FortiSIEM

René Kovács

Channel Account Manager

kovacsr@fortinet.com | +49 172.570.1736

Unsere heutige Agenda

Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche

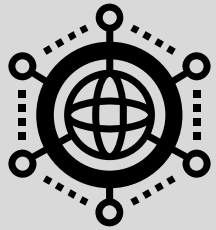
- Multi-Vendor
- On and Off Prem Umgebungen
- SaaS/IaaS
- Remote Arbeitsplätze

Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche

- Multi-Vendor
- On and Off Prem Umgebungen
- SaaS/IaaS
- Remote Arbeitsplätze

Mangel an Sichtbarkeit



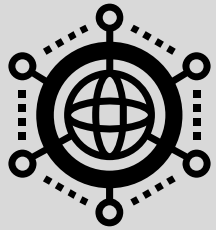
- Wo sind welche IT Assets
- Neue Bedrohungen erforschen
- Betroffene Assets

Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche

- Multi-Vendor
- On and Off Prem Umgebungen
- SaaS/IaaS
- Remote Arbeitsplätze

Mangel an Sichtbarkeit



- Wo sind welche IT Assets
- Neue Bedrohungen erforschen
- Betroffene Assets

Interne Bedrohungen

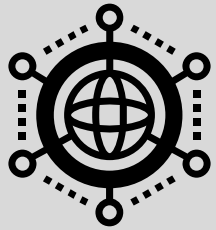
- Was ist “Normalität” für Benutzer
- Privilegierter Zugang für User
- Gewollte oder ungewollte Informationsfreigabe

Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche

- Multi-Vendor
- On and Off Prem Umgebungen
- SaaS/IaaS
- Remote Arbeitsplätze

Mangel an Sichtbarkeit



- Wo sind welche IT Assets
- Neue Bedrohungen erforschen
- Betroffene Assets

Interne Bedrohungen

- Was ist “Normalität” für Benutzer
- Privilegierter Zugang für User
- Gewollte oder ungewollte Informationsfreigabe

Compliance

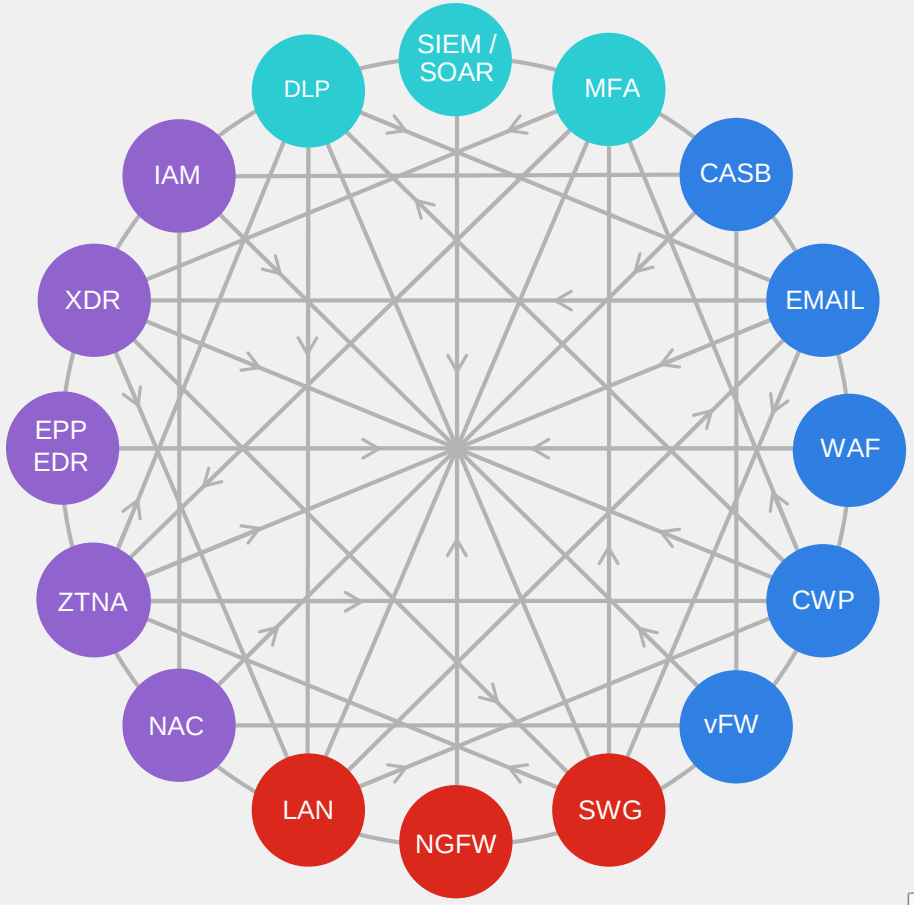
- Regularien (extern)
- Interne Vorgaben
- Praxistauglichkeit umsetzen

Security Fabric

Gartner Cybersecurity MESH Architecture (CMSA)

20 Cybersecurity Point Products (11 Vendors)

Cybersecurity Platform Approach 4-6 Platforms



Fortinet Security Fabric

Umfassend

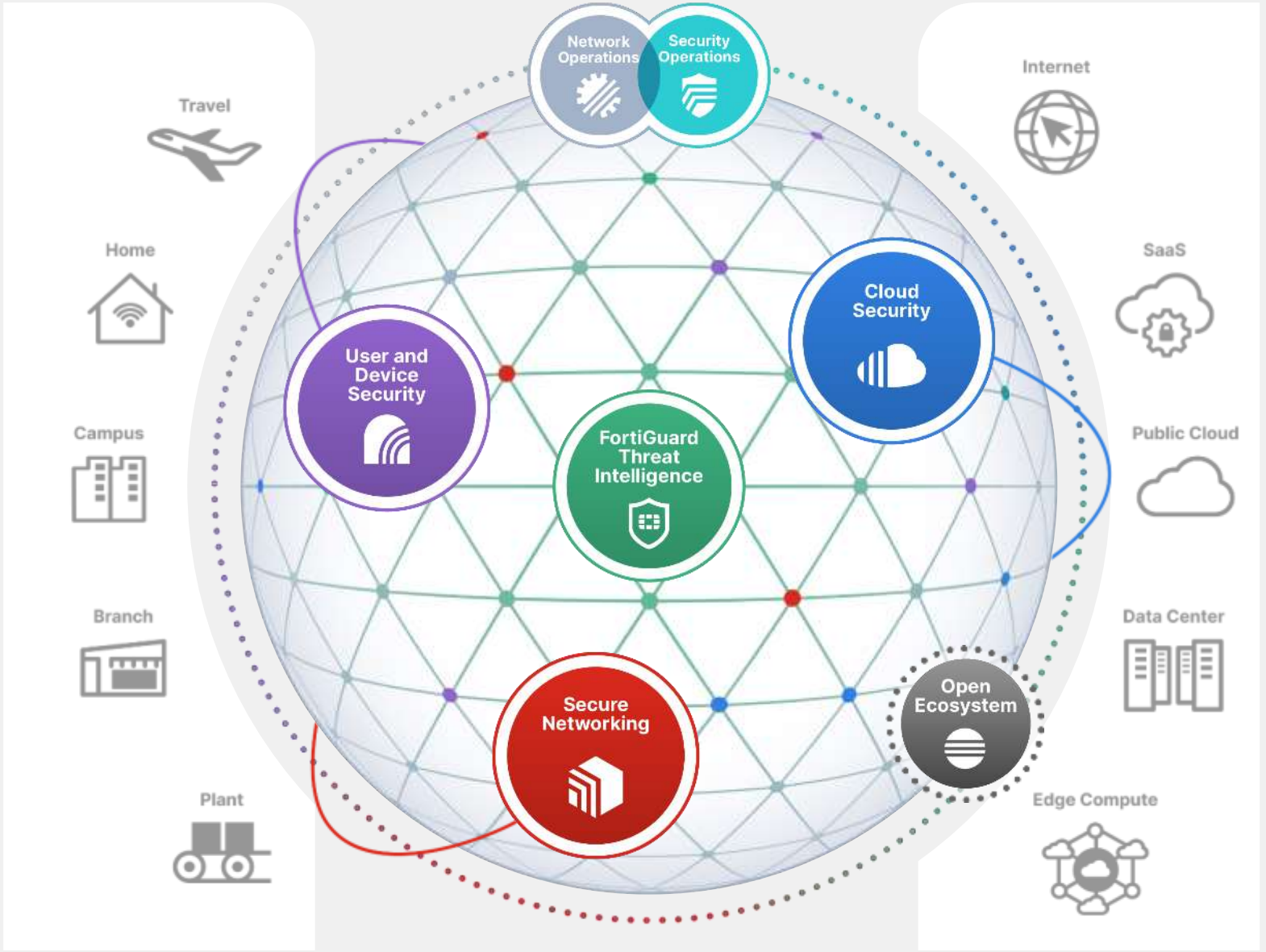
Transparenz und Schutz der gesamten digitalen Angriffsfläche für ein besseres Risikomanagement

Integriert

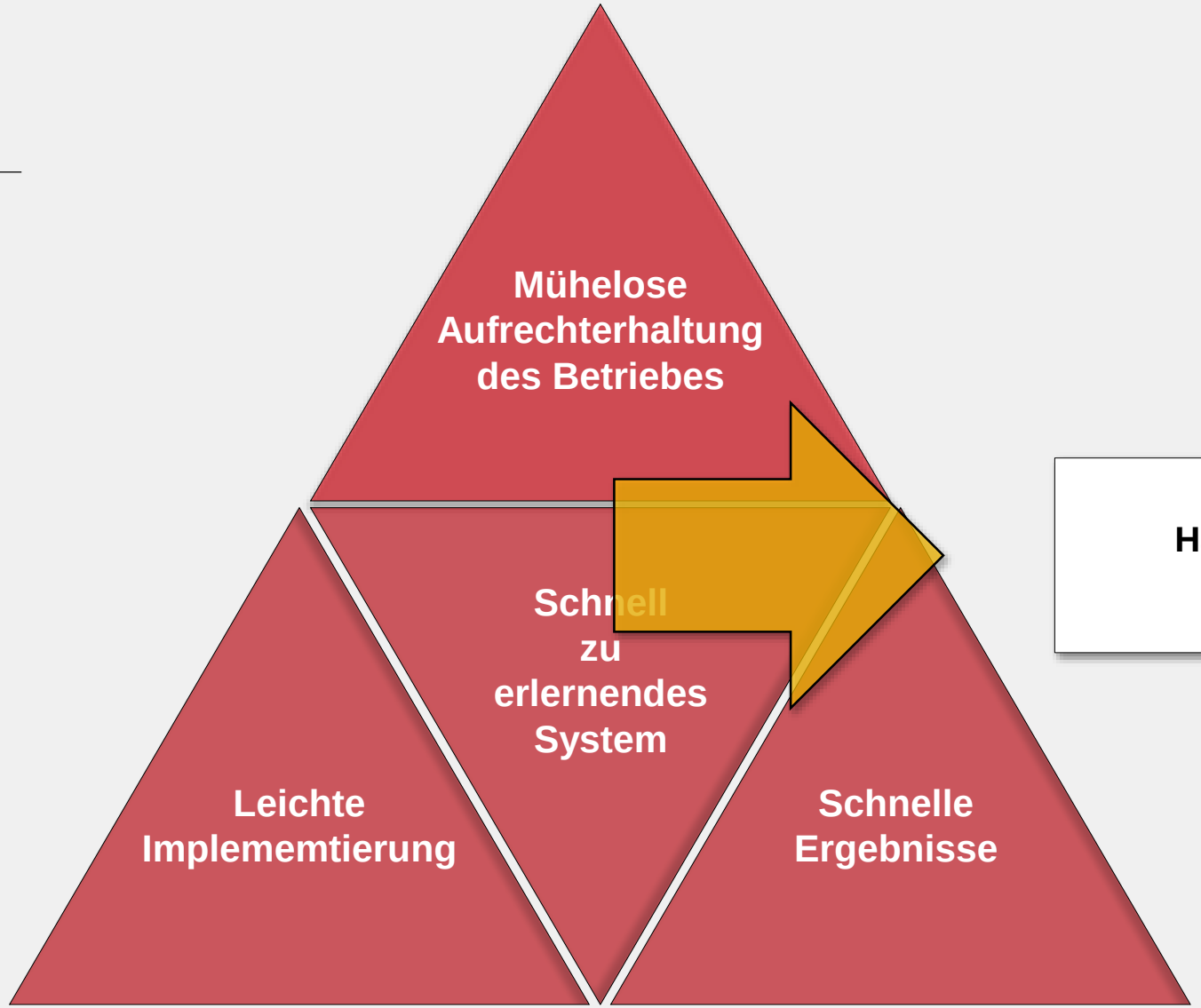
Lösung, die die Komplexität reduziert und Bedrohungsinformationen weitergibt

Automatisiert

Schutz durch selbstheilende Netzwerke mit KI-gesteuerter Sicherheit für schnellen und effizienten Betrieb



Ihre Anforderungen

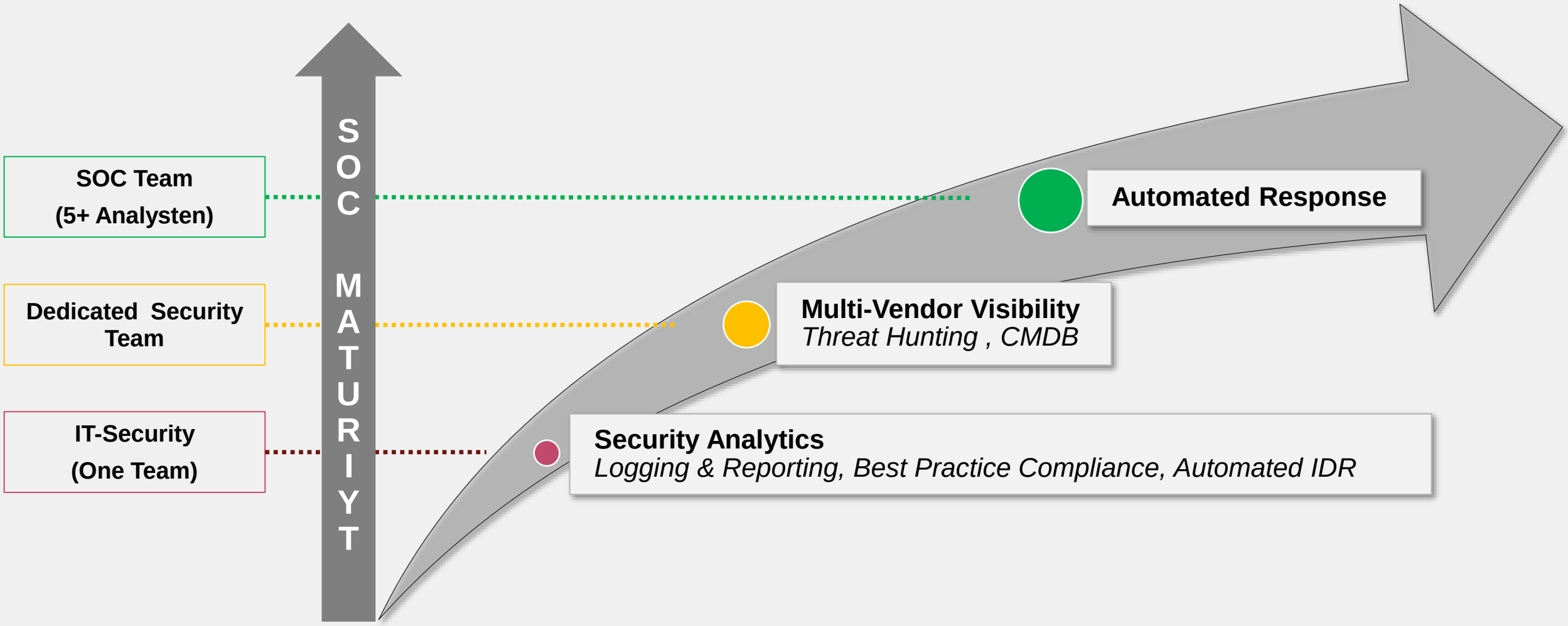


Häufiger Kundenwunsch

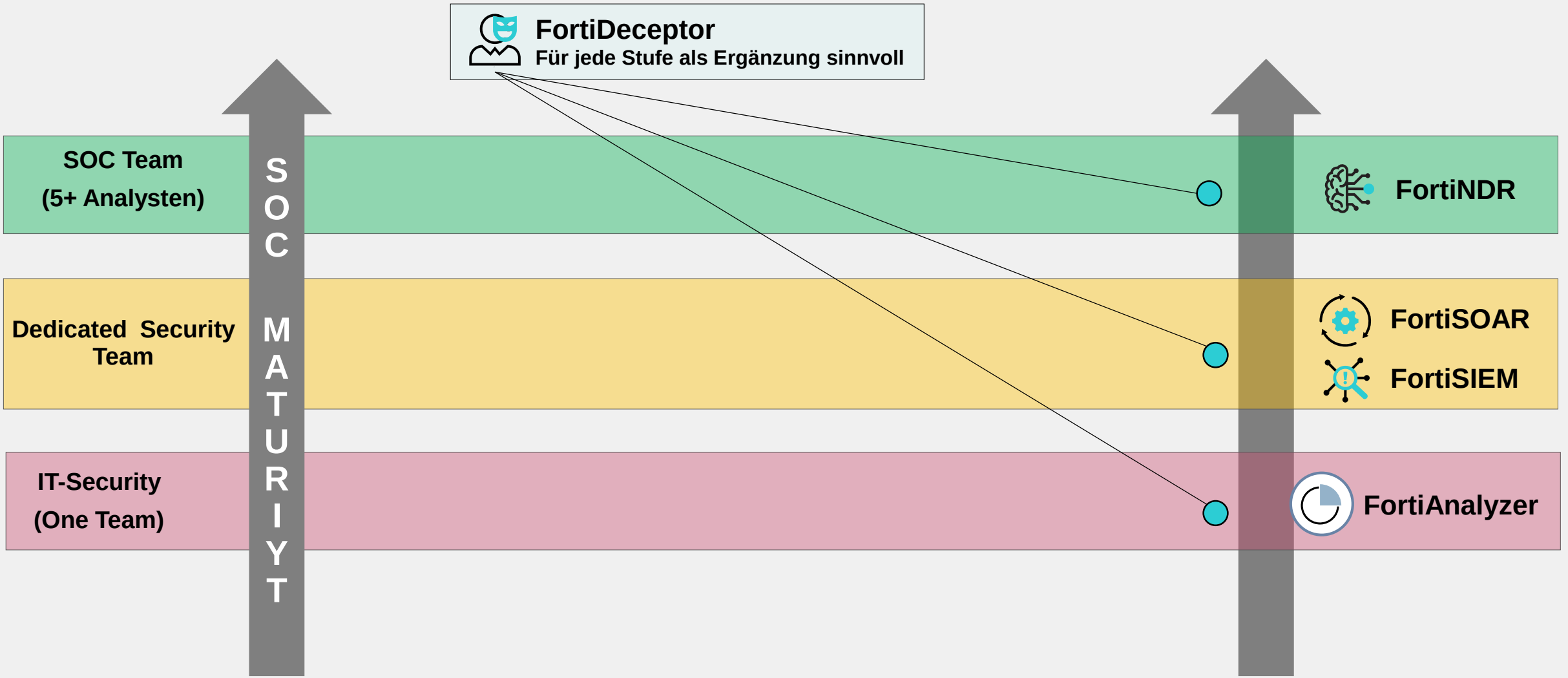
Der Weg zu einem SoC

Von der Notwendigkeit zum Security Team

Sicherheitskomplexität auf Basis der SOC Maturity

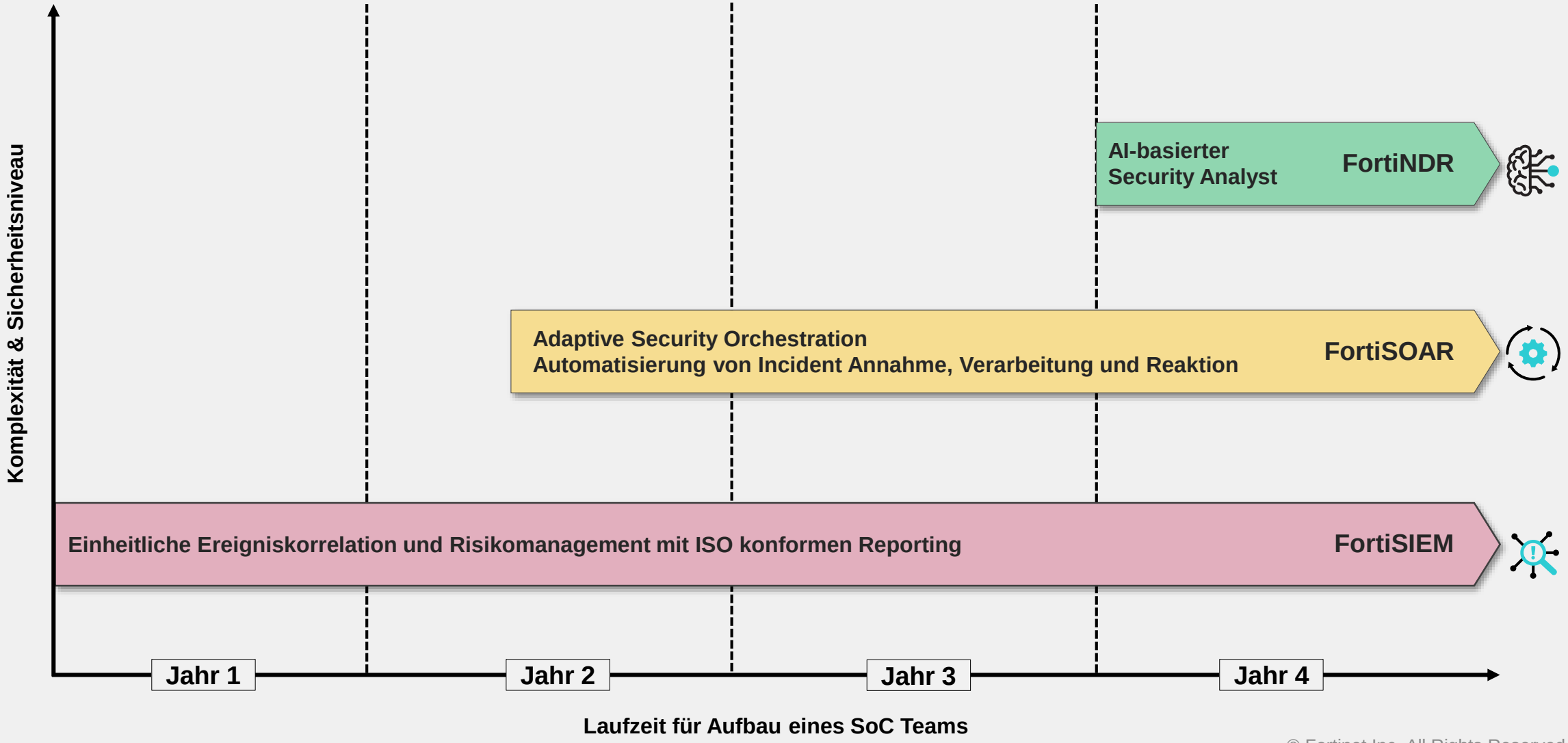


Produkteinordnung auf Basis der SOC Maturity



Produkteinführung in Phasen

Ein Beispiel



Wichtigkeit und Aufgaben eines SoC

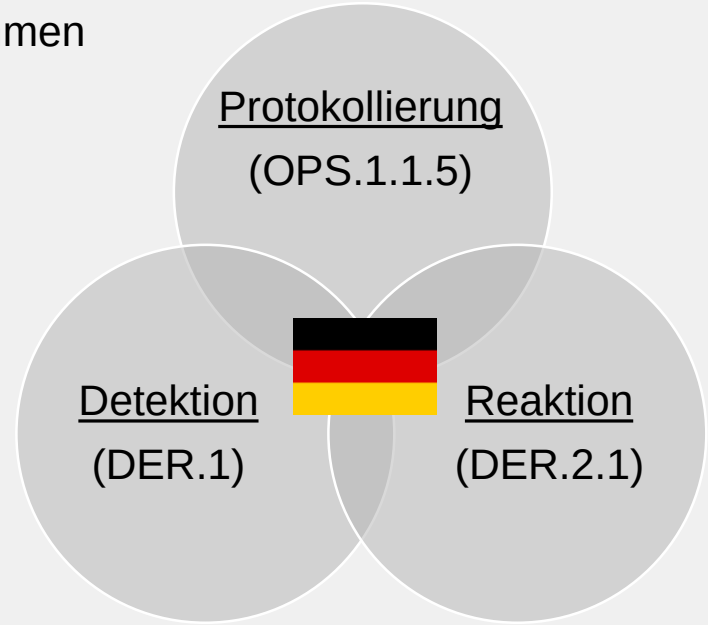
Eine Ableitung aus BSIG, IT-SIG und NIS2UmsuCG

BSI: Orientierungshilfe Angriffserkennung

Nach § 8a Absatz 1a BSIG

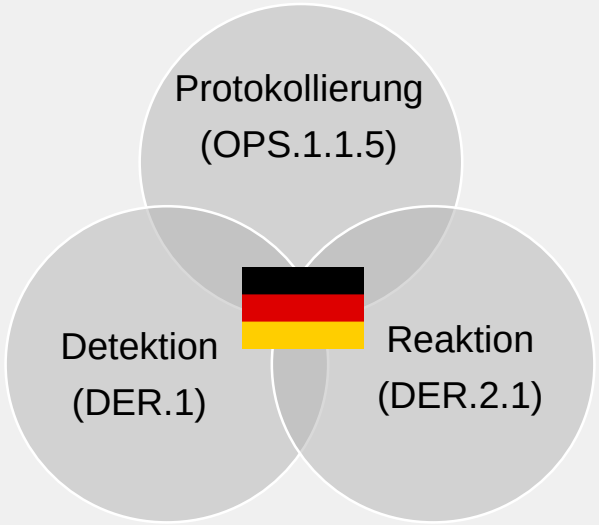
Weiterführende Orientierung:

- OPS.1.1.4: Schutz vor Schadprogrammen
- OPS.1.1.5: Protokollierung
- NET.1.2: Netzmanagement
- NET.3.2: Firewall
- DER.1: Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1: Behandlung von Sicherheitsvorfällen



Umsetzung „Angriffserkennung IT-SIG“

Produkte zur Umsetzung § 8a Absatz 1a BSIG & IEC 62443-2-1 (Ed.2)



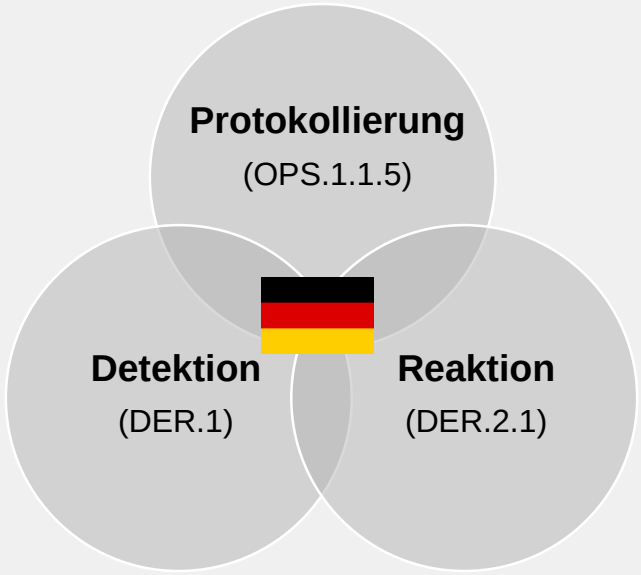
Die zur Angriffserkennung eingesetzten Systeme **SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen** ergreifen können, ….

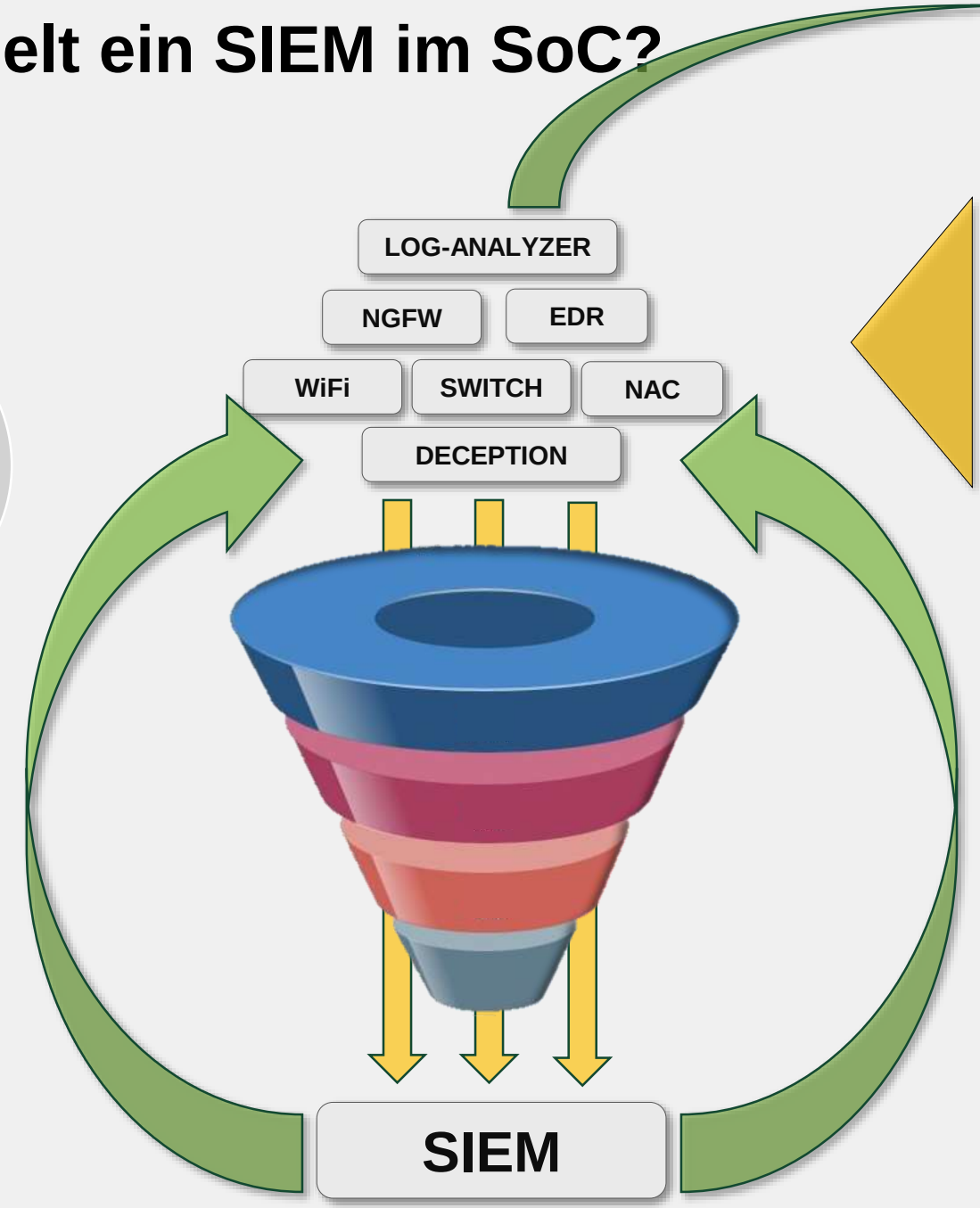
Dabei **MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können**.

Umsetzung „Angriffserkennung IT-SIG“

Produkte zur Umsetzung § 8a Absatz 1a BSIG & IEC 62443-2-1 (Ed.2)

Welche Rolle spielt ein SIEM im SoC?





IT-Systeme des Kunden und aller angeschlossenen Partner

Umsetzung der Anforderungen gemäß NIS2UmsuCG

Kryptografie
- NGFW

Zugangskontrolle/ Authentication
- NGFW
- NAC
- FAC
- Client
- Tokens
- Proxy

Asset Management
- NGFW
- Switch
- WIFI
- EDR
- NAC

Incident Management
- SOAR
- SIEM
- Analyzer
- NDR

Kommunikation
- NGFW
- Manager
- SIEM
- Analyzer

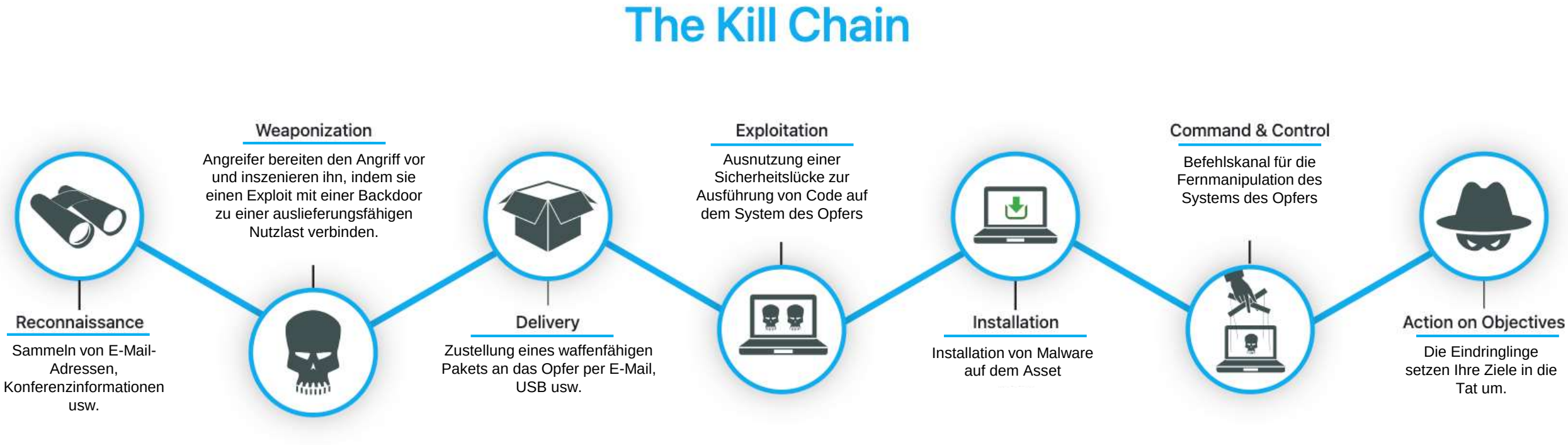
Interaktion – Korrelation – Austausch

- Single Pane Management
- Threat Intelligence
- Interoperability

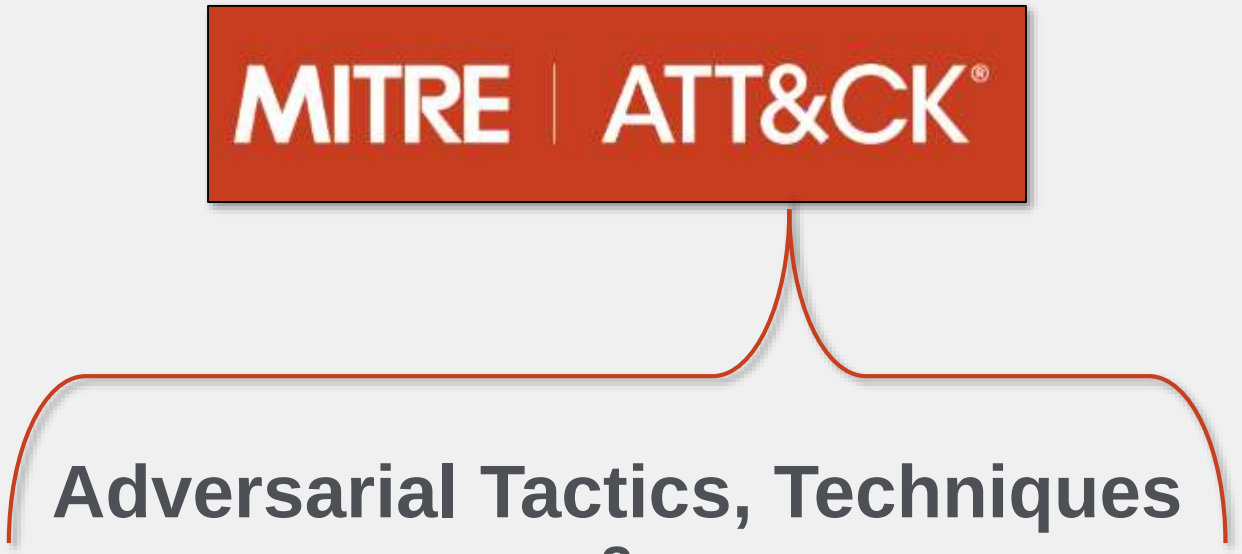
MITRE ATT&CK® Framework

Strukturierte Reaktion auf Angriffe

Wie wird angegriffen?

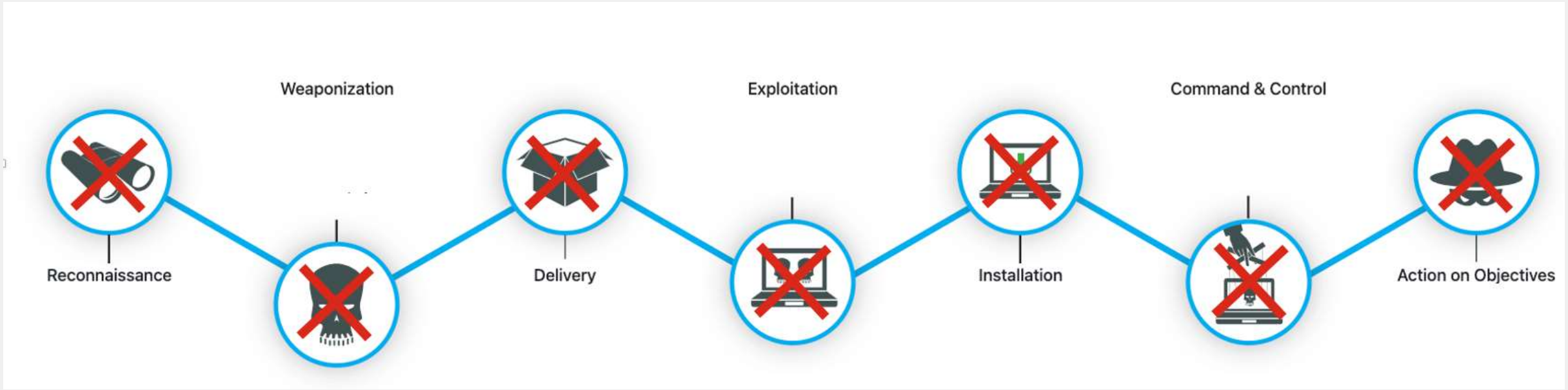


Wofür steht….

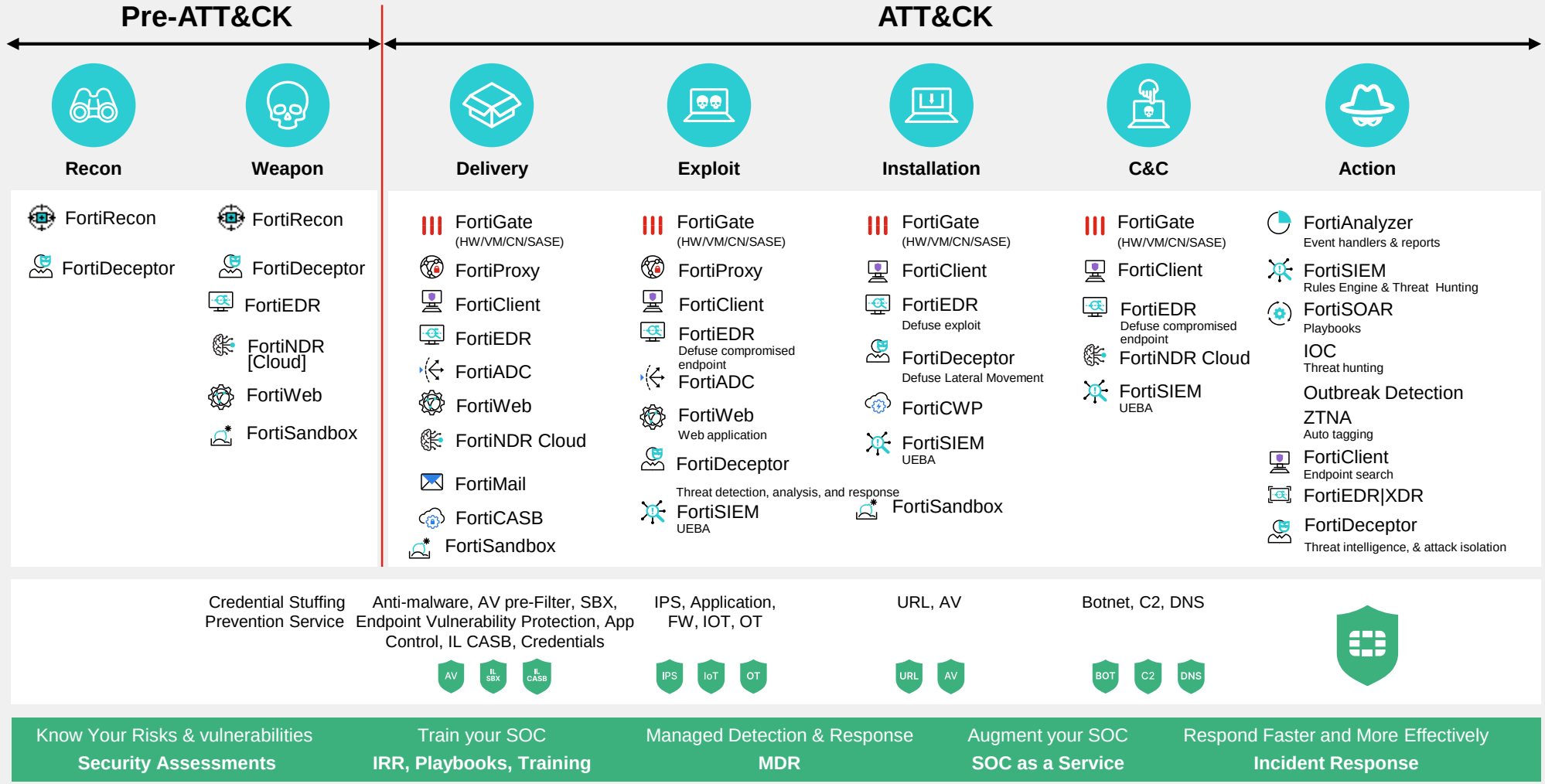


MITRE | ATT&CK®

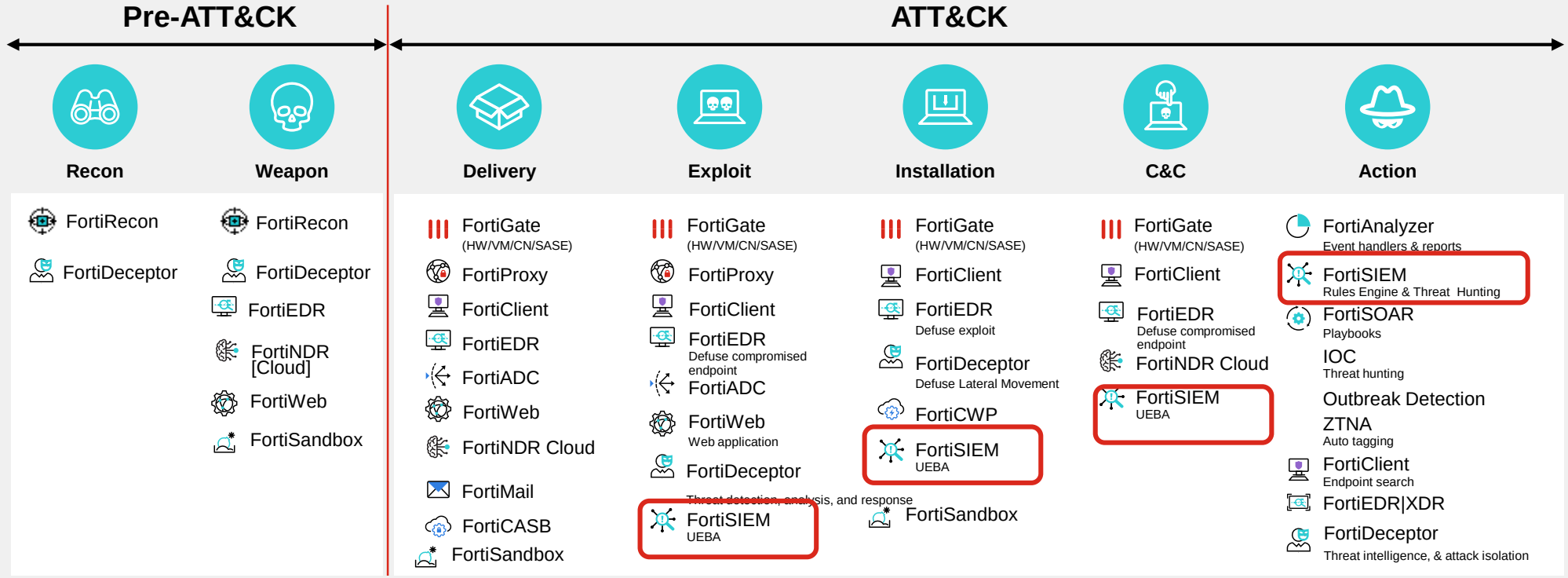
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques



Fortinet bietet Sichtbarkeit und Risikomanagement

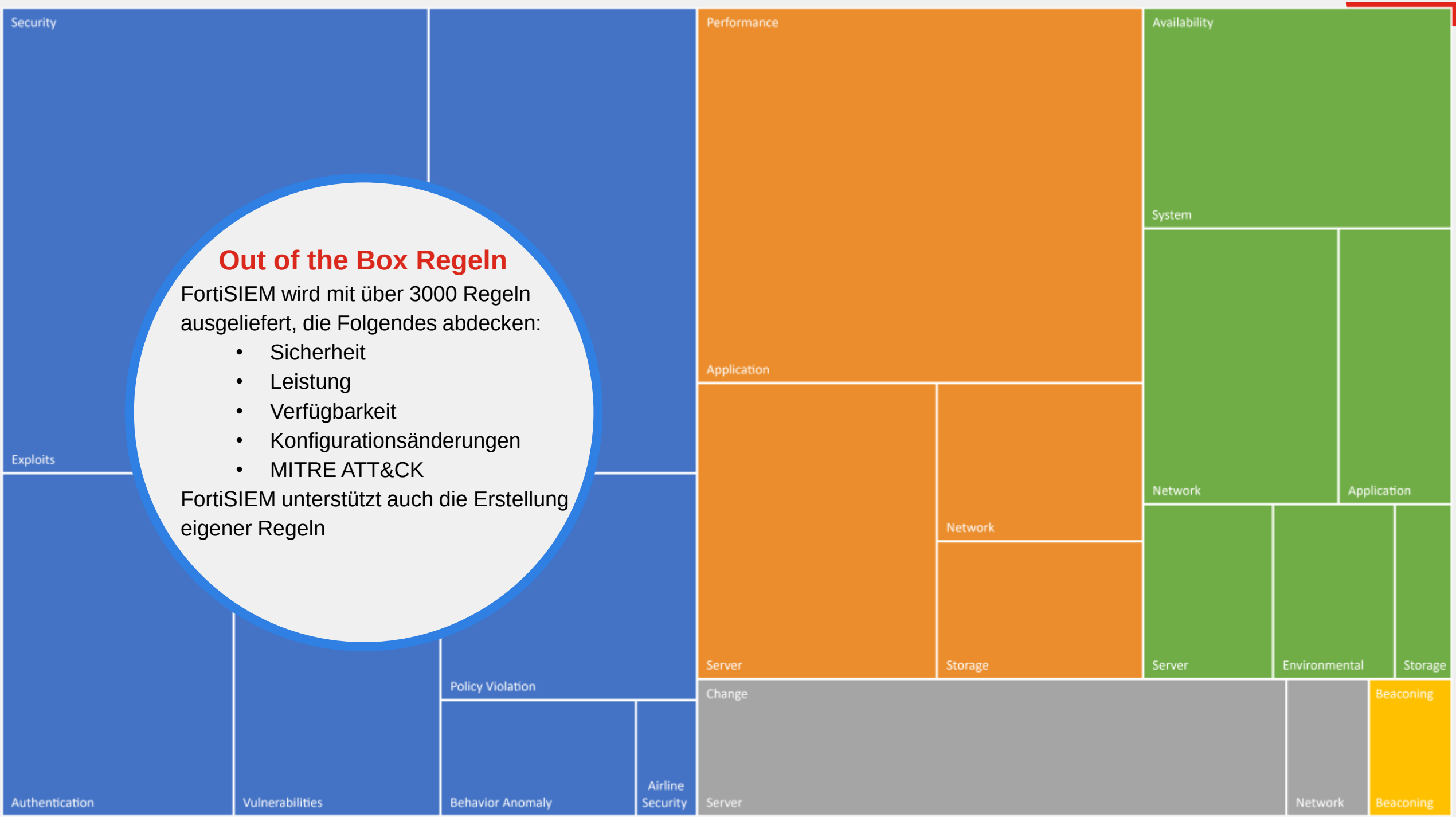


Fortinet bietet Sichtbarkeit und Risikomanagement



Warum FortiSIEM

Warum ein SIEM nicht kompliziert sein muss

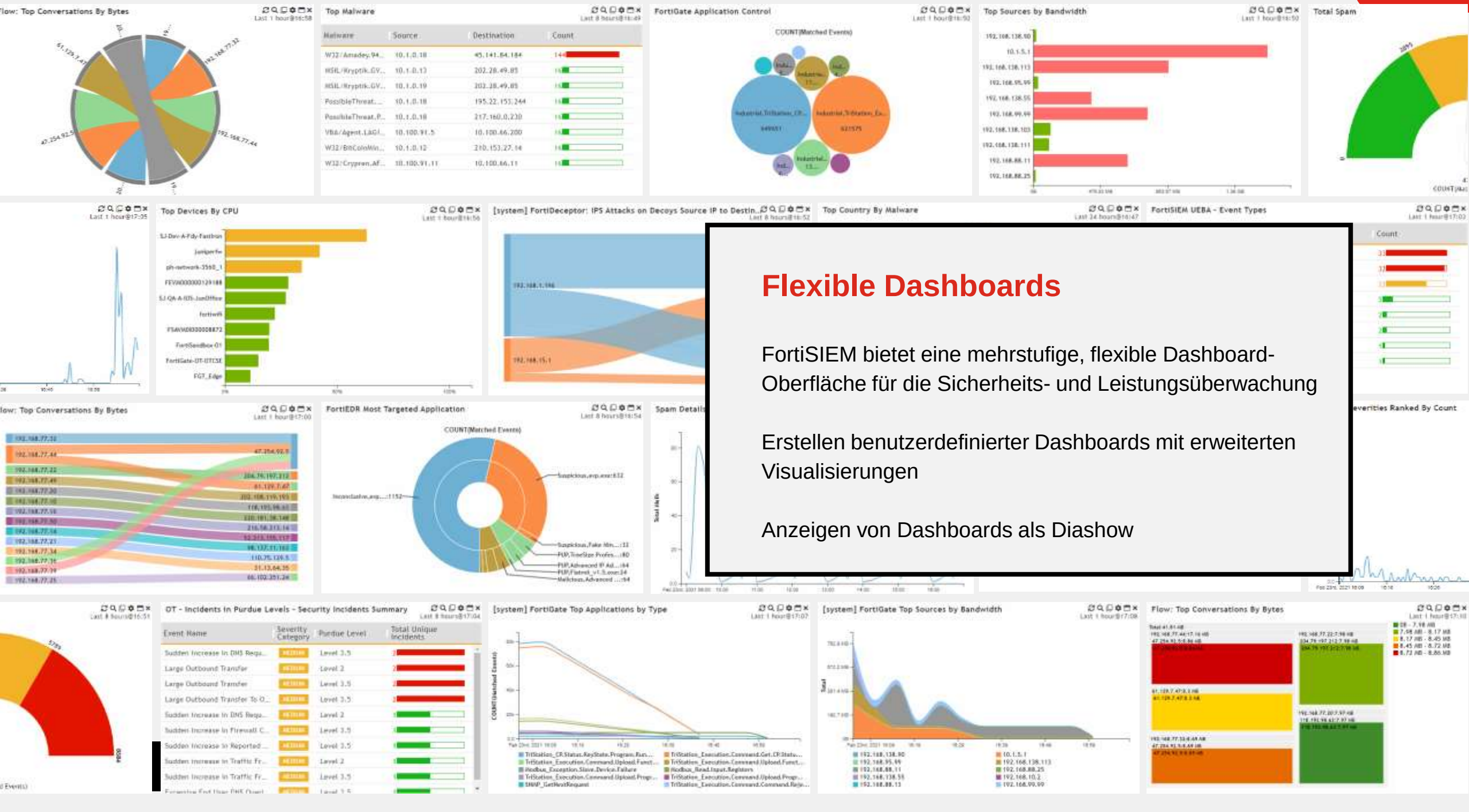


Out of the Box Regeln

FortiSIEM wird mit über 3000 Regeln ausgeliefert, die Folgendes abdecken:

- Sicherheit
- Leistung
- Verfügbarkeit
- Konfigurationsänderungen
- MITRE ATT&CK

FortiSIEM unterstützt auch die Erstellung eigener Regeln



Flexible Dashboards

FortiSIEM bietet eine mehrstufige, flexible Dashboard-Oberfläche für die Sicherheits- und Leistungsüberwachung

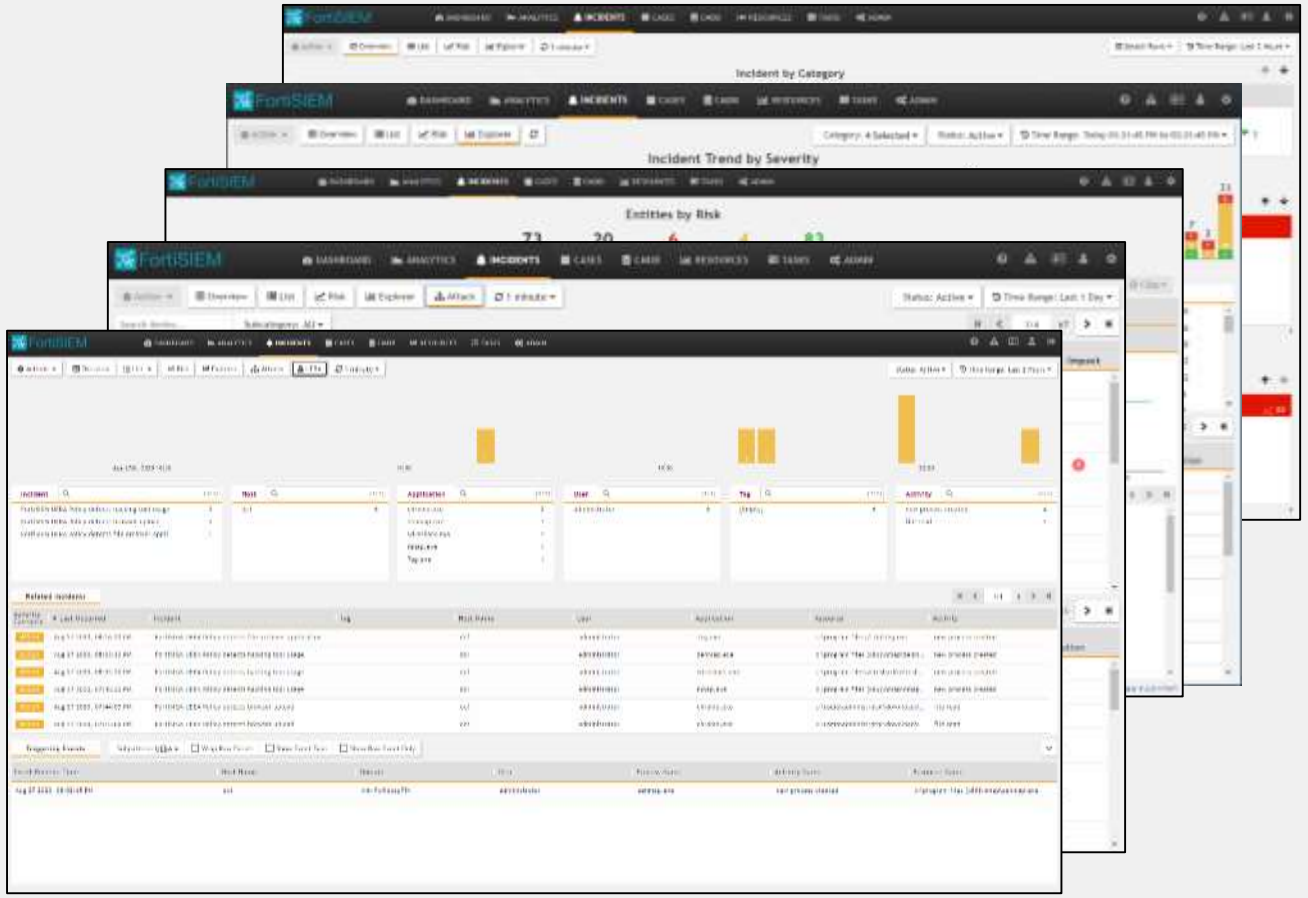
Erstellen benutzerdefinierter Dashboards mit erweiterten Visualisierungen

Anzeigen von Dashboards als Diashow

Relevante und zugängliche Vorfallinformationen

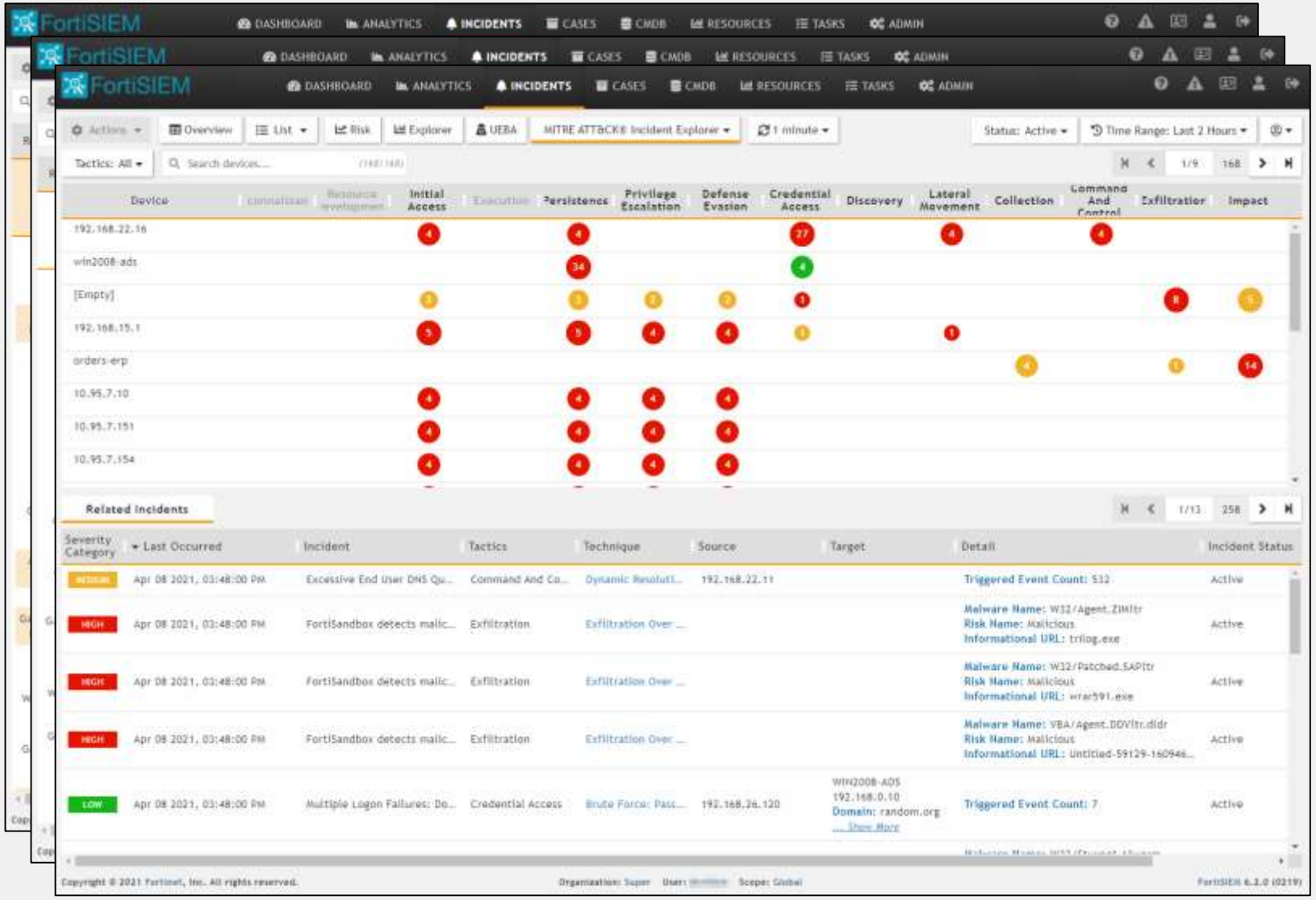
Incident Dashboards priorisieren Incident-Informationen

- Incident Overview Dashboard
  - Top level incident overview
- Incident Explorer Dashboard
  - Interactive incident investigations
- Risk Dashboard
  - Device and user risk & incident timeline
- Attack Dashboard
  - MITRE ATT&CK tactic alignment
- UEBA Dashboard
  - UEBA anomaly focused incidents

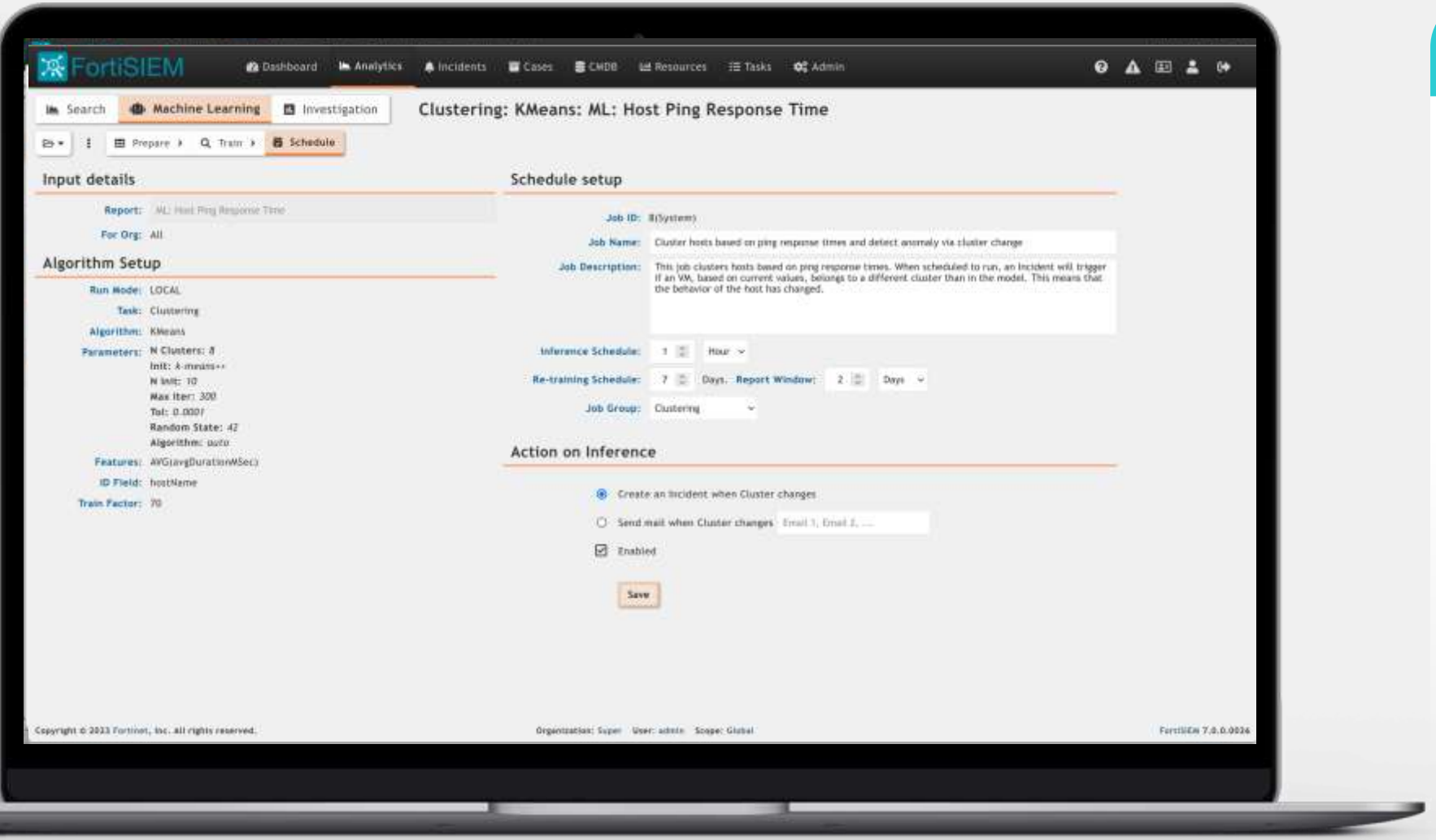


ATT&CK Dashboards

- Das Dashboard zur Regelabdeckung zeigt die MITRE ATT&CK-Abdeckung
- Incident Coverage Dashboard zeigt entsprechende Incidents an
- Incident Explorer zeigt hostzentrierte, interaktive ATT&CK-Ansicht



Machine Learning Workbench



Anomaly

CHALLENGE

- How to detect the known unknowns?
- Detect without a rule in place?
- Know ML frameworks, Python?

HOW

- Simplified ML framework
- Understand normal, look for deviations
- Recommend based on previous behaviour

BENEFIT

- **Identify the anomalies, outliers through a simplified framework**

Machine Learning Workbench

Learning Tasks Supported

Classification	Forecasting	Clustering	Regression	Anomaly Detection
Lernt, wie labels to items based on various fields	Lernt künftige Werte in bestimmten Feldern vorherzusagen	Lernt items in Gruppen zusammenzuführen basierend auf ähnlichen Eigenschaften	Lernt, wie man ein Zielfeld auf der Grundlage anderer Felder in einem Datensatz vorhersagen kann	Lernt, was als “normal” betrachtet wird in einem Datensatz

Beispiele für inkludierte vorgefertigte Modelle

Incident Resolution Recommendation

Zuweisung einer Wahrscheinlichkeit (0-100), dass es sich bei einem neuen Vorfall um einen "True Positive" handelt, basierend auf den Attributen früherer gelöster Vorfälle

Login Anomaly Detection via Bipartite Graph Edge Anomaly Algorithm

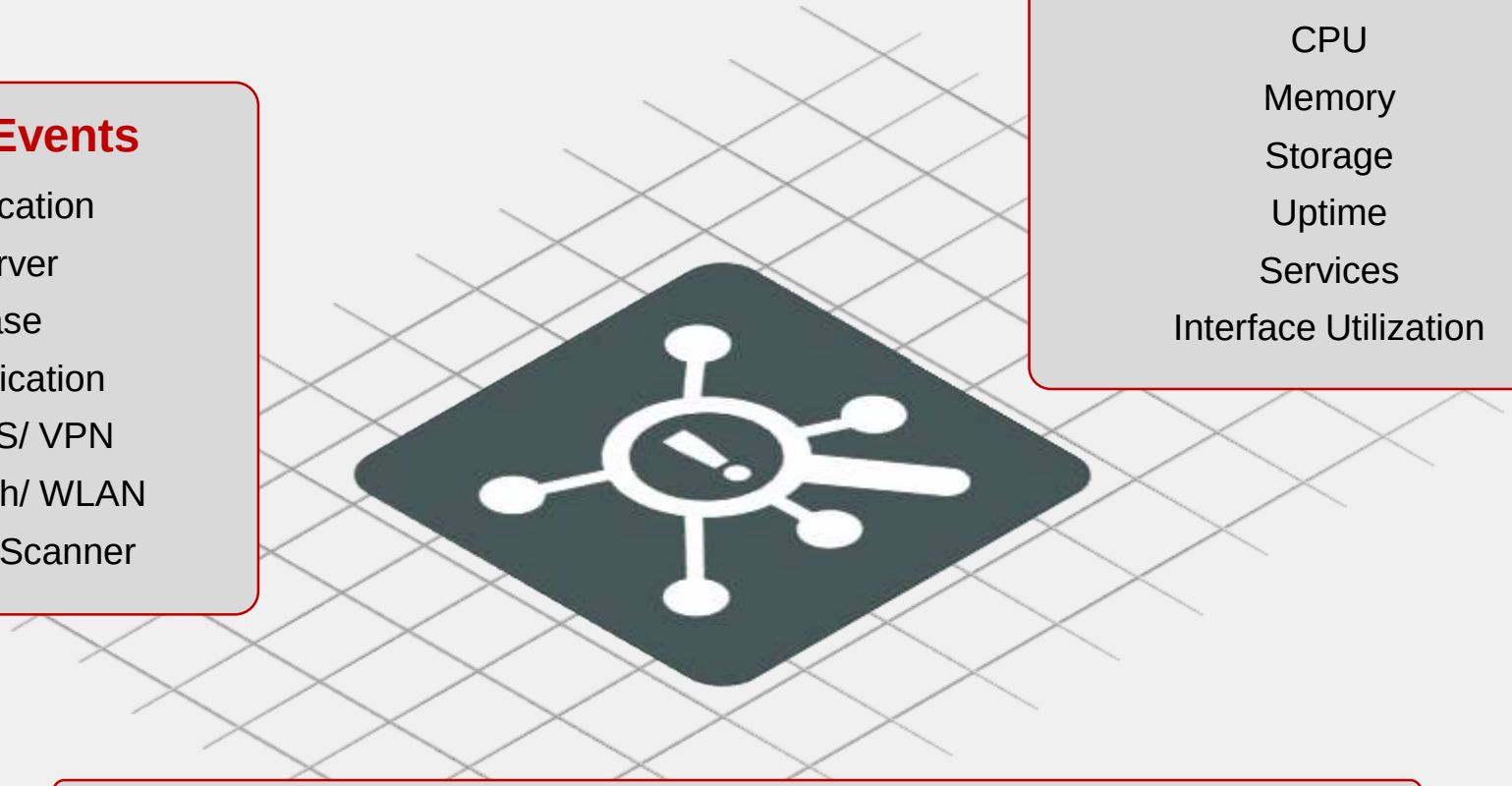
Erkennen von Anmeldeanomalien durch Lernen von Anmeldemustern zwischen Benutzern und Arbeitsstationen und Bilden dynamischer Peer-Benutzergruppen mit ähnlichen Anmeldemustern

Combined SOC & NOC Analytics

Solving the SOC Visibility Puzzle

Security Events

Web Application
AAA Server
Database
Cloud Application
Firewall/ IPS/ VPN
Router/ Switch/ WLAN
Vulnerability Scanner



Performance Metrics

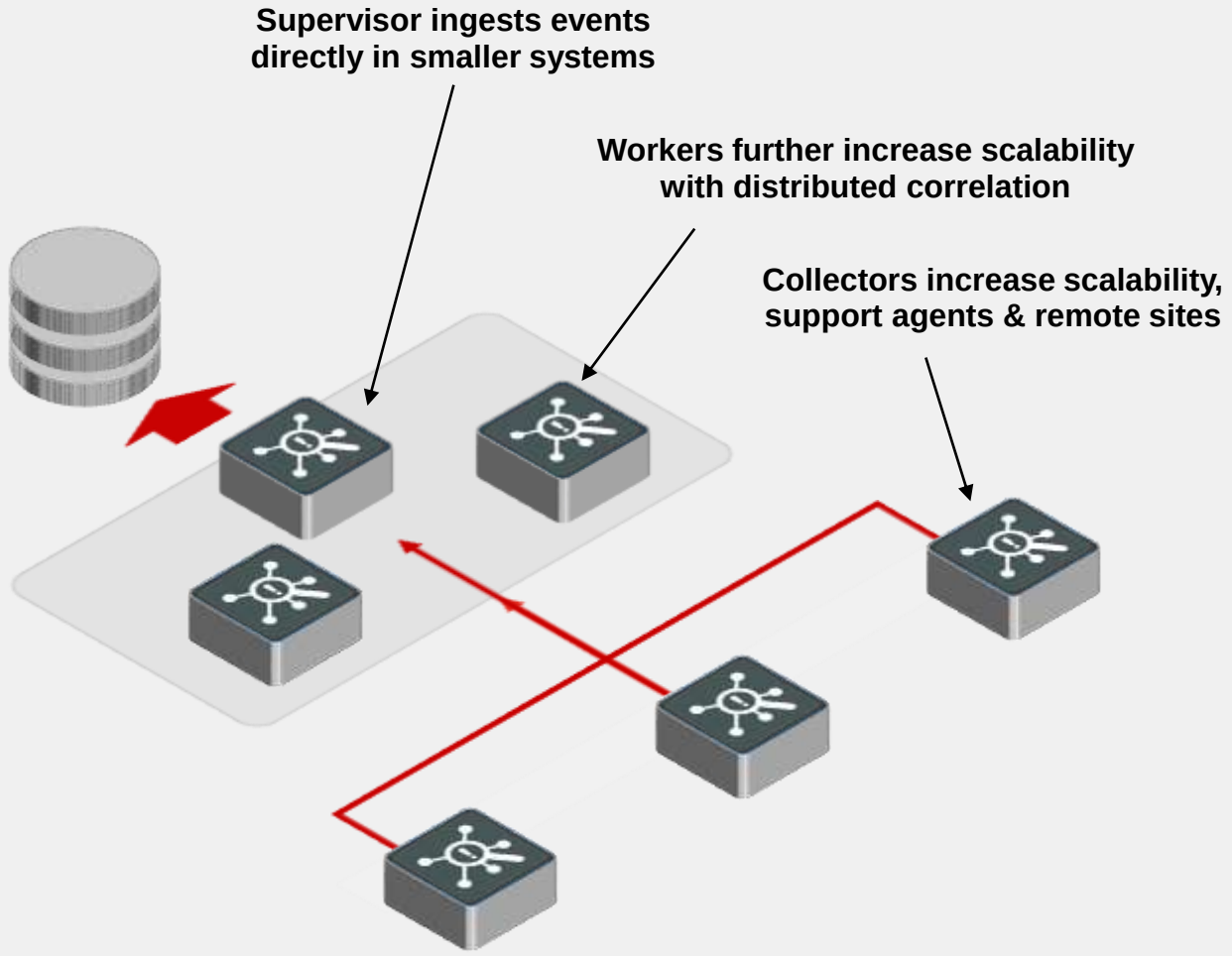
CPU
Memory
Storage
Uptime
Services
Interface Utilization

Combined SOC & NOC

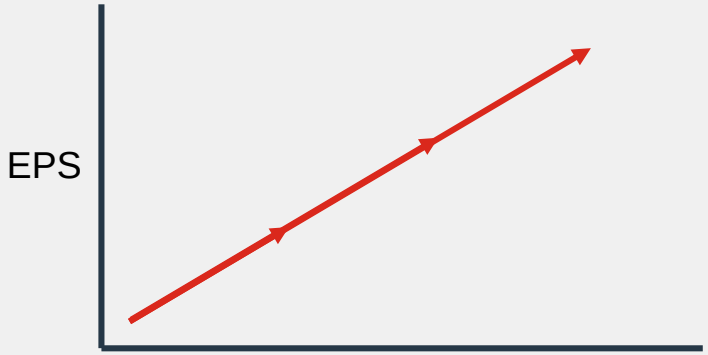
Integrated CMDB | FortiGuard Threat Intelligence

Increased Functionality | Increased Visibility | Reduced Time to Respond

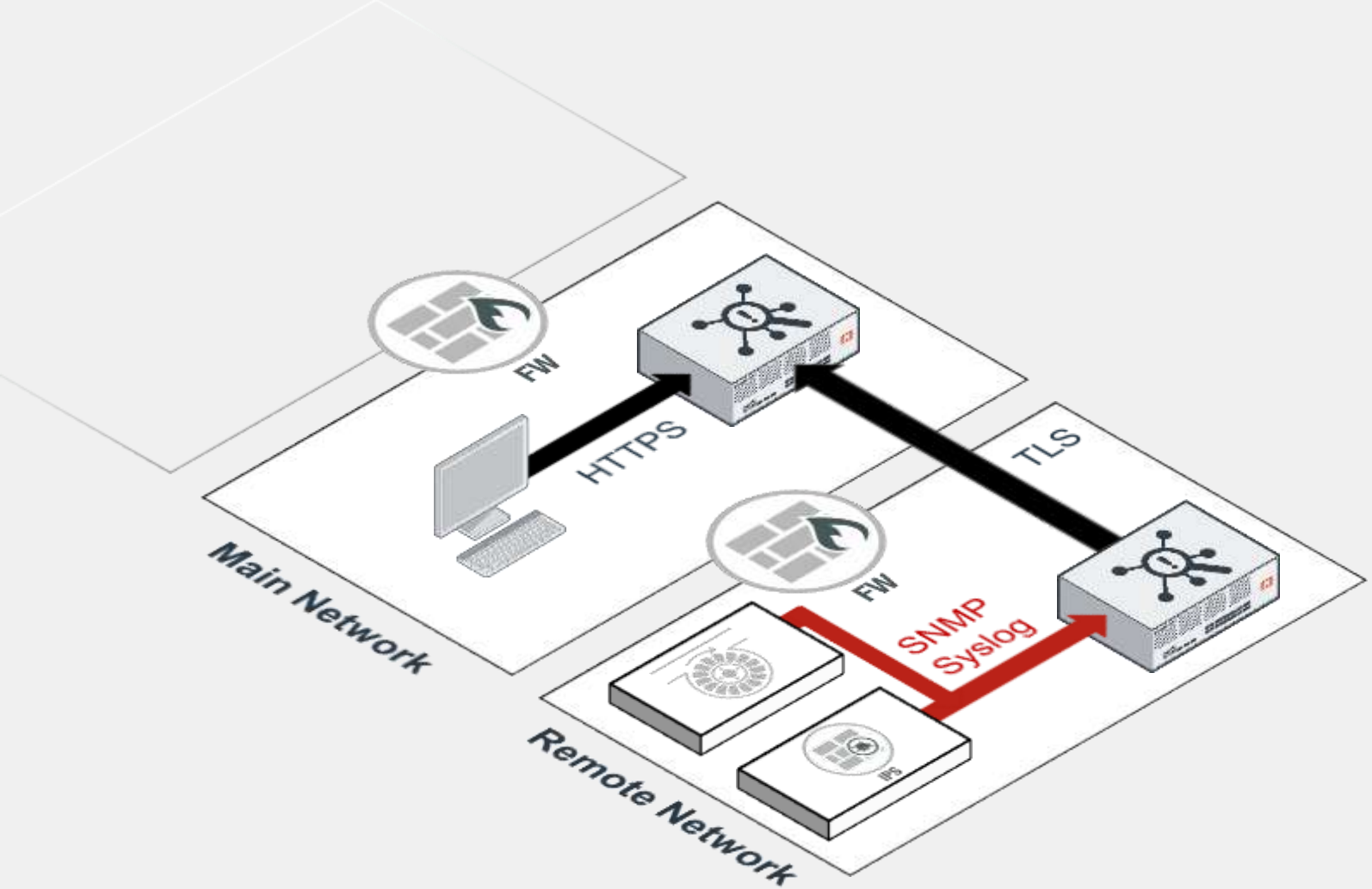
Rapid Scale Architecture



- Scale as you grow
- Distributed parsing & correlation
- No per-VM license charge



FortiSIEM Collectors – Remote Network Log Collection

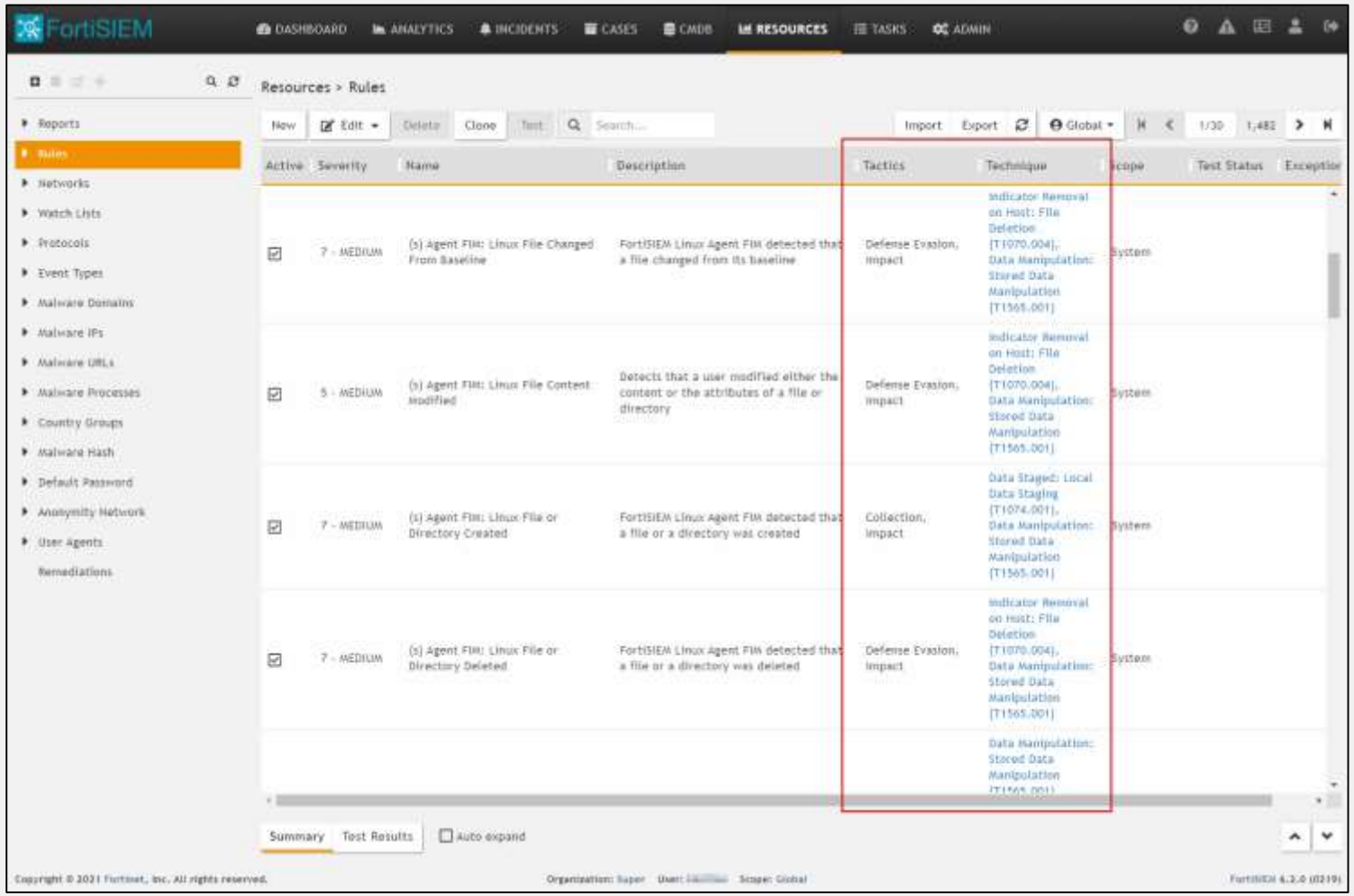


- Remote network log collection
- Secure TLS upload
- Initial log processing
- Log compression
- Remote network discovery
- Performance monitoring

MITRE ATT&CK® Framework

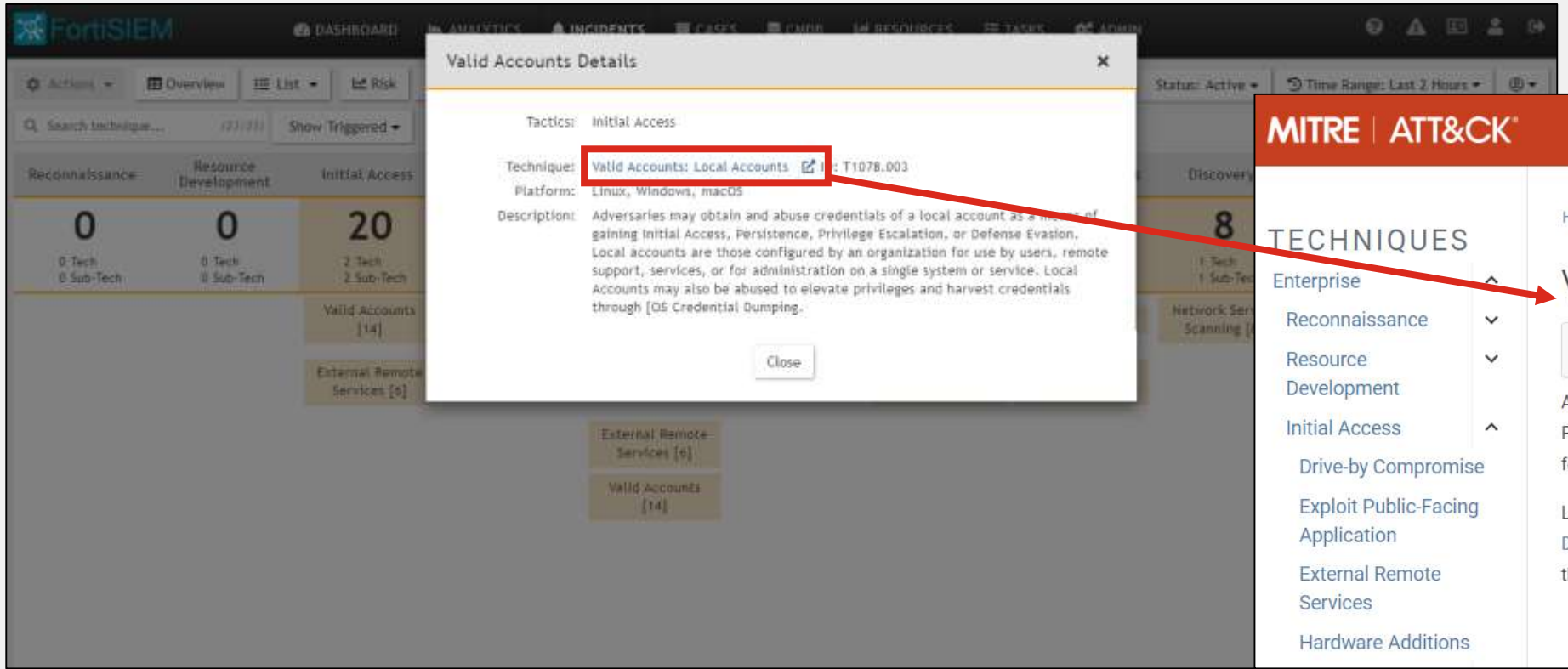
ATT&CK Rule Association

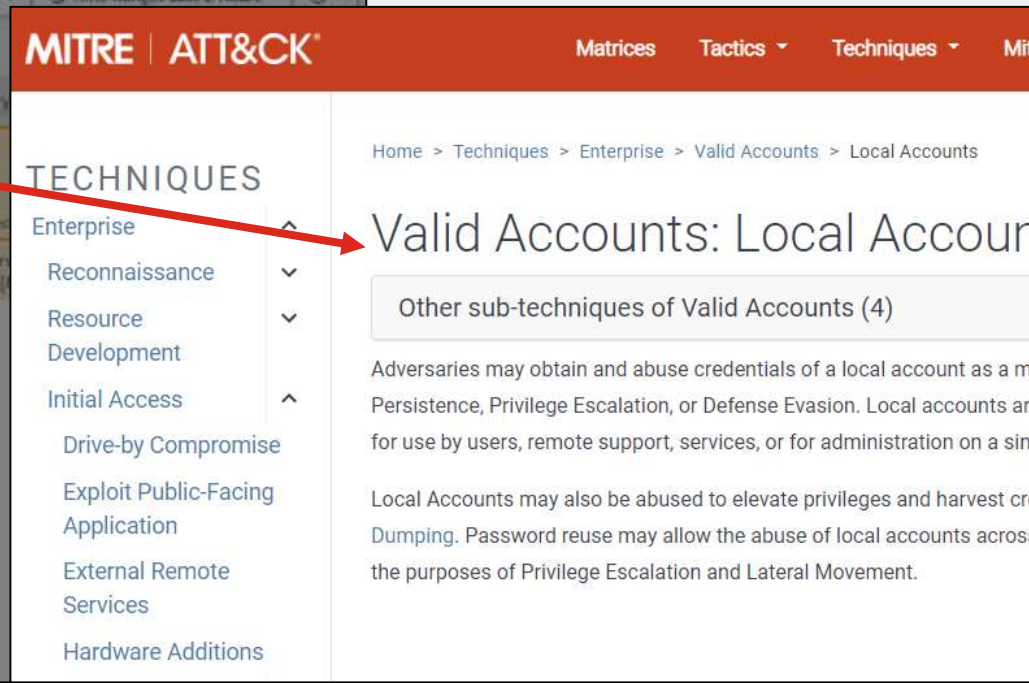
- Assoziieren Sie FortiSIEM-Regeln mit MITRE ATT&CK-Techniken
- „Eine zu vielen“ Zuordnungen
- Funktioniert für system- und benutzerdefinierte Regeln
- Über 900 eingebaute MITRE ATT&CK gemappte Regeln



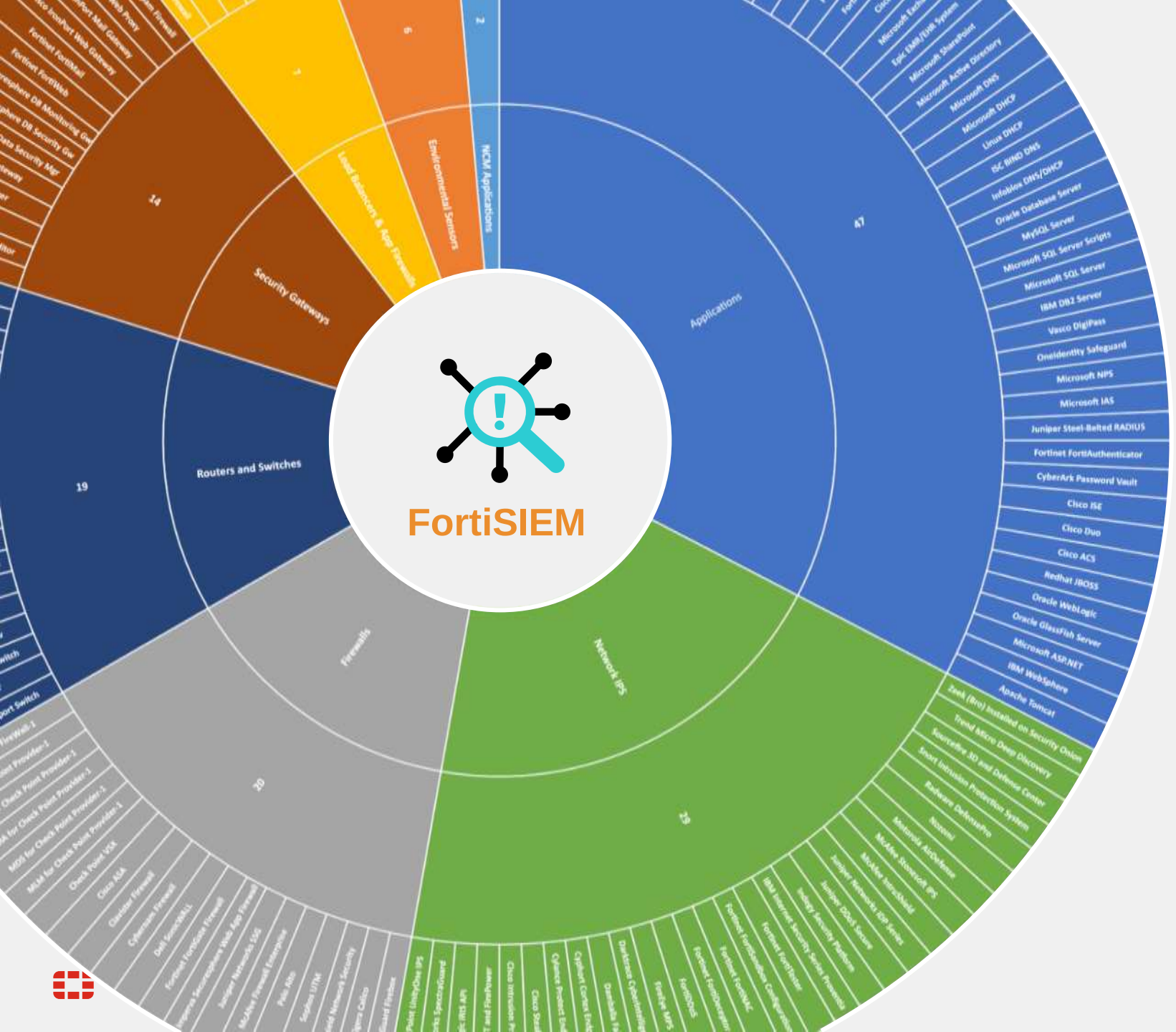
Einfacher Zugriff auf MITRE ATT&CK®-Daten

- Zugriff auf ATT&CK-Daten aus FortiSIEM heraus
- Direkter Zugriff zu MITRE ATT&CK für zusätzliche Informationen





Integrationen



Umfangreiche Geräteunterstützung

FortiSIEM unterstützt von Haus aus etwa 450 Hersteller, Geräte und Anwendungen.

Benutzerdefinierte Parser können erstellt werden, um noch mehr zu unterstützen.

FortiSIEM Integrations

300+ Integrations across vendors and applications

Service Desks & Cloud

Security & Intelligence

Applications

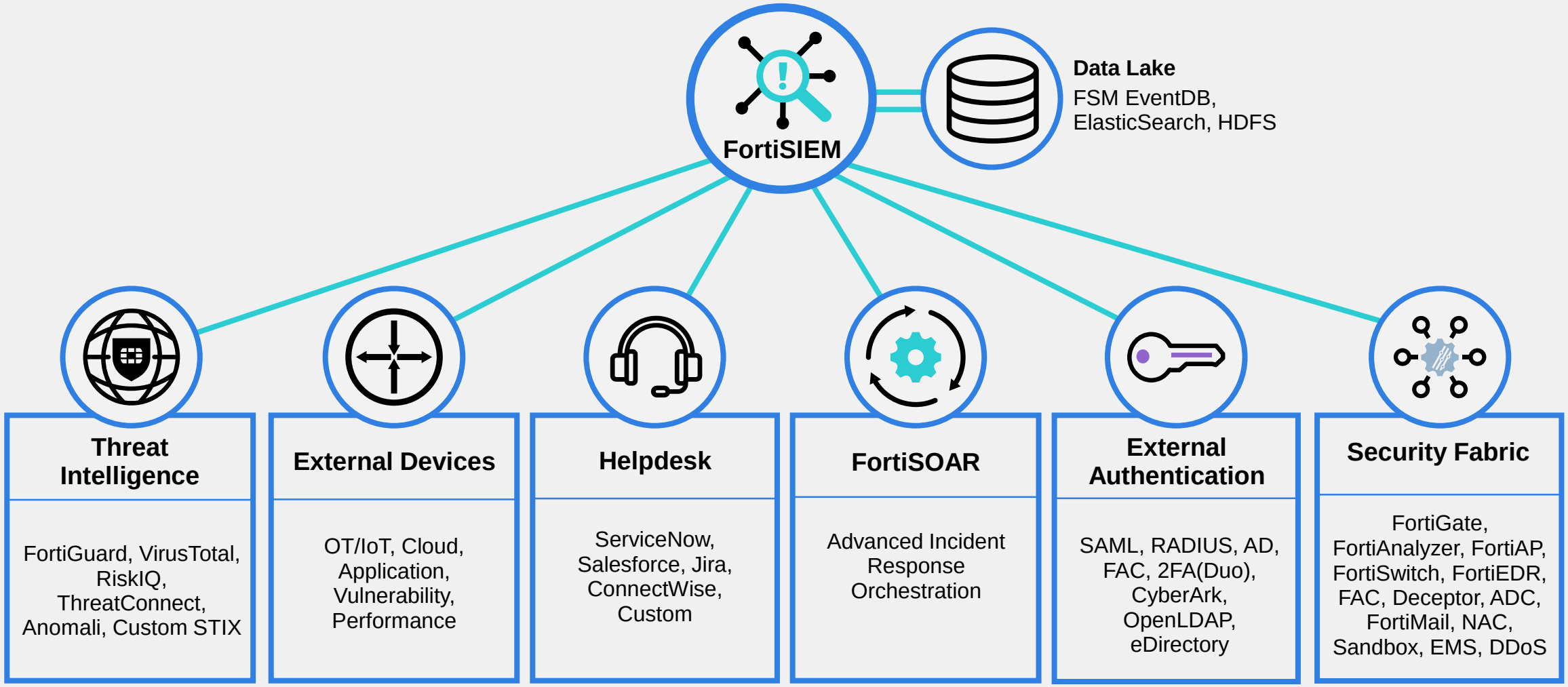
Operating Systems

Infrastructure

Platforms

FORTINET

Hauptbereiche der Integration




FORTINET