Sicherheit im digitalen Zeitalter

Cyber Defense und Identitätsschutz als Grundpfeiler sicherer digitaler Prozesse

03.2024

- Einführung in die digitale Ära und Herausforderungen
- Bedeutung von Cyber Defense und Identity Management
- Dringlichkeit im Incident Response
- Rolle des Security Operation Center (SOC)
- Erkennung von Identitätsdiebstahl
- Innovative Abwehrmethoden
- Schlussfolgerungen und Best Practices

Digitale Ära und Herausforderungen

- Rasanter Fortschritt
- Vernetzte Welt
- Arbeitswelt im Wandel

Cyberangriffe
Ransomware, die Systeme sperrt; DDoS-Angriffe, die Dienste lahmlegen

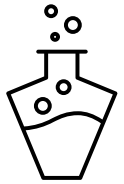
Datenschutz
Datenlecks bei großen Unternehmen, die Kundendaten offenlegen.

Identitätsdiebstahl
Phishing-E-Mails, die persönliche Daten stehlen.

Red Canary Threat Detection Report 2024

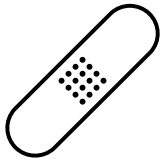
Phishing

Mark-of-the-Web (MOTW)
Powershell
MSIX files
Installer



SEO poisoning

Malvertising



Vulnerability exploitation

Quelle:redcanary

Cyber Defense und Identity Management

Cyber Defense		Identity Management
Schutzmaßnahmen und -technologien, die eingesetzt werden, um Cyberangriffe abzuwehren, Netzwerke zu sichern und Datenintegrität zu gewährleisten.	Definition	Prozesse und Technologien zur Verwaltung und Sicherung digitaler Identitäten, einschließlich Authentifizierung, Autorisierung und Nutzerverwaltung.
Unverzichtbar für die Abwehr von Bedrohungen wie Malware, Phishing und Ransomware-Angriffen. Schützt kritische Infrastrukturen und sensible Daten.	Bedeutung	Zentral für die Sicherheit, da es die richtige Zugangskontrolle gewährleistet und sicherstellt, dass nur berechtigte Nutzer Zugriff auf Ressourcen haben.

Warum sind diese Bereiche Ecksteine der digitalen Sicherheit?

Fundamentaler Schutz:
Sie bilden die Basis für eine robuste Sicherheitsarchitektur und sind entscheidend für die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten.

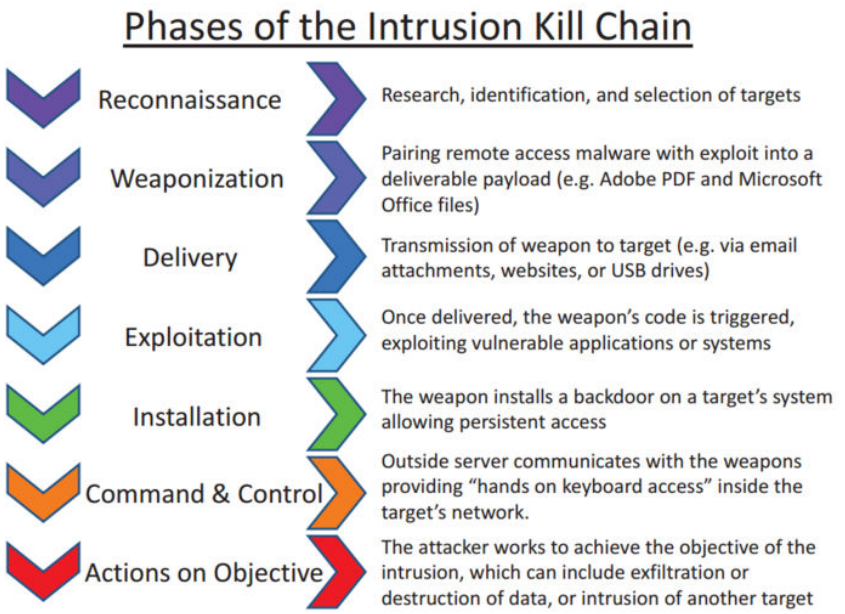
Vorbeugung und Reaktion:
Ermöglichen nicht nur die Vorbeugung von Sicherheitsvorfällen, sondern auch eine effektive Reaktion im Falle eines erfolgreichen Angriffs.

Vertrauen und Compliance:
Tragen wesentlich dazu bei, das Vertrauen von Kunden und Partnern zu erhalten und gesetzliche sowie branchenspezifische Compliance-Anforderungen zu erfüllen.

Was ist ein Angriff ?

Phasen des MITRE Att&ck Framework

- Einfallstor #1: Phishing Mail:
  Ziel: Code auf einem Client Rechner zum Laufen bringen
- Code nachladen (Fernsteuerung) – und festsetzen:
  - ein Account / Rechner gekapert
  - Schaden noch gering
- Umsehen was darf dieser User z.B. Zugriff auf File Server, SAP etc.:
  - Rechte erweitern – über Windows Eigenschaften an Admin Rechte kommen
  - weitere (Reserve) Zugänge schaffen
  - Spuren verbergen
- Wertvolle Daten finden und …
  - stehlen, verschlüsseln, verändern
  - vernichten, Kommunikation fälschen
  - Restore unterbinden)



Wo ist der „Angriff“ – wenn das Finanzsystem verschlüsselt ist?
Oder wenn die erste Phishing Mail das erste Postfach erreicht?

Incident Response – Jede Sekunde zählt

Bedeutung schneller Reaktionen bei Sicherheitsvorfällen

- **Sofortige Eindämmung:** Eine rasche Reaktion kann die Ausbreitung von Malware verhindern und die Kontrolle über betroffene Systeme schnell wiederherstellen.
- **Schadensbegrenzung:** Je schneller ein Vorfall erkannt und behoben wird, desto geringer ist der potenzielle Datenverlust und Schaden für das Unternehmen.
- **Wiederherstellung des Betriebs:** Eine effiziente Incident Response ermöglicht eine schnellere Wiederherstellung der betrieblichen Abläufe und minimiert Unterbrechungen.

Auswirkungen verzögerter Reaktionen auf die Unternehmenssicherheit

- **Erhöhtes Risiko von Datenlecks:** Verzögerungen in der Reaktion erhöhen die Wahrscheinlichkeit, dass sensible Informationen kompromittiert werden.
- **Finanzielle Verluste:** Die Kosten eines Sicherheitsvorfalls steigen mit der Zeit, die benötigt wird, um ihn zu bewältigen, erheblich an.
- **Reputationsverlust:** Ein langsamer Umgang mit Sicherheitsvorfällen kann das Vertrauen von Kunden und Partnern beeinträchtigen und langfristig das Image des Unternehmens schädigen.
- **Rechtliche Konsequenzen:** Verzögerungen in der Incident Response können dazu führen, dass gesetzliche Meldefristen nicht eingehalten werden, was zu Strafen und Bußgeldern führen kann.

Fragestellungen im Angriffsfall

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?

Die Rolle des Security Operation Centers (SOC)

Was ist ein SOC und welche Funktionen erfüllt es?

Definition: Ein SOC ist eine zentrale Einheit, die sich mit Sicherheitsvorfällen auf organisatorischer Ebene befasst und diese überwacht, bewertet und darauf reagiert.

Funktionen:

- **Überwachung und Analyse:** Kontinuierliche Überwachung und Analyse der Netzwerkaktivitäten auf Anzeichen von Sicherheitsverletzungen.
- **Vorfallmanagement:** Koordination der Reaktion auf Sicherheitsvorfälle, einschließlich Eindämmung, Untersuchung und Wiederherstellung.
- **Bedrohungsintelligenz:** Sammlung und Analyse von Informationen über aktuelle Bedrohungen und Schwachstellen.

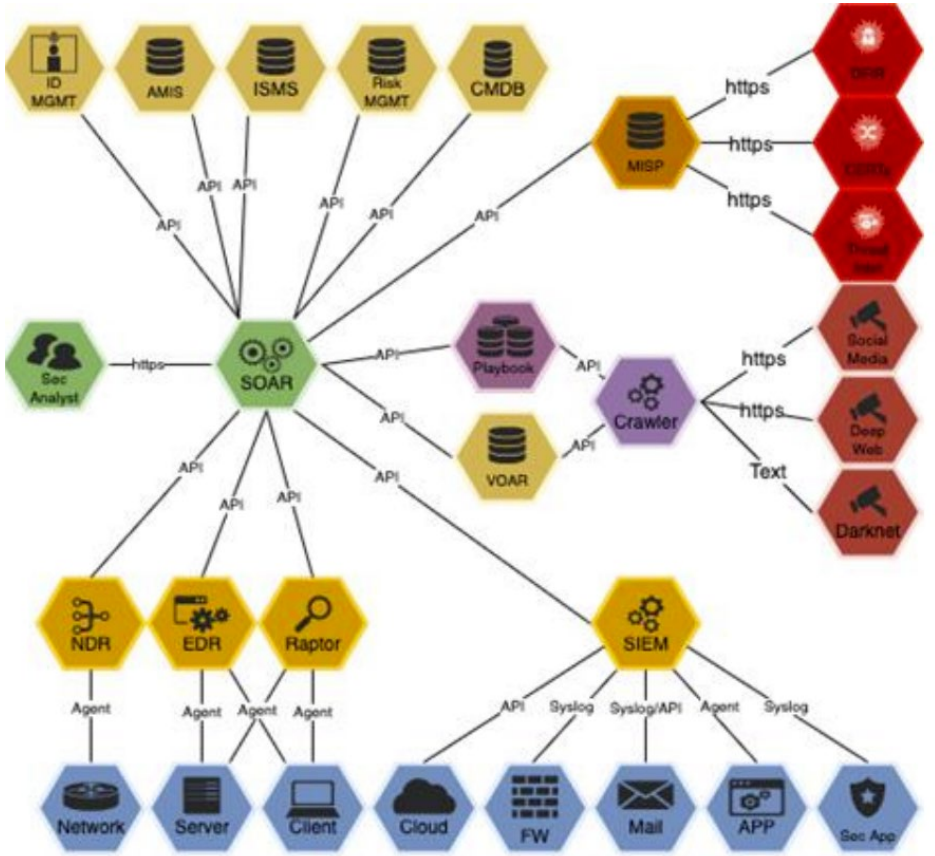
Warum ein effektives SOC entscheidend für das Identity Management ist

- **Proaktive Überwachung:** Ein SOC identifiziert proaktiv verdächtige Aktivitäten, die auf Identitätsdiebstahl hinweisen könnten.
- **Schnelle Reaktion:** Die Fähigkeit, schnell auf Identitätsdiebstähle zu reagieren, minimiert potenzielle Schäden.
- **Compliance und Richtlinien:** Unterstützt die Einhaltung von Datenschutz- und Sicherheitsrichtlinien im Zusammenhang mit Identitätsmanagement.

Bechtle CDC

Modulares Gesamtkonzept

- Offene SOAR (Security Orchestration, Administration & Response) Engine von Google Chronicle für die Automatisierung und als zentrale Plattforminstanz
- EDR & NDR für schnelle Anomalie Erkennung am Endpoint und im Netzwerk
- Umfassende Analyse weiterer Logquellen über SIEM-Integrationen
- Threat Intelligence Feed von Virus Total als zusätzliche Informationsquelle zur Anreicherung der Telemetriedaten
- Bechtle CTI zur Sammlung von aktuellen Schwachstelleninformationen, welche noch nicht bekannt sind.



Erkennung von Identitätsdiebstahl

Gemeinsame Anzeichen und Indikatoren für Identitätsdiebstähle

- Unerwartete Kontobewegungen
- Warnungen aus div Quellen, wie Partner, Feeds, Deep/Darknet Monitoring
- Unbekannte Anmeldeversuche

Realweltbeispiele und Fallstudien

- Beispiel 1: Betrüger verwenden gestohlene Identitätsdaten.
- Beispiel 2: Phishing-Kampagne führt zum Diebstahl von Mitarbeiter-Zugangsdaten, was unbefugten Zugriff ermöglicht.

Innovative Abwehrmethoden

Überblick über innovative Techniken zur Identifizierung und Abwehr von Bedrohungen

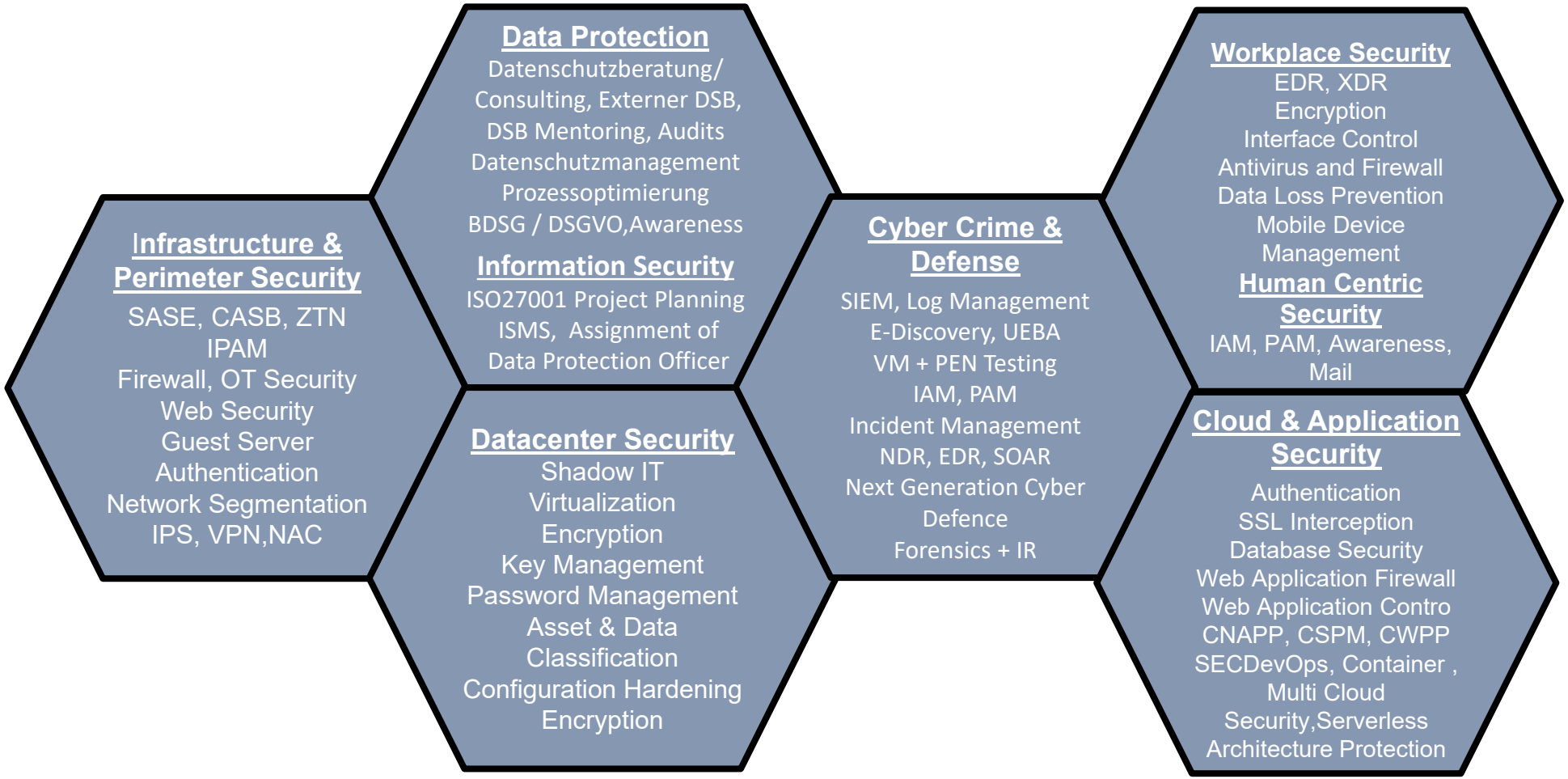
- **Anomalieerkennung**: Identifizierung von Mustern, die von der Norm abweichen.
- **Verhaltensbasierte Analyse**: Überwachung des Nutzerverhaltens, um Missbrauch zu erkennen.

Rolle von KI, maschinellem Lernen und automatisierten Systemen

- **KI & maschinelles Lernen**: Verbesserung der Erkennungsgenauigkeit durch Lernen aus historischen Daten und Trends.
- **Automatisierung**: Beschleunigung der Reaktionszeiten auf Sicherheitsvorfälle und Minimierung menschlicher Fehler.

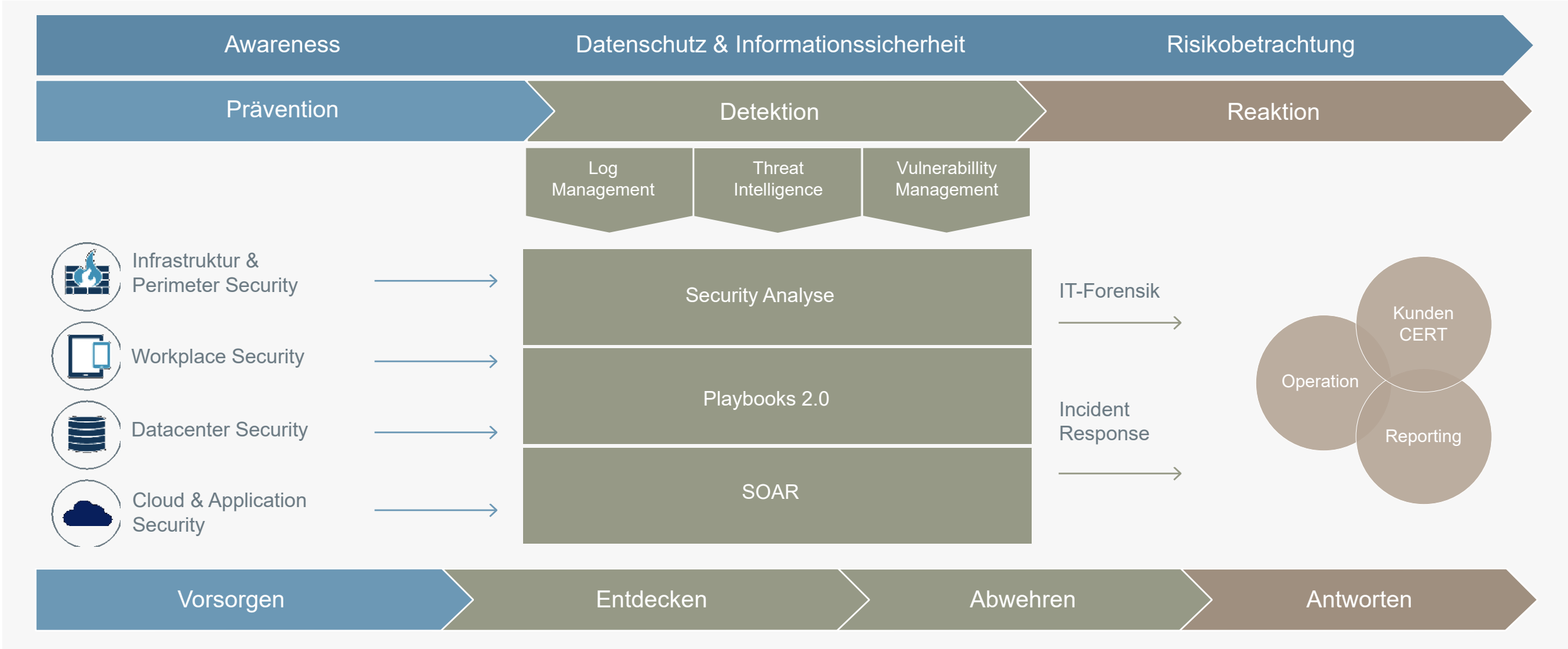
Practice Übersicht

Security



Ganzheitliche Betrachtung - Zielszenario

Cyber Defense Konzept



Schlussfolgerungen und Best Practices

Zusammenfassung der wichtigsten Punkte

- Bedeutung von Cyber Defense und Identity Management
- Wichtigkeit schneller Incident Response
- Rolle des SOCs und innovativer Technologien

Empfehlungen für Unternehmen

- Investition in fortschrittliche Sicherheitstools und -technologien
- Regelmäßige Schulungen und Bewusstseinsbildung bei Mitarbeitern
- Implementierung strenger Zugriffskontrollen und Überwachungssysteme

Danke.