

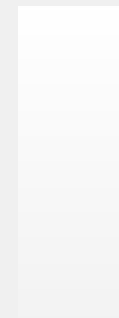
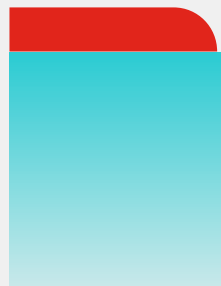
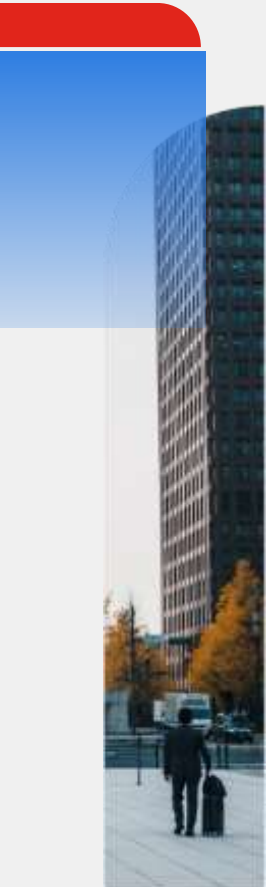
FORTINET[®]

FortiSIEM

René Kovács

Channel Account Manager

kovacsr@fortinet.com | +49 172.570.1736



Unsere heutige Agenda



**Ihre
Anforderungen**



**Der Weg zu
einem SoC**

Vom Gedanken zum
Security Team



**Wichtigkeit und
Aufgaben eines
SoC**

Strukturiert ans Ziel



**Strukturierter
Umgang mit
Incidents**

MITRE ATT&CK
als roter Faden



**Warum
FortiSIEM**

Eine Betrachtung auf
Basis Ihrer
Anforderungen

Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche



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

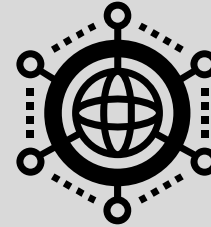
Zu lösende Herausforderungen in Unternehmen

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

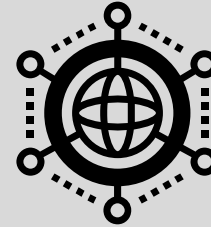
Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche



- Multi-Vendor
- On and Off Prem Umgebungen
- SaaS/laaS
- 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

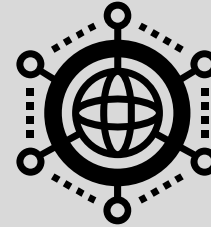
Zu lösende Herausforderungen in Unternehmen

wachsende Angriffsfläche



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

Mangel an Sichtbarkeit



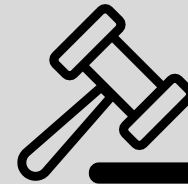
- Wo sind welche IT Assets
- Neue Bedrohungen erforschen
- Betroffene Assets

Interne Bedrohungen



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

Compliance

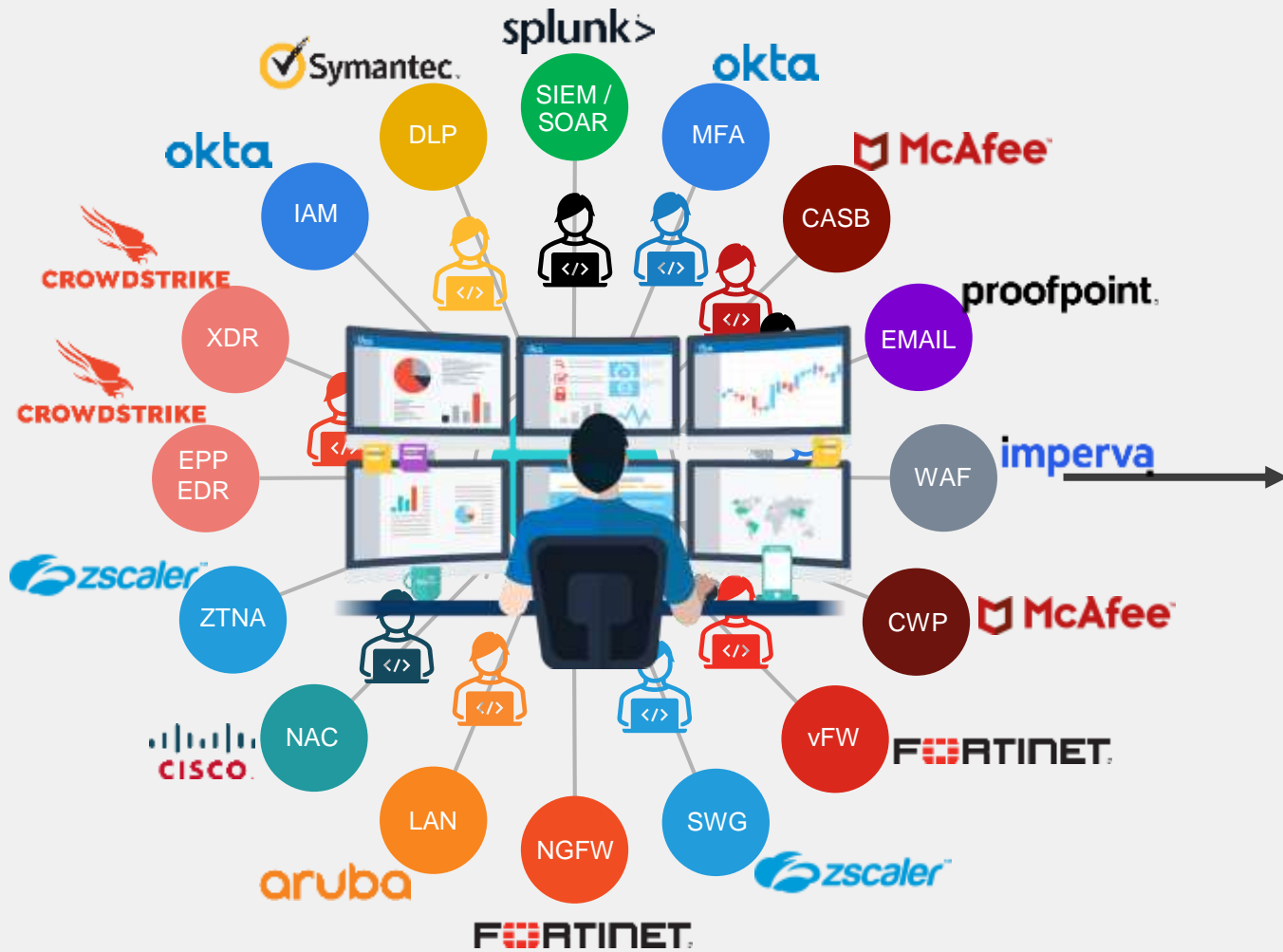


- Regularien (extern)
- Interne Vorgaben
- Praxistauglichkeit umsetzen

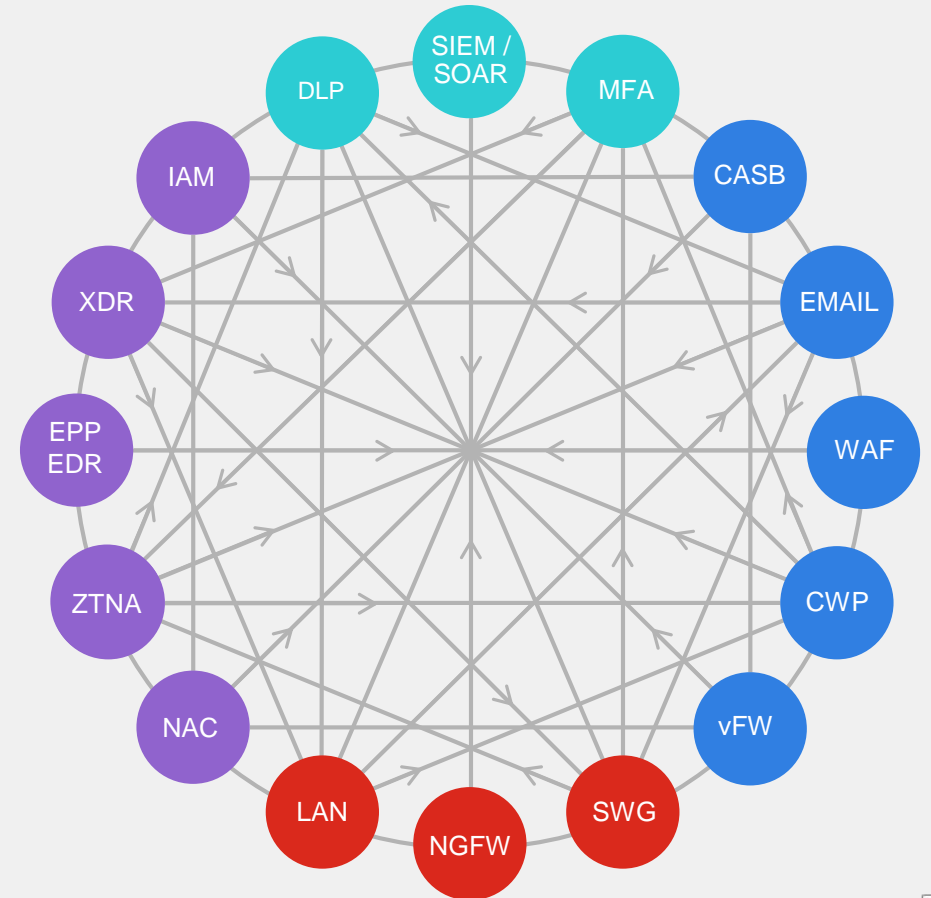
Security Fabric

Gartner Cybersecurity MESH Architecture (CMSA)

20 Cybersecurity Point Products (11 Vendors)



Cybersecurity Platform Approach 4-6 Platforms



Fortinet Security Fabric

Umfassend

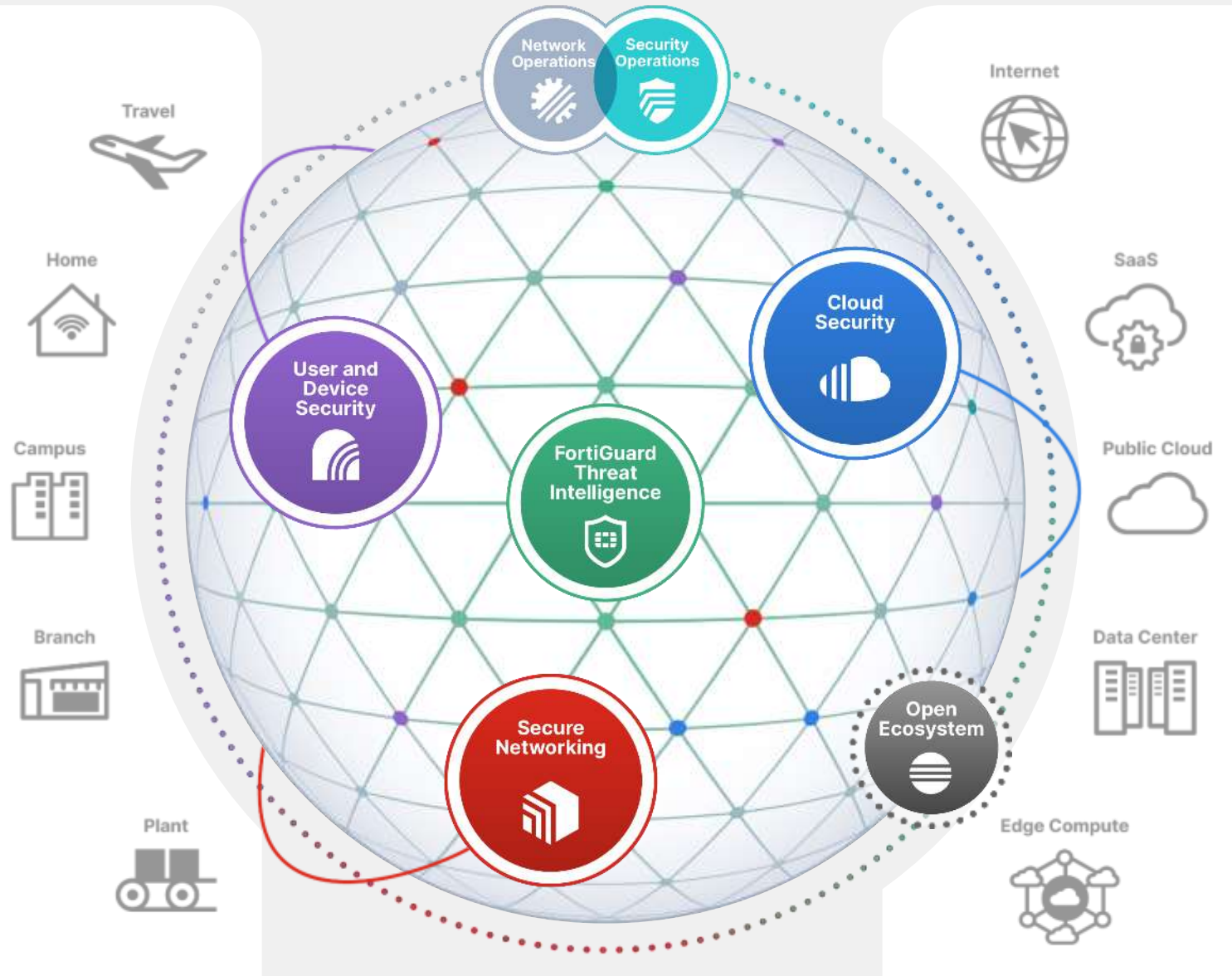
Transparenz und Schutz der gesamten digitalen Angriffsfläche für ein besseres Risikomanagement

Integriert

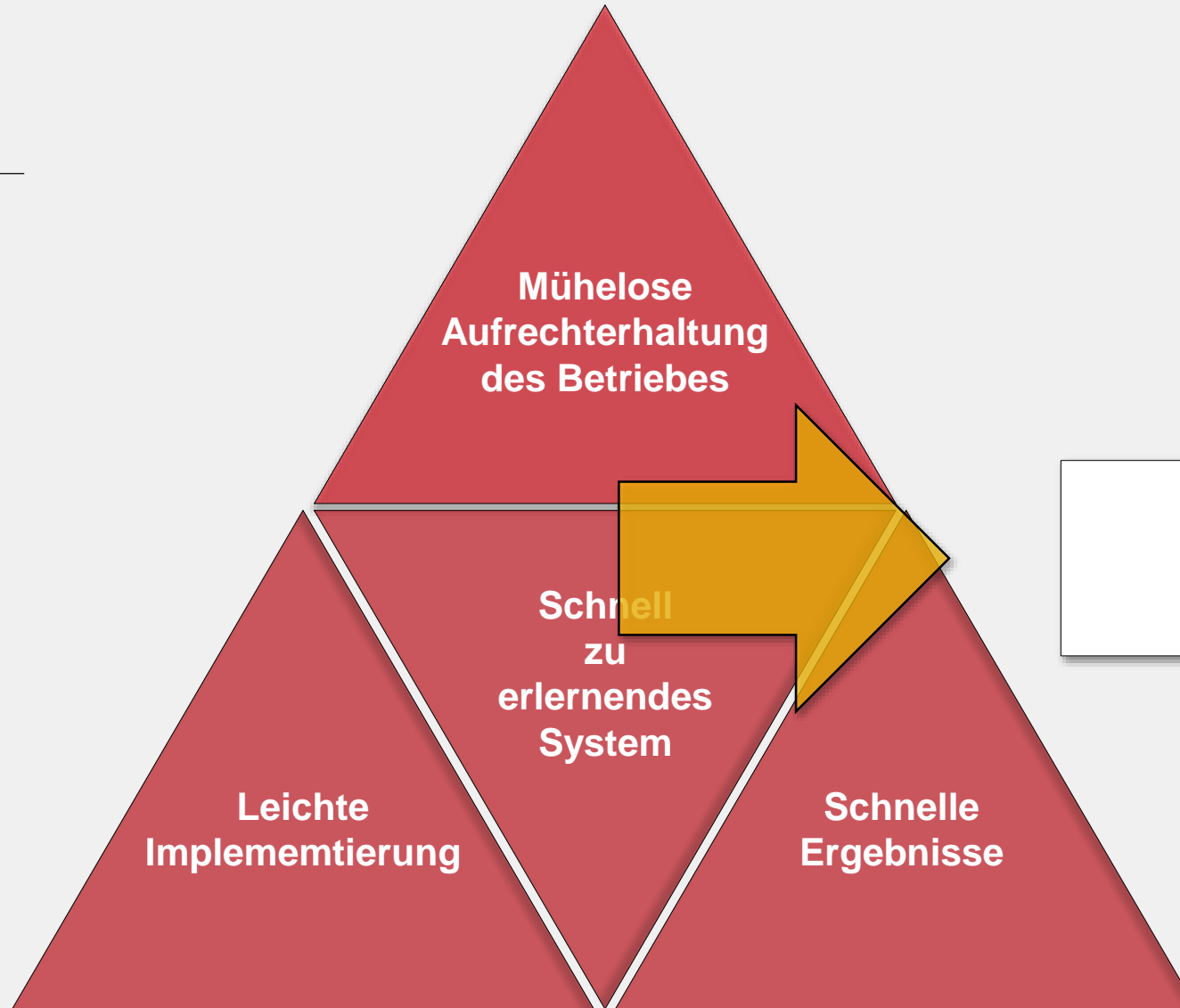
Lösung, die die Komplexität reduziert und Bedrohungsinformationen weitergibt

Automatisiert

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



Ihre Anforderungen

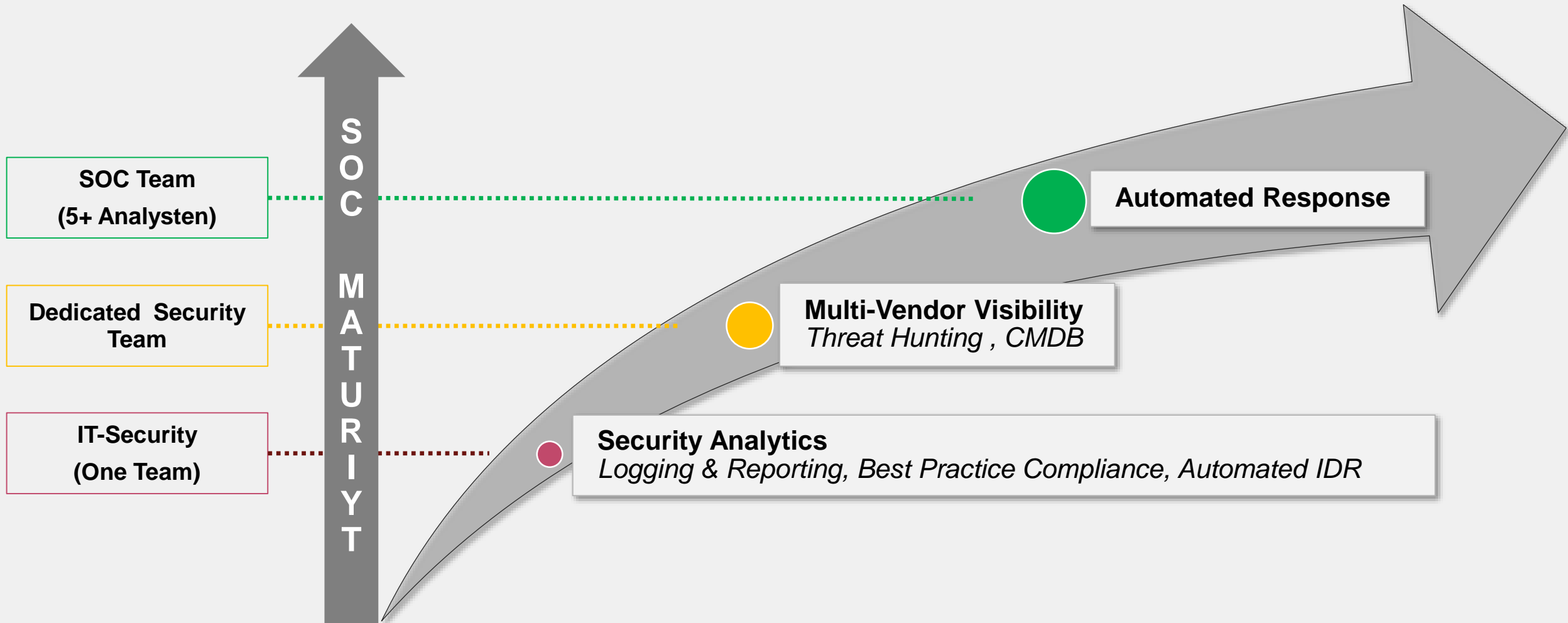


Der Weg zu einem SoC

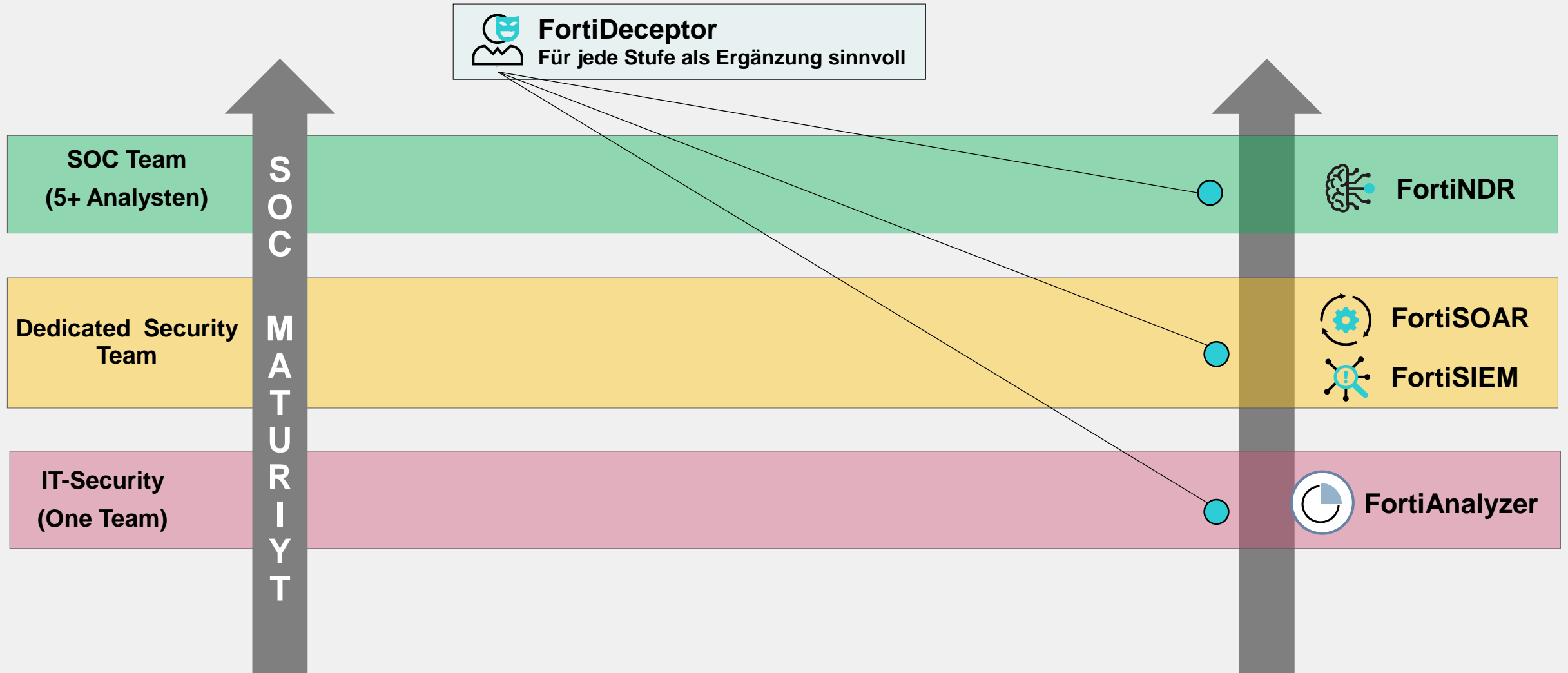
Von der Notwendigkeit zum Security Team



Sicherheitskomplexität auf Basis der SOC Maturity

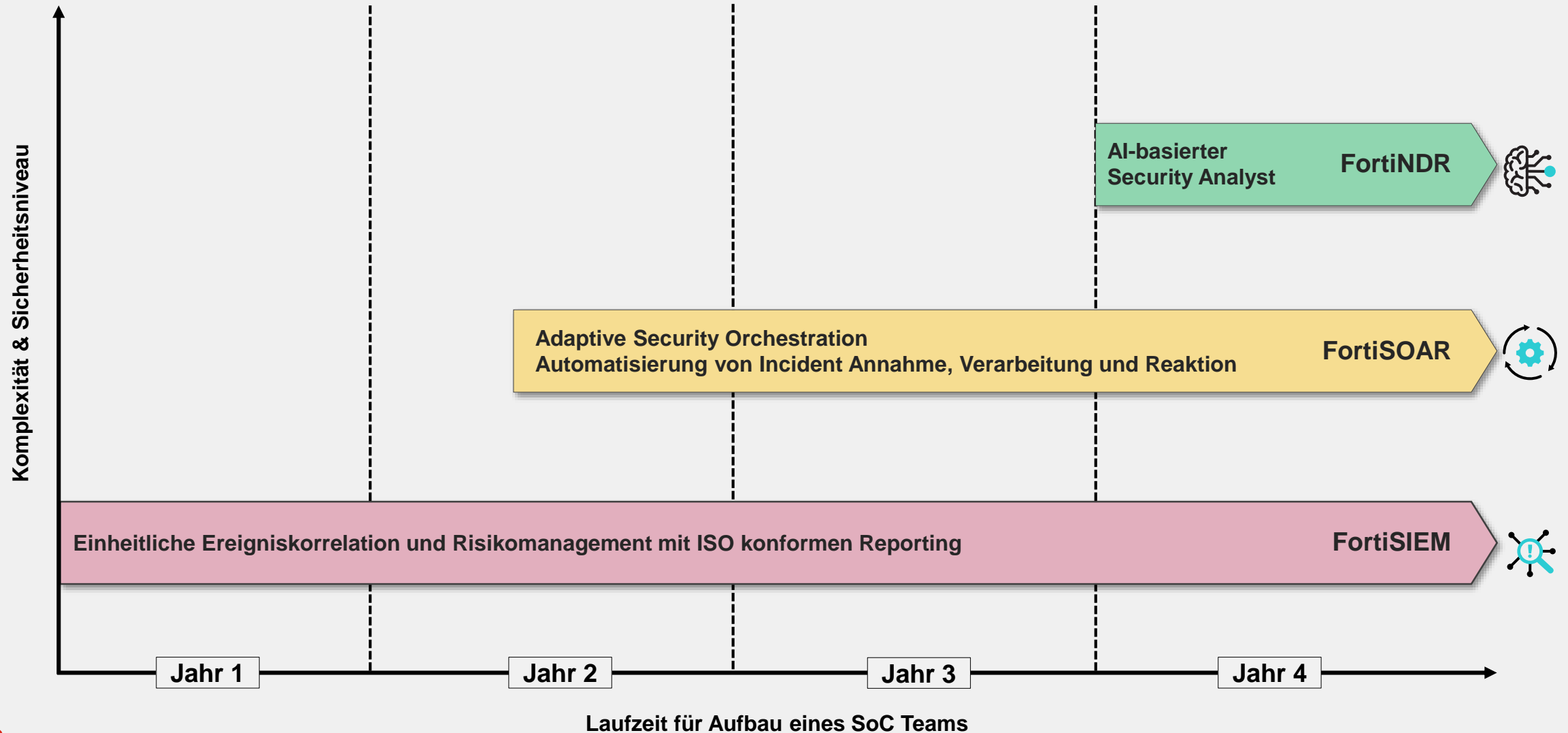


Produkteinordnung auf Basis der SOC Maturity



Produkteinführung in Phasen

Ein Beispiel



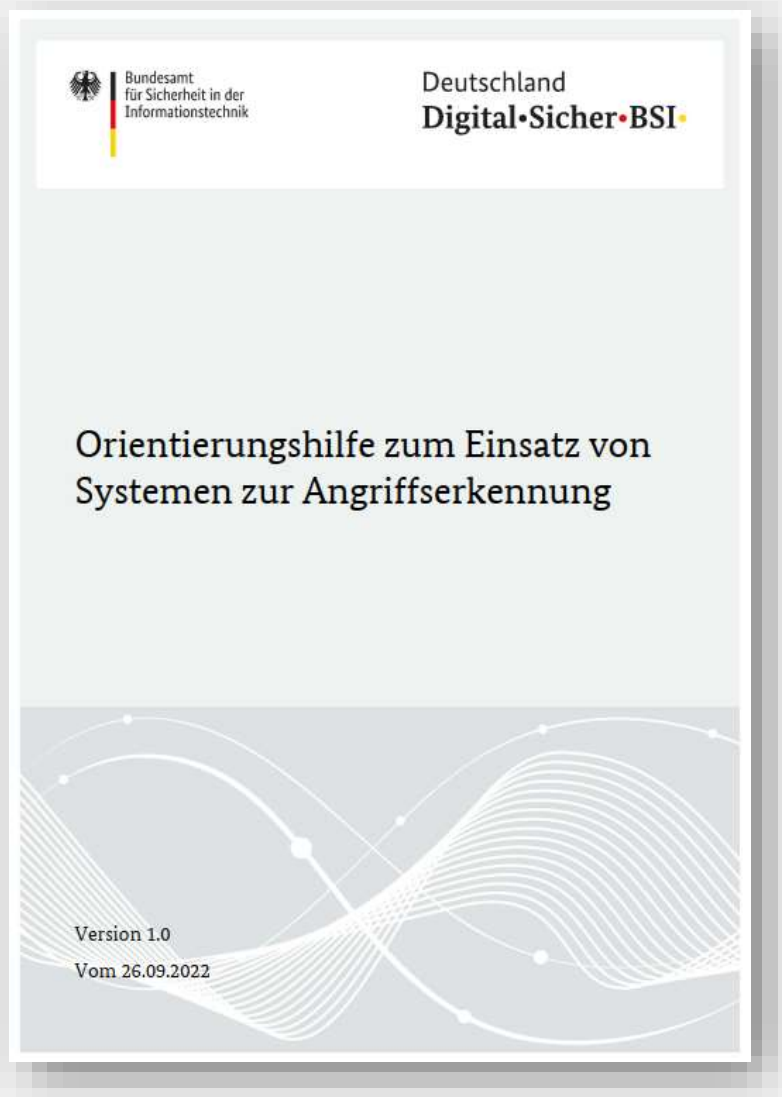
Wichtigkeit und Aufgaben eines SoC

Eine Ableitung aus BSIG, IT-SIG und NIS2UmsuCG



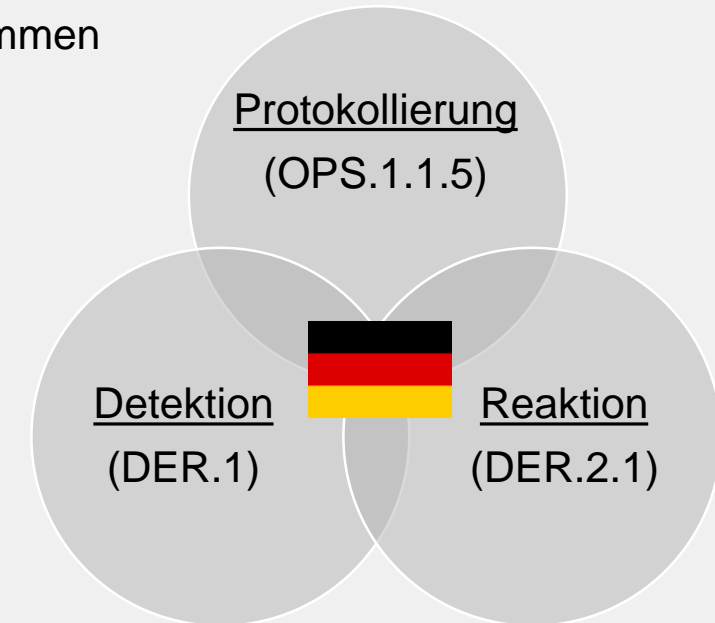
BSI: Orientierungshilfe Angriffserkennung

Nach § 8a Absatz 1a BSIg



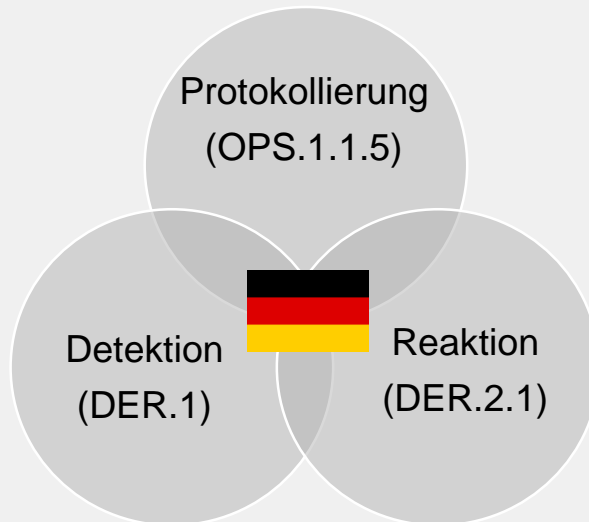
Weiterführende Orientierung:

- 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)

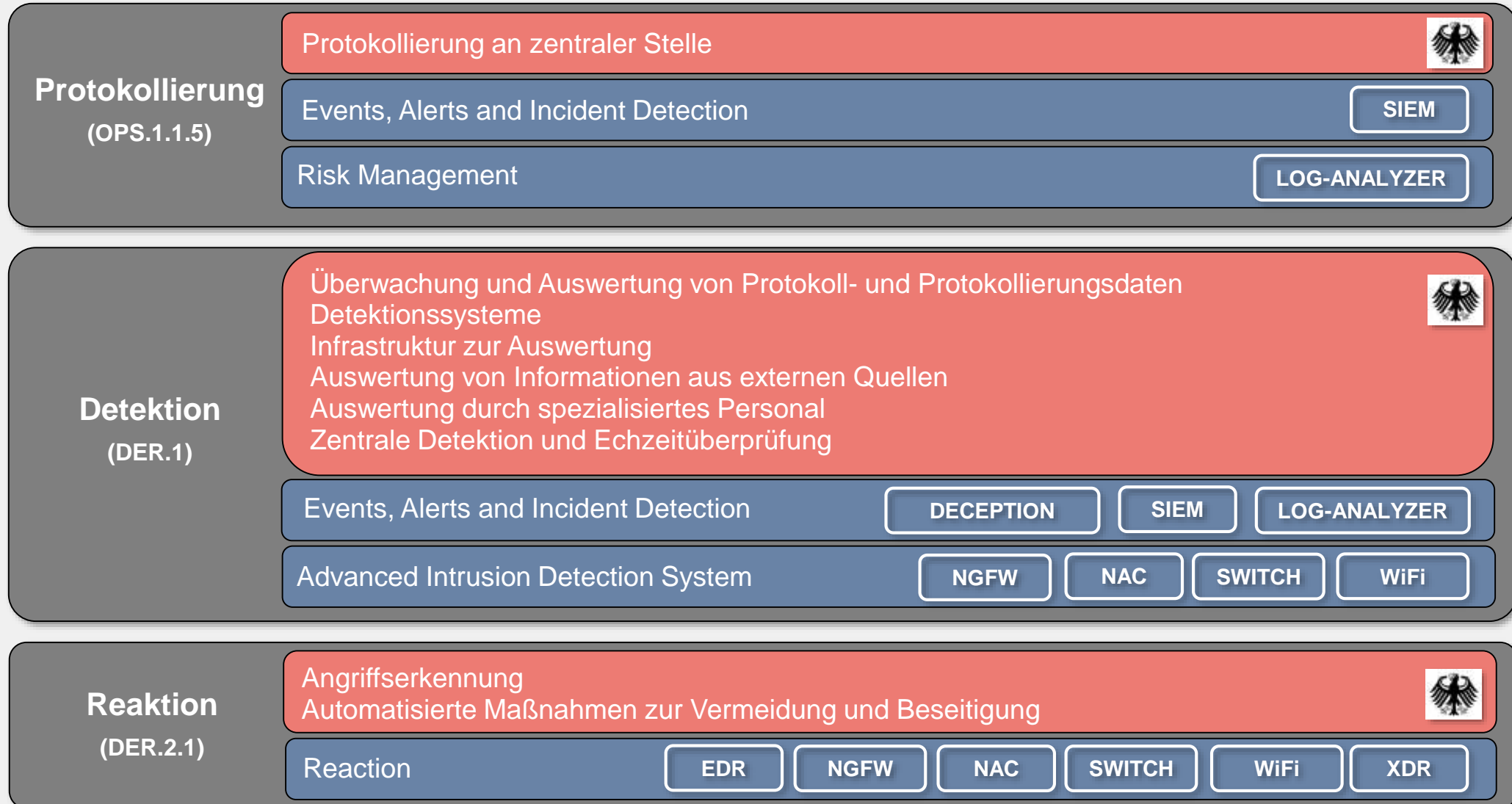


Die zur Angriffserkennung eingesetzten Systeme **SOLLTEN** automatisiert **Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen** ergreifen können,

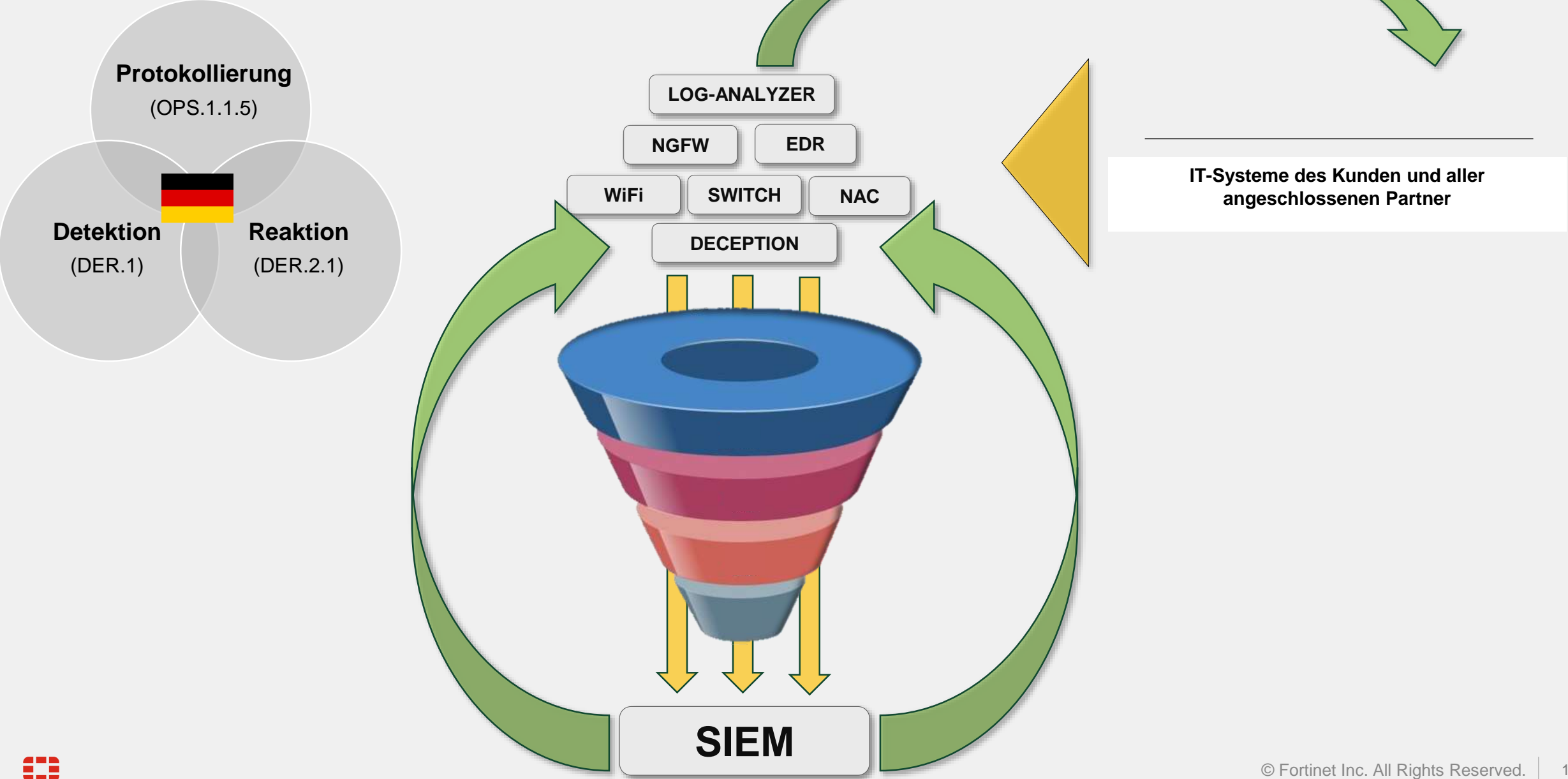
Dabei **MUSS** gewährleistet sein, dass **ausschließlich** automatisiert ergriffene **Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.**

Umsetzung „Angriffserkennung IT-SIG“

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



Welche Rolle spielt ein SIEM im SoC?



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



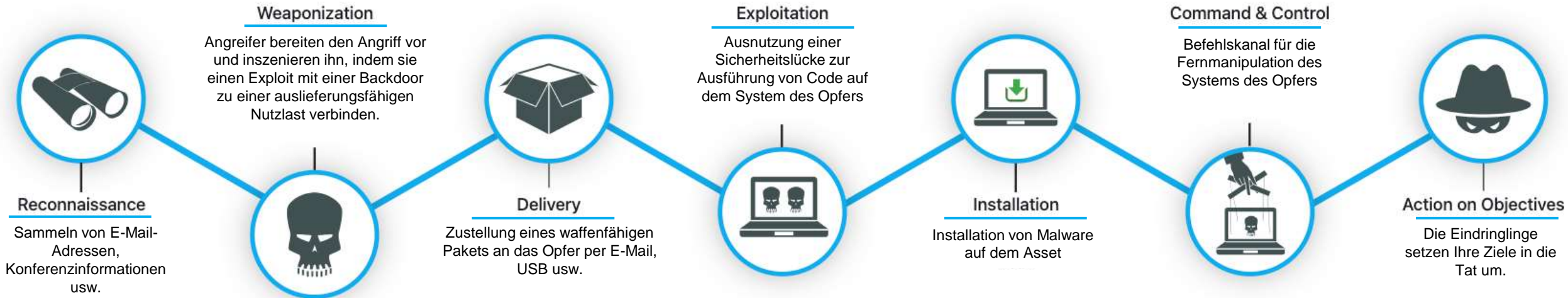
MITRE ATT&CK[®] Framework

Strukturierte Reaktion auf Angriffe



Wie wird angegriffen?

The Kill Chain



Wofür steht....

MITRE | ATT&CK[®]

**Adversarial Tactics, Techniques
&
Common Knowledge**



MITRE | ATT&CK®

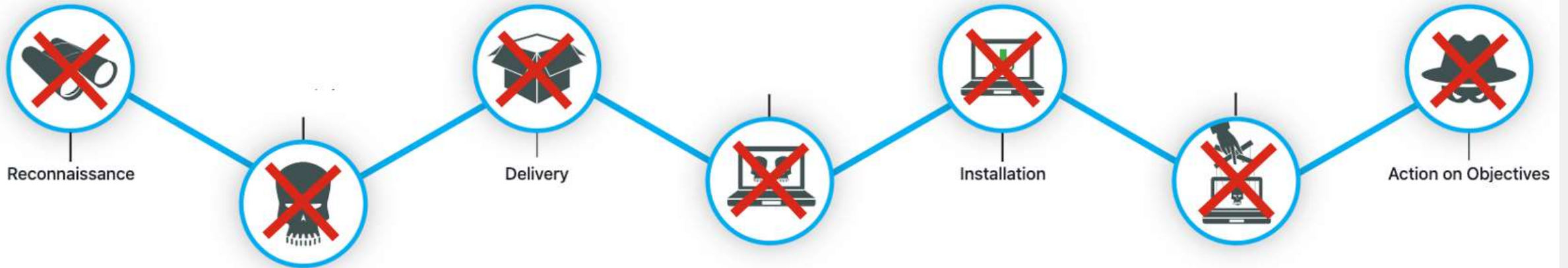
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection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



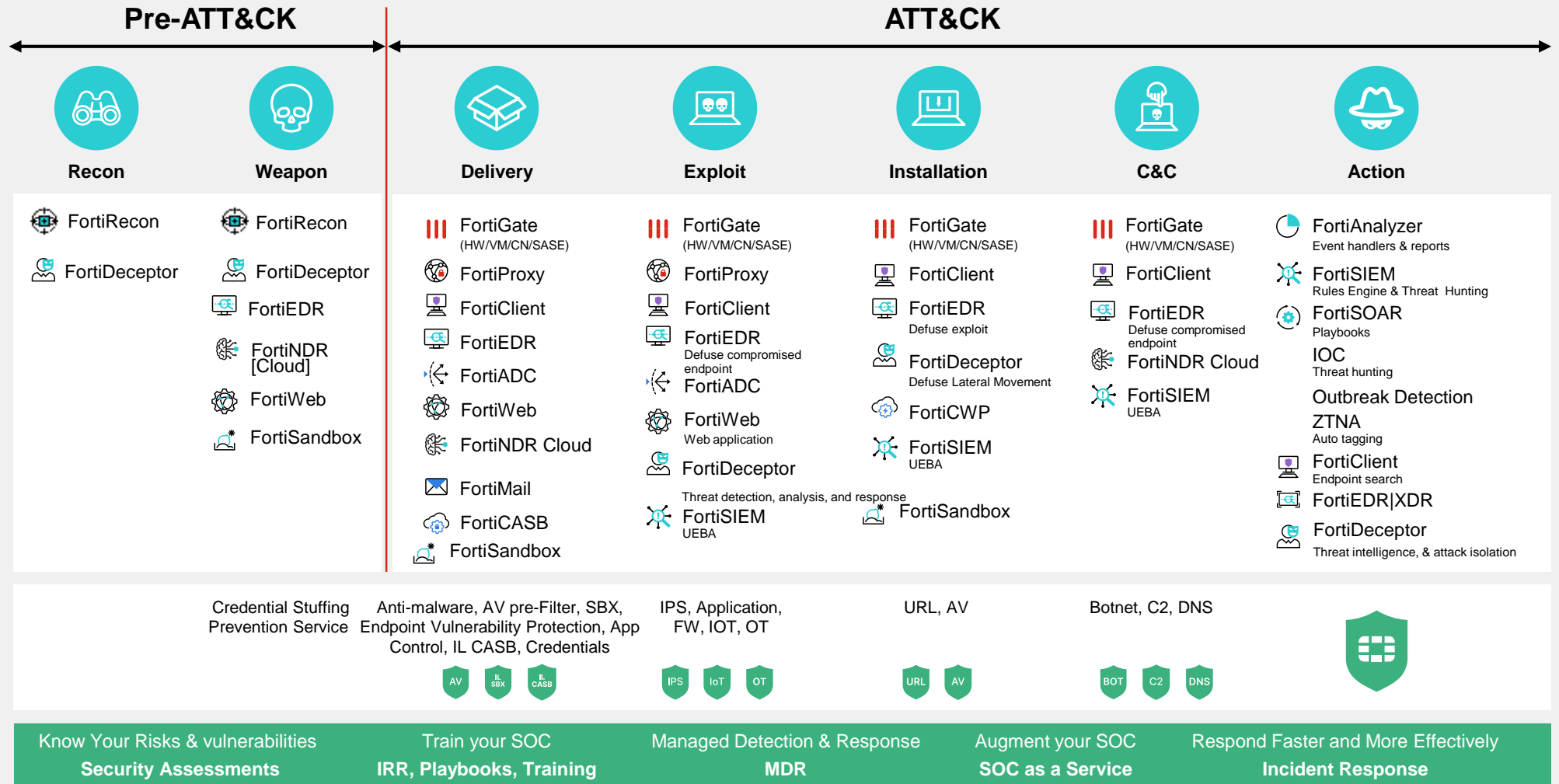
Weaponization

Exploitation

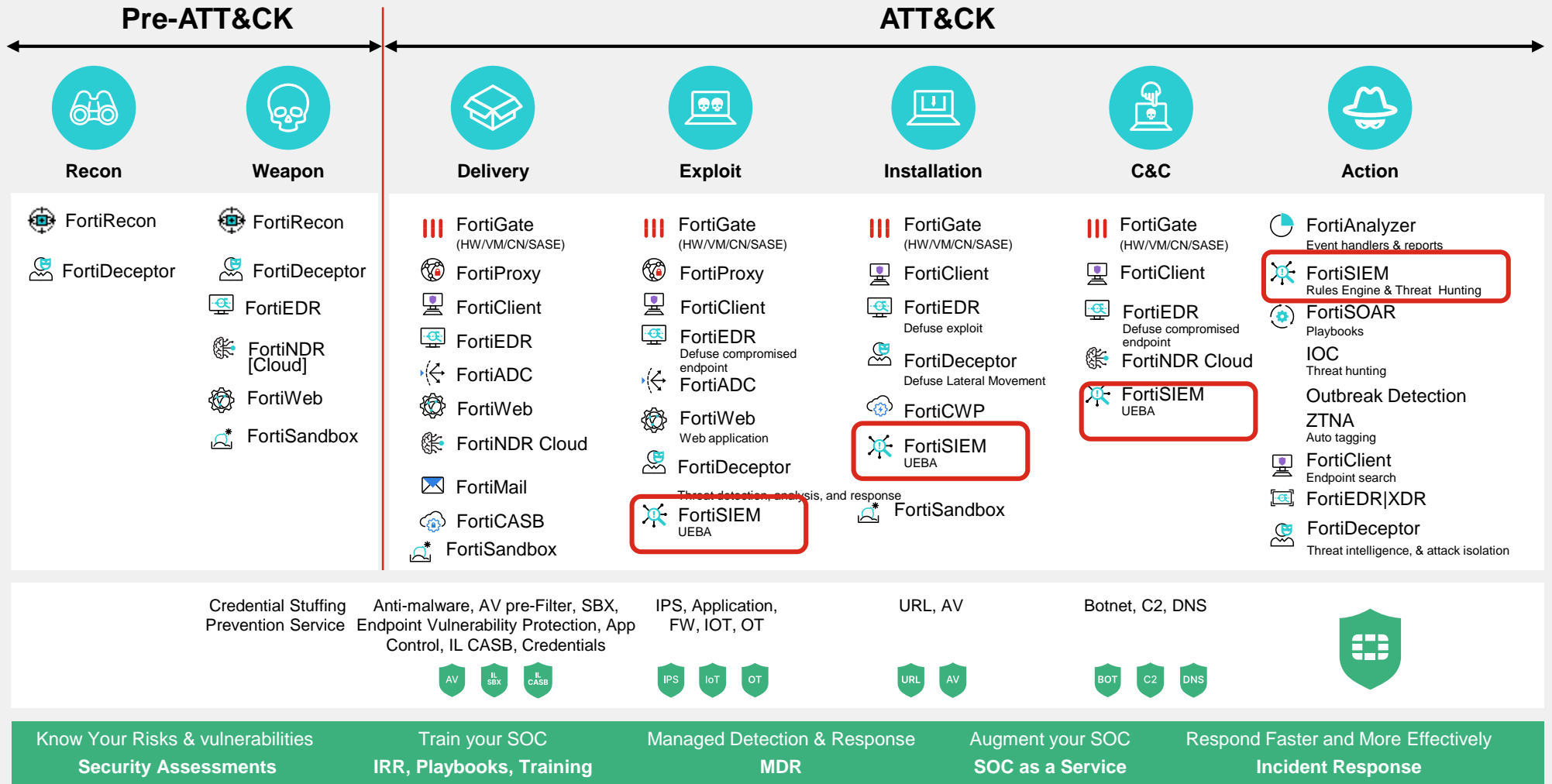
Command & Control



Fortinet bietet Sichtbarkeit und Risikomanagement



Fortinet bietet Sichtbarkeit und Risikomanagement



Warum FortiSIEM

Warum ein SIEM nicht kompliziert sein muss



Security

Exploits

Authentication

Vulnerabilities

Policy Violation

Behavior Anomaly

Airline Security

Performance

Application

Server

Change

Server

Network

Storage

Availability

System

Network

Server

Environmental

Network

Application

Beaconing

Beaconing

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

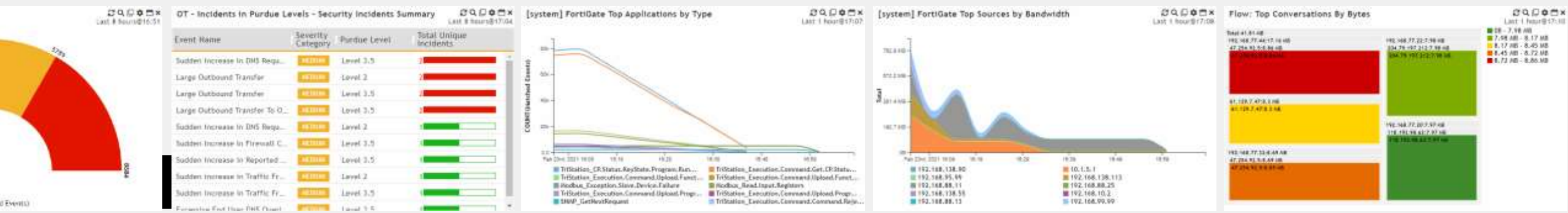
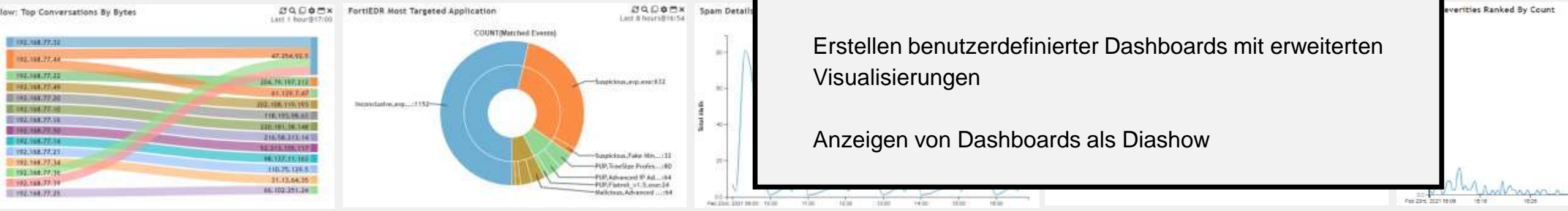


Flexible Dashboards

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

Erstellen benutzerdefinierter Dashboards mit erweiterten Visualisierungen

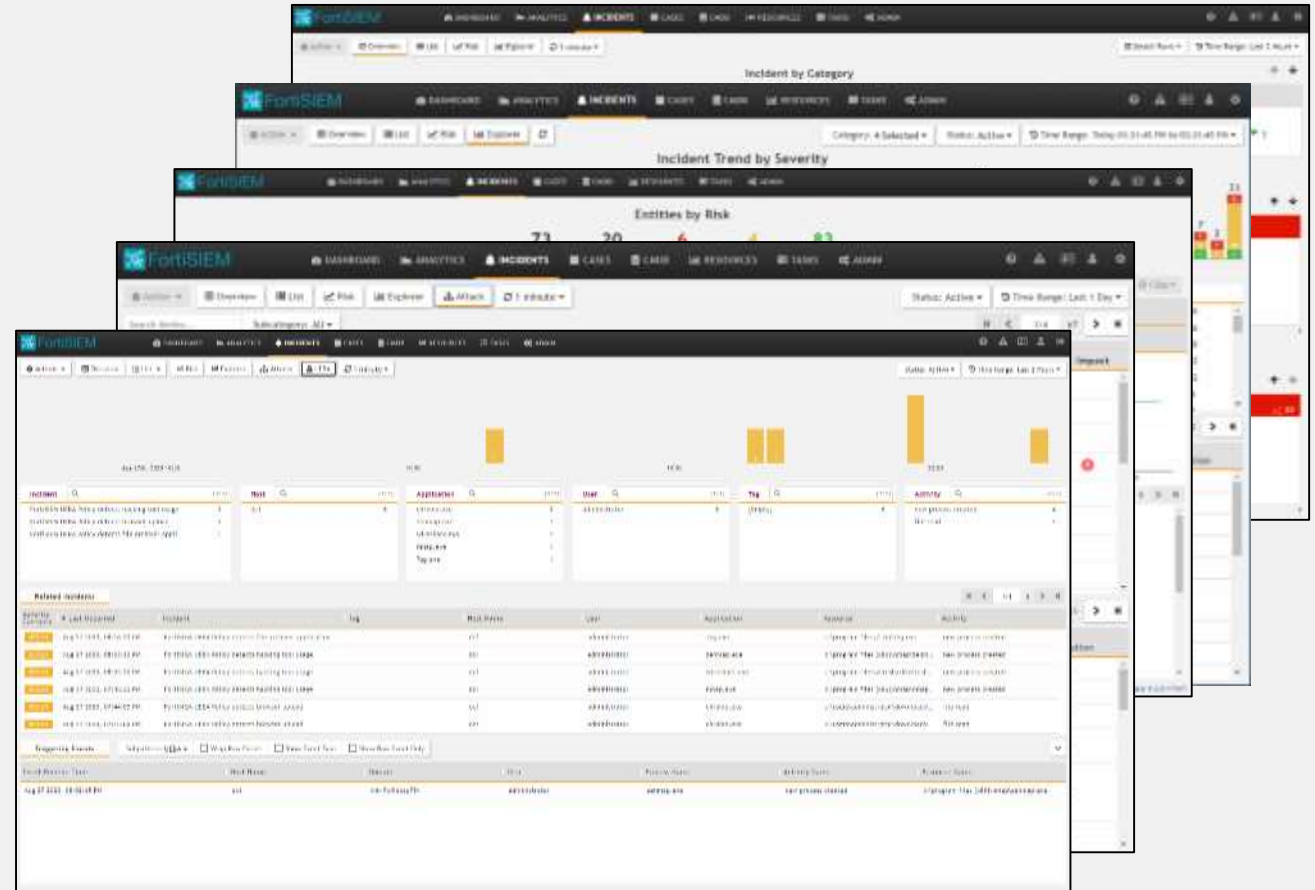
Anzeigen von Dashboards als Diashow



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

The screenshot displays the FortiSIEM Incident Explorer interface. The top navigation bar includes 'DASHBOARD', 'ANALYTICS', 'INCIDENTS', 'CASES', 'CMDB', 'RESOURCES', 'TASKS', and 'ADMIN'. The main content area is titled 'MITRE ATT&CK: Incident Explorer' and shows a table of device coverage for various MITRE ATT&CK tactics. Below this, a 'Related incidents' section lists specific events with their severity, occurrence time, incident details, tactics, techniques, sources, targets, and status.

Device	Command and Control	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
192.168.22.16		4		4			27		4		4		
win2008-ads				34			3						
[Empty]		3		3	2	2	1					8	5
192.168.15.1		5		5	4	4	1		1				
orders-erp										4		1	14
10.95.7.10		4		4	4	4							
10.95.7.151		4		4	4	4							
10.95.7.154		4		4	4	4							

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status
MEDIUM	Apr 08 2021, 03:48:00 PM	Excessive End User DNS Qu...	Command And Co...	Dynamic Resolut...	192.168.22.11		Triggered Event Count: 512	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: W32/Agent.ZIMTr Risk Name: Malicious Informational URL: trilog.exe	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: W32/Patched.SAPTr Risk Name: Malicious Informational URL: wrac591.exe	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: VBA/Agent.DOVTr.dldr Risk Name: Malicious Informational URL: Untitled-59129-160948...	Active
LOW	Apr 08 2021, 03:48:00 PM	Multiple Logon Failures: Do...	Credential Access	Brute Force: Pass...	192.168.26.120	WIN2008-ADS 192.168.0.10 Domain: random.org Show More	Triggered Event Count: 7	Active



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**

FortiSIEM

Dashboard Analytics Incidents Cases CMDB Resources Tasks Admin

Search Machine Learning Investigation Clustering: KMeans: ML: Host Ping Response Time

Prepare Train Schedule

Input details

Report: ML: Host Ping Response Time

For Org: All

Algorithm Setup

Run Mode: LOCAL

Task: Clustering

Algorithm: KMeans

Parameters: N Clusters: 8
Init: k-means++
N Init: 10
Max Iter: 300
Tol: 0.0001
Random State: 42
Algorithm: auto

Features: AVGavgDurationWSec

ID Field: hostName

Train Factor: 70

Schedule setup

Job ID: #System

Job Name: Cluster hosts based on ping response times and detect anomaly via cluster change

Job Description: This job clusters hosts based on ping response times. When scheduled to run, an incident will trigger if an VM, based on current values, belongs to a different cluster than in the model. This means that the behavior of the host has changed.

Inference Schedule: 1 Hour

Re-training Schedule: 7 Days Report Window: 2 Days

Job Group: Clustering

Action on Inference

Create an incident when Cluster changes

Send mail when Cluster changes Email 1, Email 2, ...

Enabled

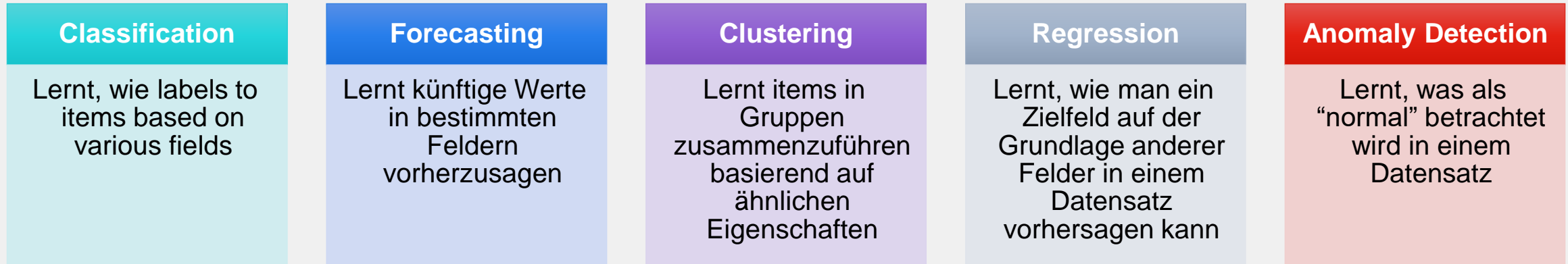
Save

Copyright © 2023 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 7.8.0.0024



Machine Learning Workbench

Learning Tasks Supported



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 Anmeldeusername zwischen Benutzern und Arbeitsstationen und Bilden dynamischer Peer-Benutzergruppen mit ähnlichen Anmeldeusername



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

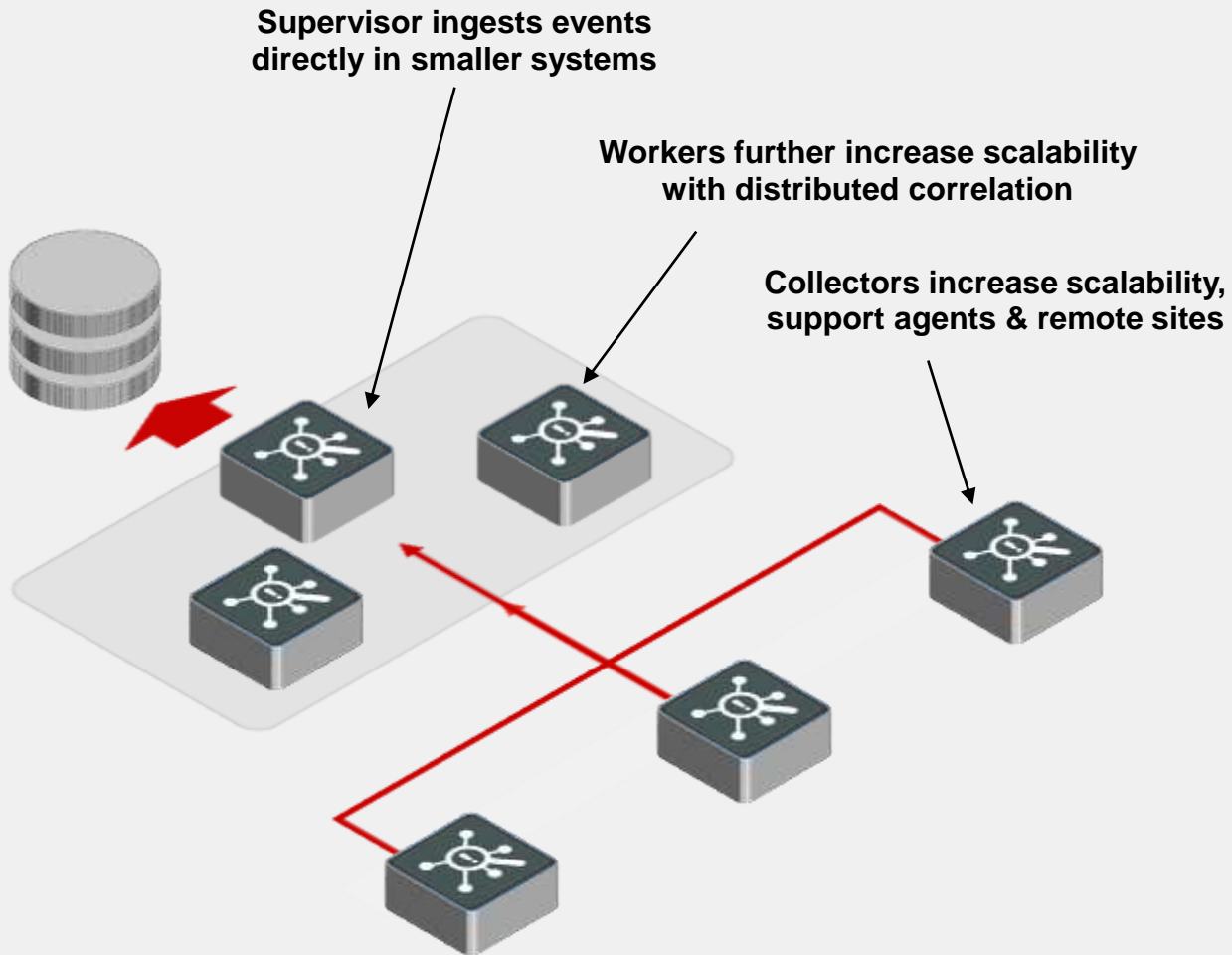
CPU
Memory
Storage
Uptime
Services
Interface Utilization

Combined SOC & NOC

Integrated CMDB | FortiGuard Threat Intelligence
Increased Functionality | Increased Visibility | Reduced Time to Respond



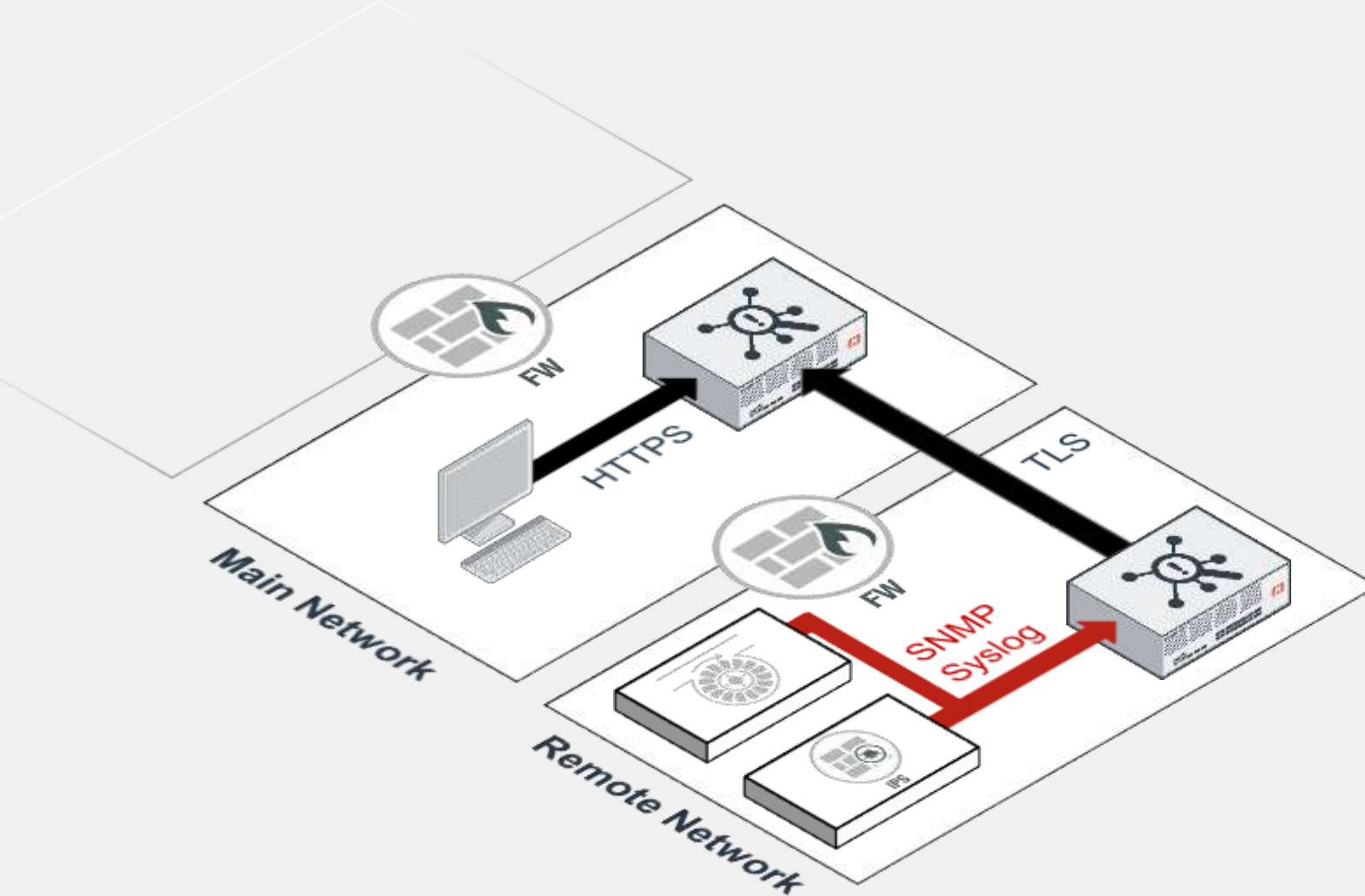
Rapid Scale Architecture



- 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

The screenshot shows the FortiSIEM interface with the 'Rules' page selected. The table below is a representation of the data shown in the screenshot:

Active	Severity	Name	Description	Tactics	Technique	Scope	Test Status	Exception
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux File Changed From Baseline	FortiSIEM Linux Agent FIM detected that a file changed from its baseline	Defense Evasion, Impact	Indicator Removal on Host: File Deletion [T1070.004], Data Manipulation: Stored Data Manipulation [T1565.001]	System		
<input checked="" type="checkbox"/>	5 - MEDIUM	(s) Agent FIM: Linux File Content Modified	Detects that a user modified either the content or the attributes of a file or directory	Defense Evasion, Impact	Indicator Removal on Host: File Deletion [T1070.004], Data Manipulation: Stored Data Manipulation [T1565.001]	System		
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux File or Directory Created	FortiSIEM Linux Agent FIM detected that a file or a directory was created	Collection, Impact	Data Staged: Local Data Staging [T1074.001], Data Manipulation: Stored Data Manipulation [T1565.001]	System		
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux File or Directory Deleted	FortiSIEM Linux Agent FIM detected that a file or a directory was deleted	Defense Evasion, Impact	Indicator Removal on Host: File Deletion [T1070.004], Data Manipulation: Stored Data Manipulation [T1565.001]	System		
					Data Manipulation: Stored Data Manipulation [T1565.001]			

Einfacher Zugriff auf MITRE ATT&CK®-Daten

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

The image shows a screenshot of the FortiSIEM interface. A dialog box titled "Valid Accounts Details" is open, displaying the following information:

- Tactics: Initial Access
- Technique: **Valid Accounts: Local Accounts** (ID: T1078.003)
- Platform: Linux, Windows, macOS
- Description: Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping].

A red box highlights the "Valid Accounts: Local Accounts" link in the dialog box. A red arrow points from this link to the MITRE ATT&CK website. The website shows the "Valid Accounts: Local Accounts" page, which includes a navigation menu and a description of the technique.

The MITRE ATT&CK website navigation menu includes:

- Home > Techniques > Enterprise > Valid Accounts > Local Accounts
- Techniques
- Enterprise
- Reconnaissance
- Resource Development
- Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions

The main content of the page is titled "Valid Accounts: Local Accounts" and includes a sub-section "Other sub-techniques of Valid Accounts (4)". The description states: "Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping]. Password reuse may allow the abuse of local accounts across the purposes of Privilege Escalation and Lateral Movement."



Integrationen



FortiSIEM Integrations

300+ Integrations across vendors and applications

Service Desks & Cloud



Security & Intelligence



Applications



Operating Systems



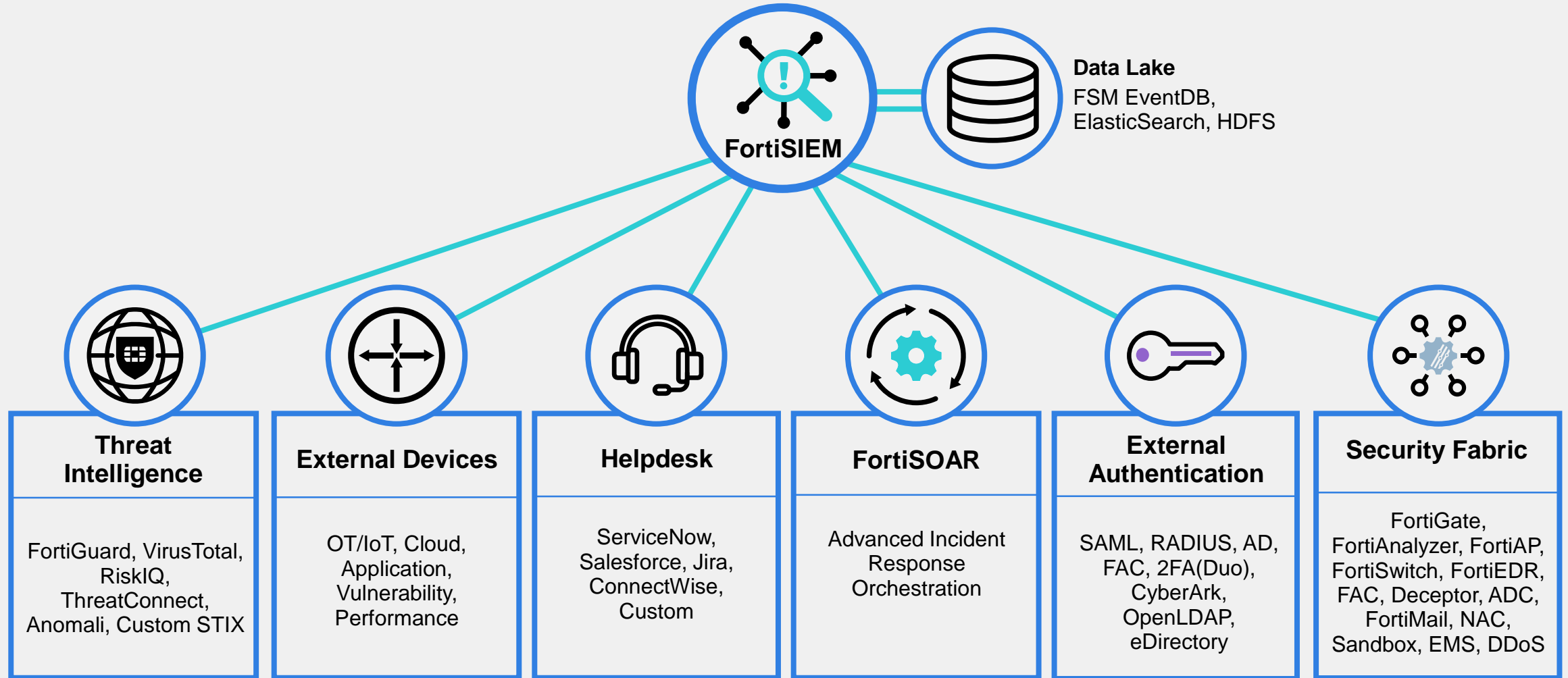
Infrastructure



Platforms



Hauptbereiche der Integration



F**RTINET**®