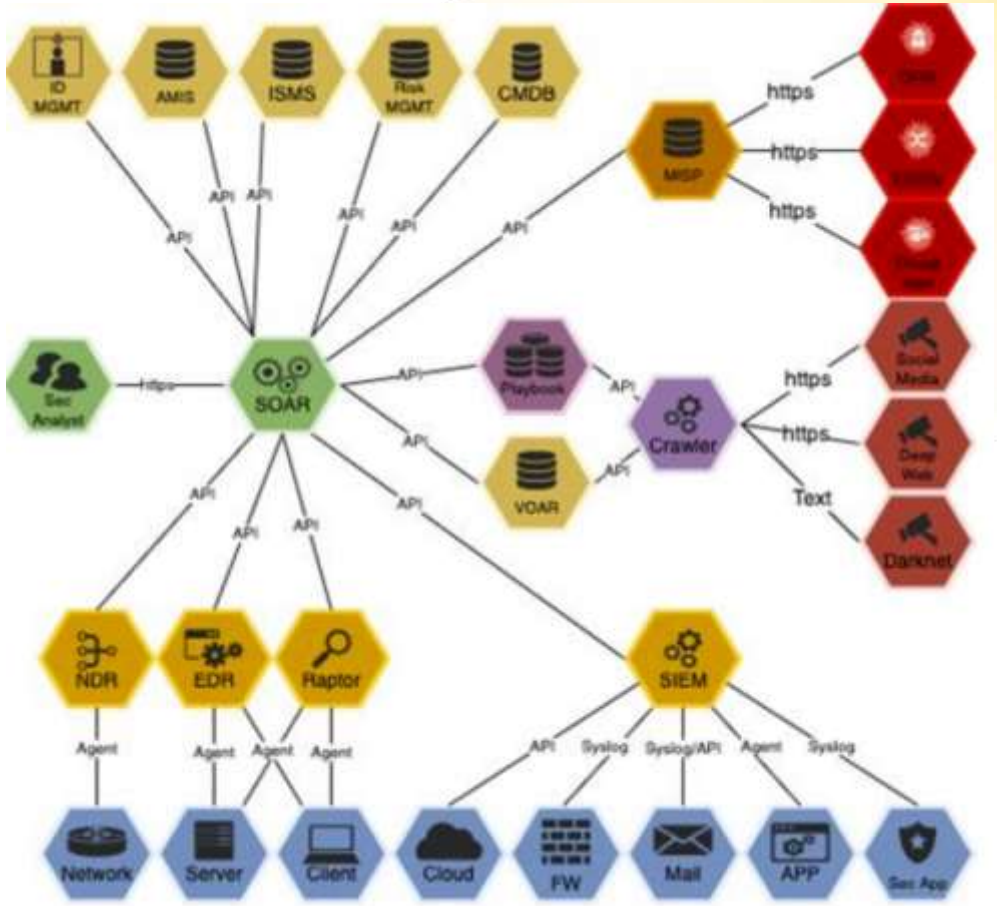


Microsoft Referenz Architektur

Security Operation Center

Bechtle SOC Architektur

- Kontinuierliche Aktivitätsprüfung
- Fortlaufendes Lernen
- Automatische Anomalienerkennung
- Sofortige Alarmierung
- Unsupervised Maschine Learning
- Überwachung der Aktivitäten am Endpunkt auf Kernel-Level
- Integration der Microsoft Informationen aus Microsoft Cyber Defence Operation Center (Uses Case Verstöße und anomales Verhalten aus der „MS Welt“)
- Integration LogPoint und MS Sentinel



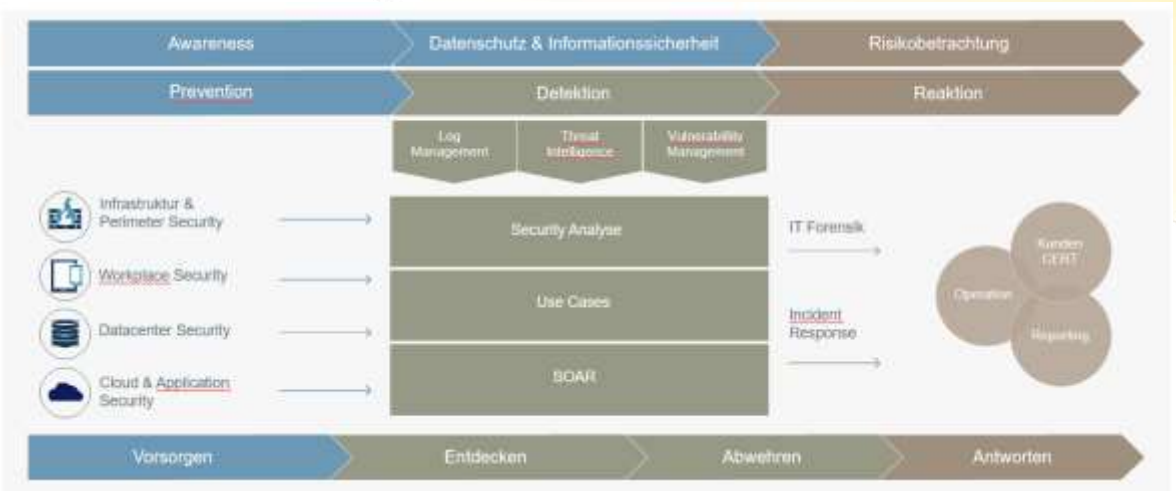
Zusammenfassung

Ende zu Ende Sicherheit

Zusammenspiel der Disziplinen notwendig

- Security Awareness
- Cyber-Defence Konzept
- Übergreifende Security-Architektur ob klassisch, hybrid oder Cloud
- Regulatorische Anforderungen beachten
- Incident- und Notfall-Management

Prevention-Detection-Reaction



Zeit für Fragen.

It-Security@Bechtle.com
Halle 7 Stand 7-441