FORTINET

Meshed Security
Moderne Sicherheitsstrategien

Mirko Herth – Business Consultant

Cyber Kill Chain®

Eine historische Sichtweise

Reconnaissance
Erkundung
Aufklärung

Weaponization
Bewaffnung
Angriffsvektor

Delivery
Zustellung
Umsetzung

Exploit
Ausnutzung
Ausbeutung

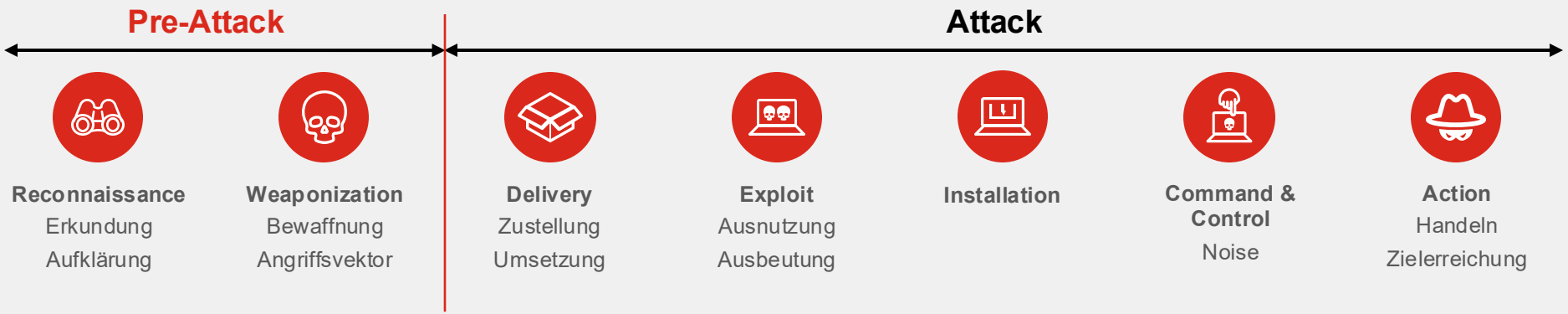
Installation

Command & Control
Noise

Action
Handeln
Zielerreichung

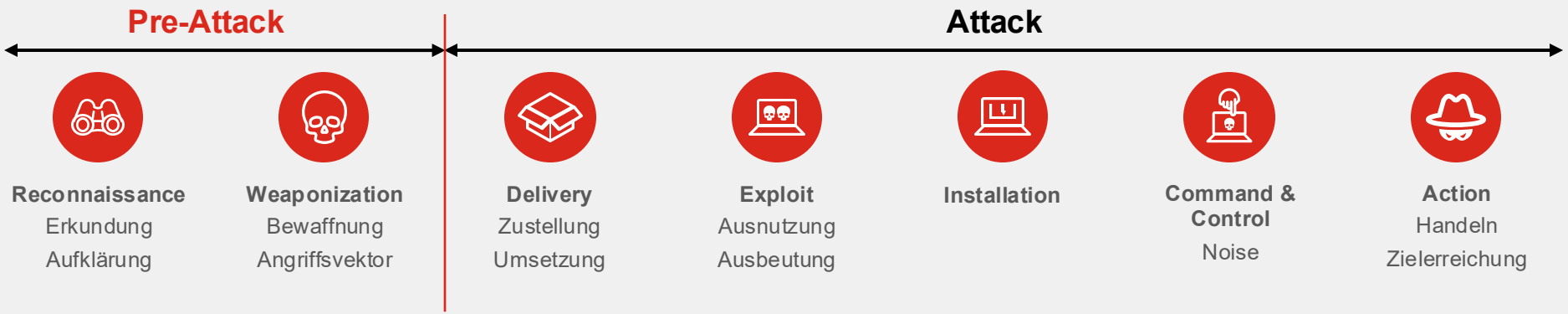
Cyber Kill Chain®

Eine historische Sichtweise



Erkundung ist heutzutage immer!

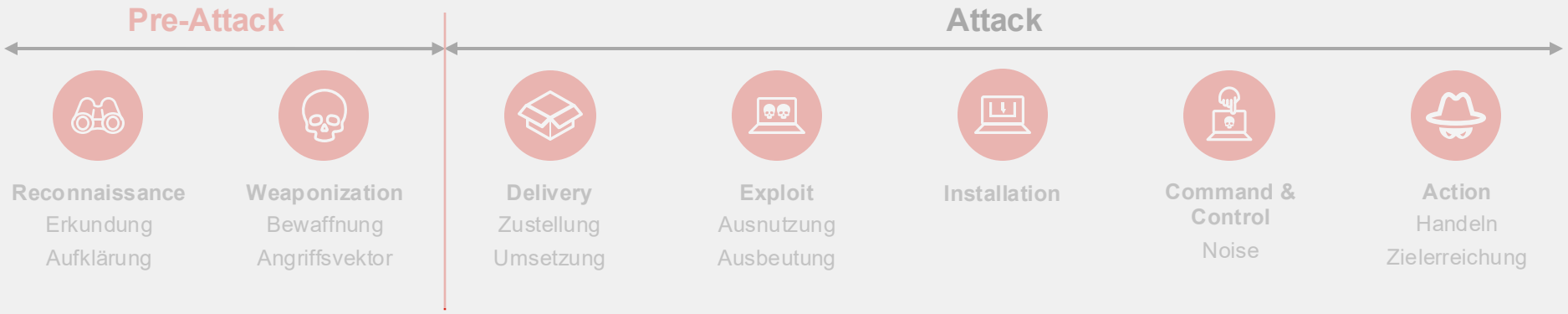
Perimeter nicht klar abzugrenzen



- **Advanced Persistent Threats**: Nicht „eine“ Aktion
- **Ausweitung der Erkundung**: Im Netzwerk, in der Cloud, Lieferkette
- **Unbemerkt**: Fileless, LOTL

IT-Security aus Sicht der Angreifer

Welche Ziele verfolgen Angreifer?



- **Monetarisierung**
  - **Diebstahl**: Datenexfiltration (Ausschleusung von Daten), pbD oder geistiges Eigentum usw.
  - **Verschlüsseln**: Ransomware-Angriffe, um Lösegeld zu erpressen
- **Zerstörung**: Cyber-Terrorismus, gezieltes Löschen, Manipulation oder Beschädigung von Daten

Fortify your data

1 Data in motion

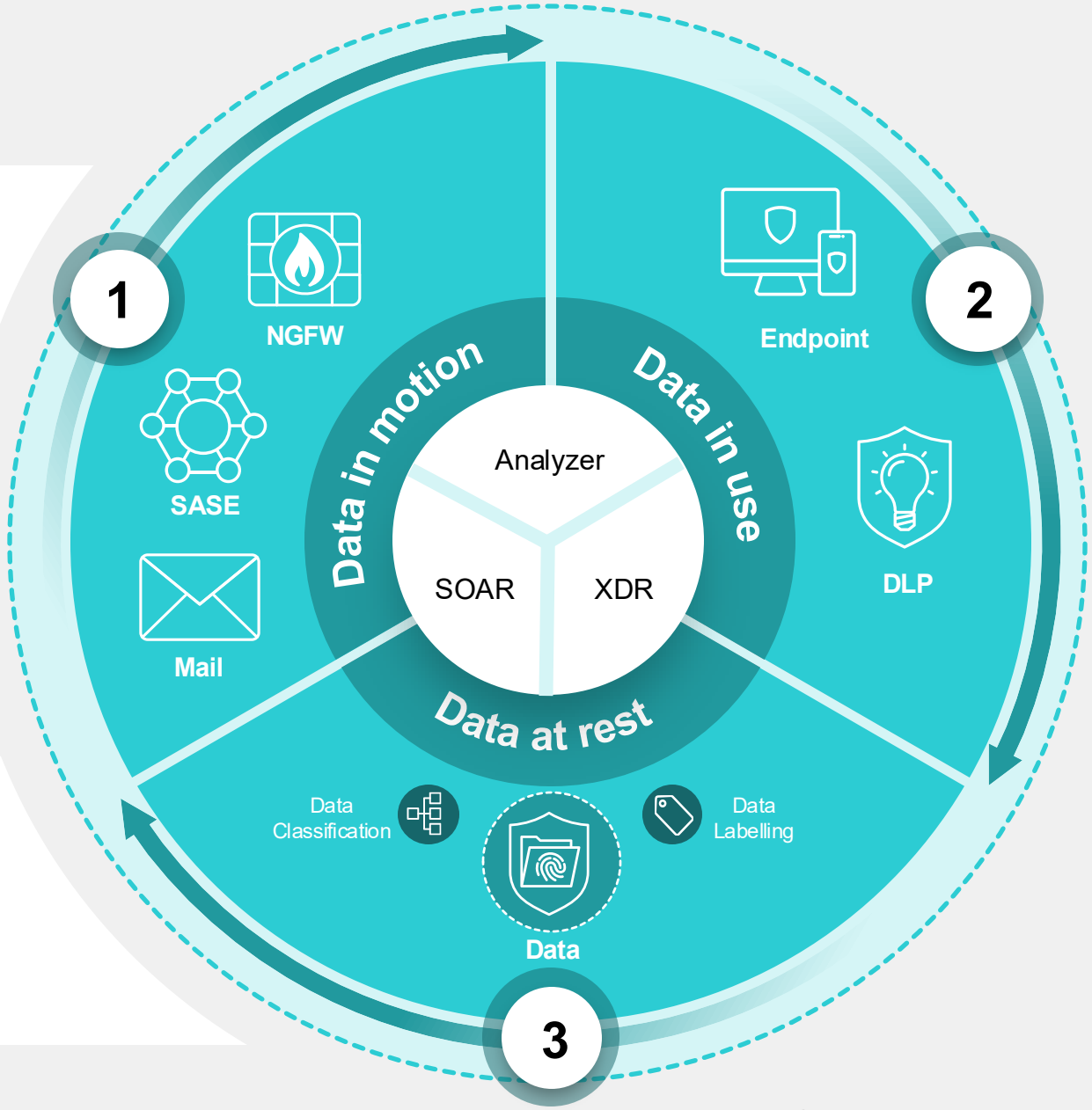
- Massive amounts of data
- BYOD, Cloud storage, hybrid work environments result in the footprint of sensitive data multiplying manifold

2 Data in use

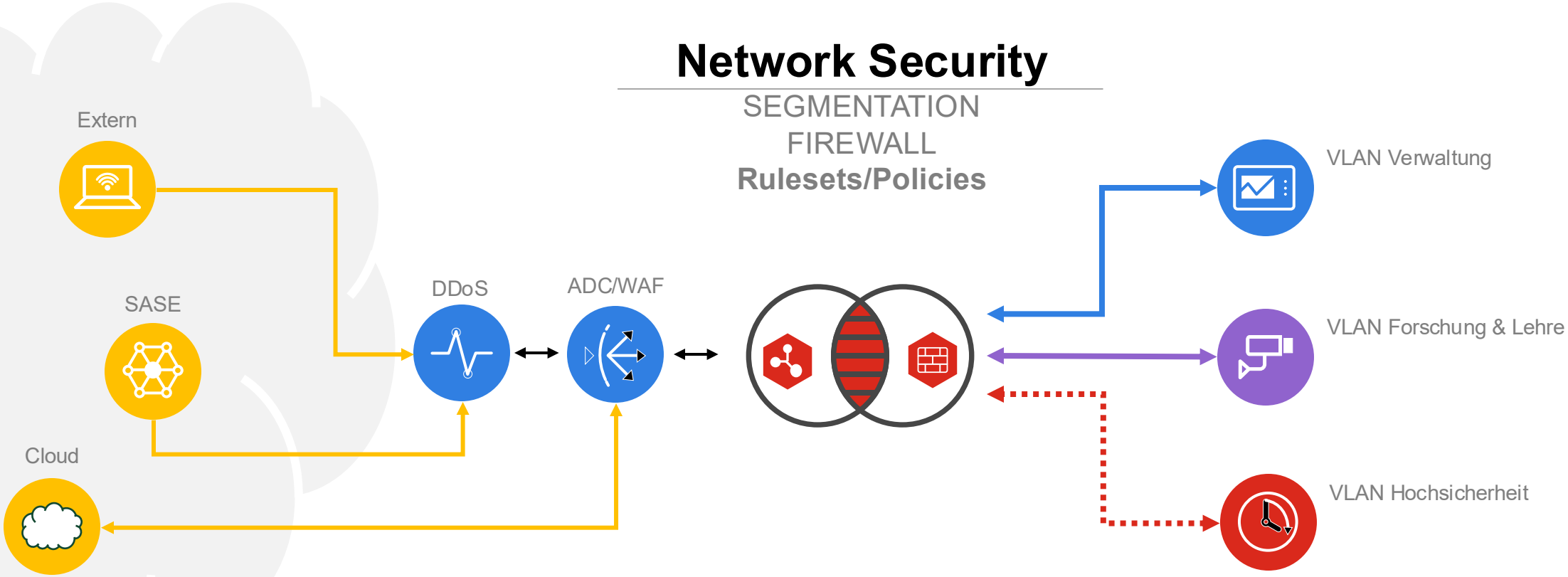
- Push towards using GenAI for productivity leads to sensitive corporate data being fed into applications like ChatGPT. Corporate sensitive data being accessed from anywhere

3 Data at rest

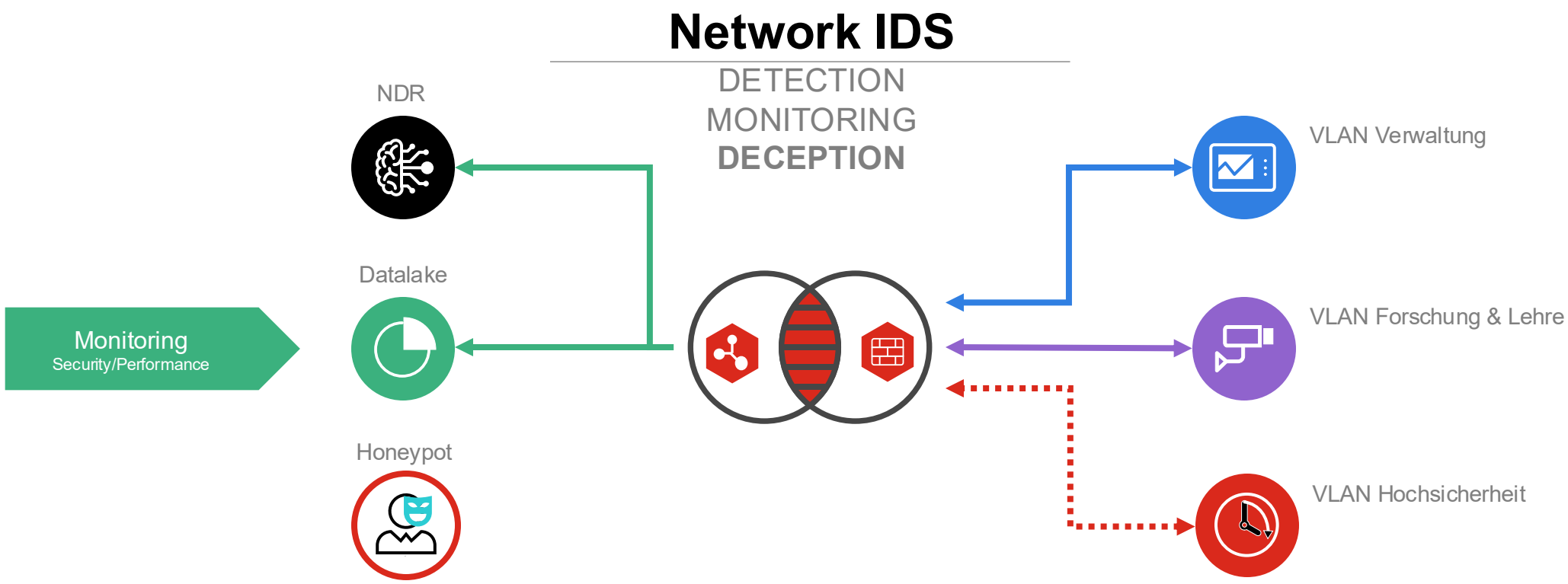
- FortiData enables the customer to discover and label sensitive data on cloud and on-premises data stores using modern AI machine learning technology. Integration with FortiGate brings additional context about the data for better automated enforcement



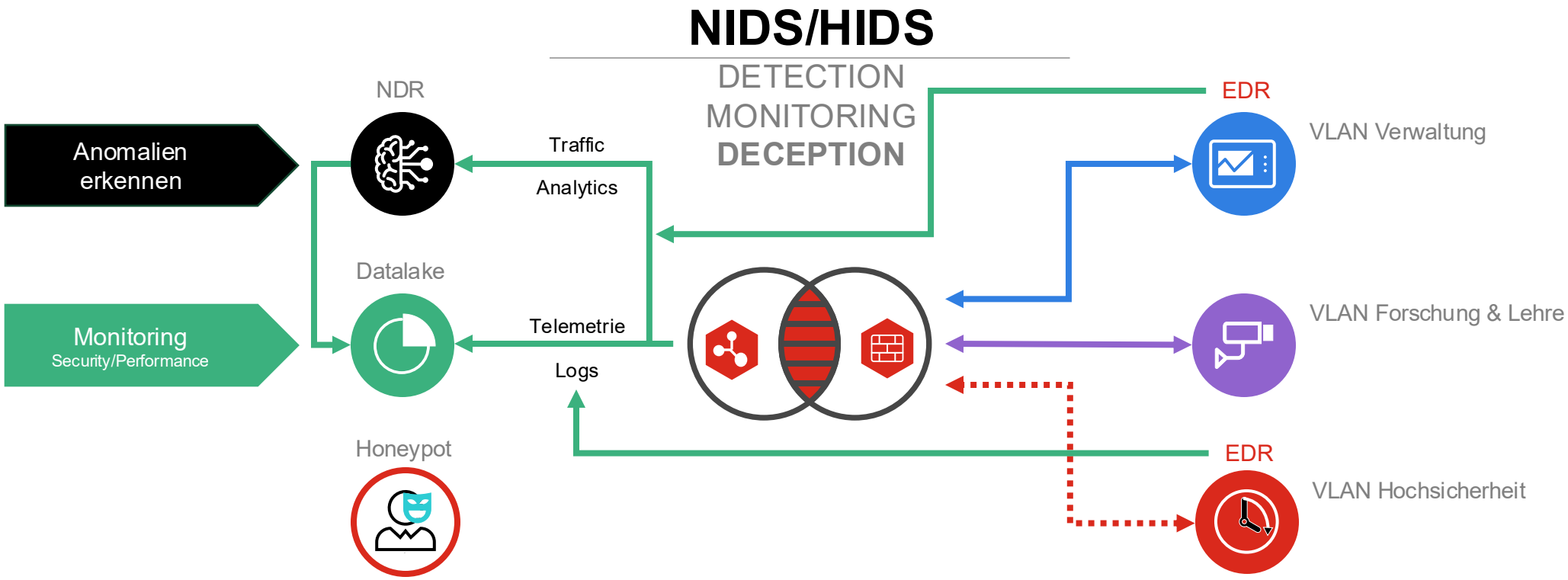
Technologisch: Kenne dein Netzwerk



Technologisch: Behaviour Analytics

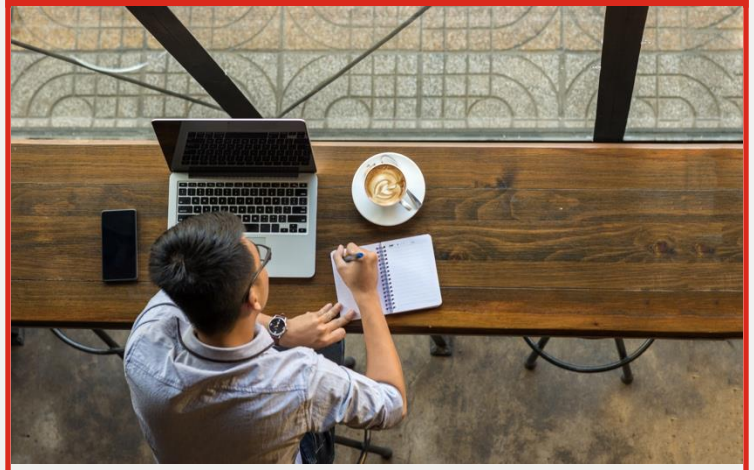


Technologisch: Behaviour Analytics



Sichtbarkeit – Detection & Response

EDR

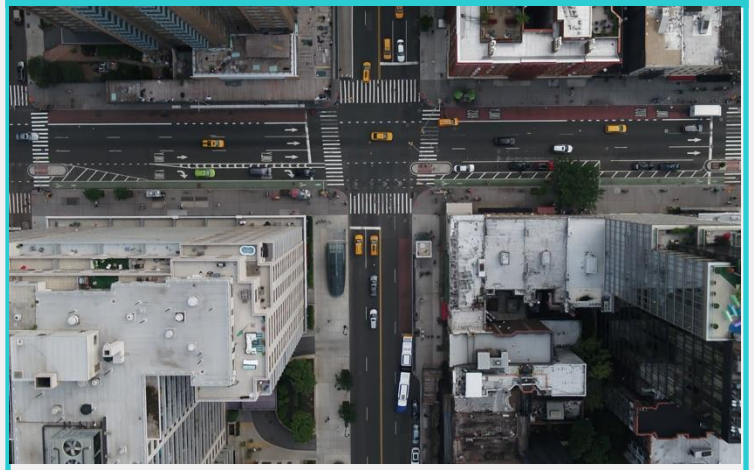


- Endpoint Detection & Response

SIEM

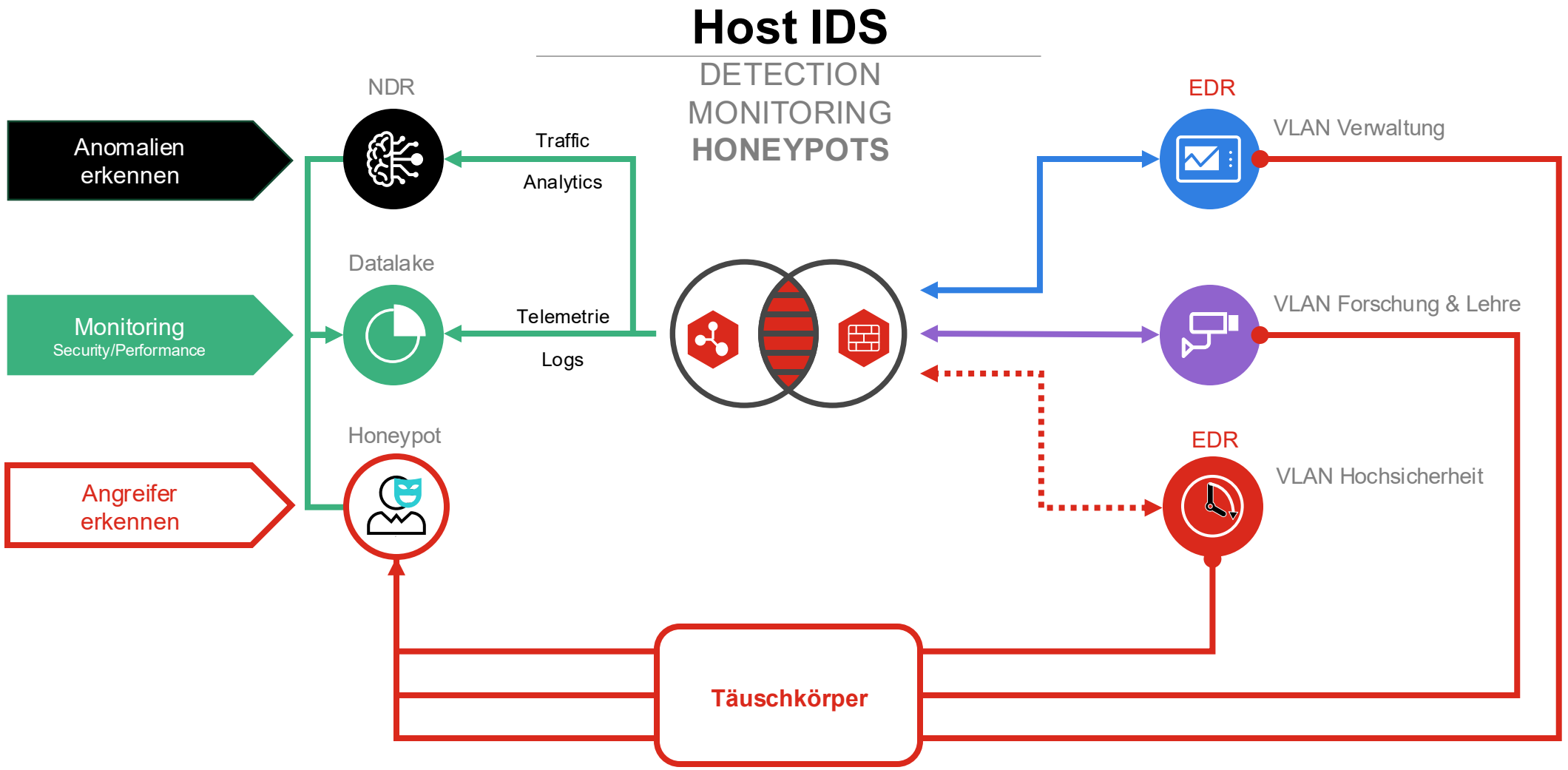
- Security Information & Event Management

NDR

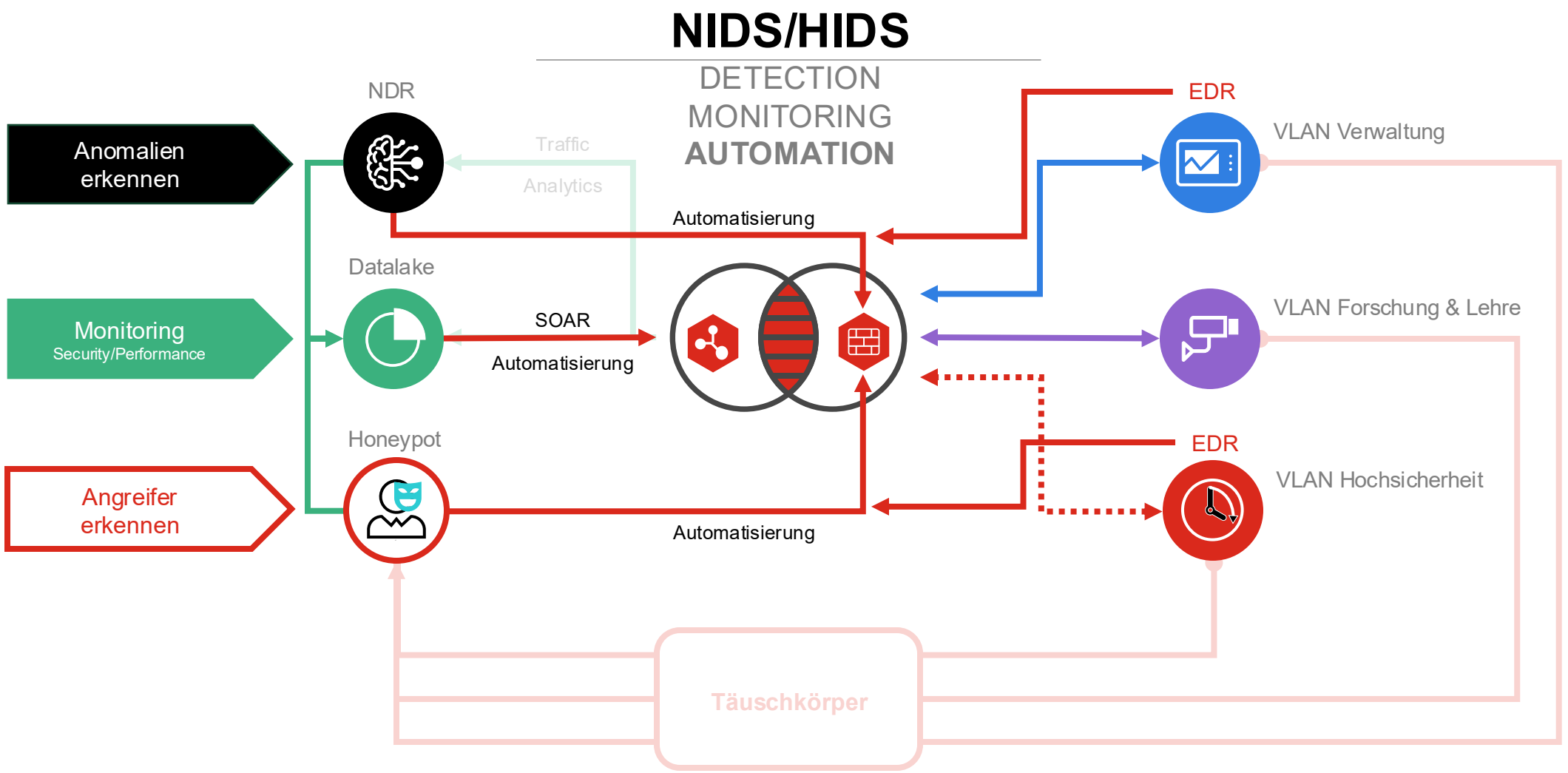


- Network Detection & Response

Technologisch: Täuschen

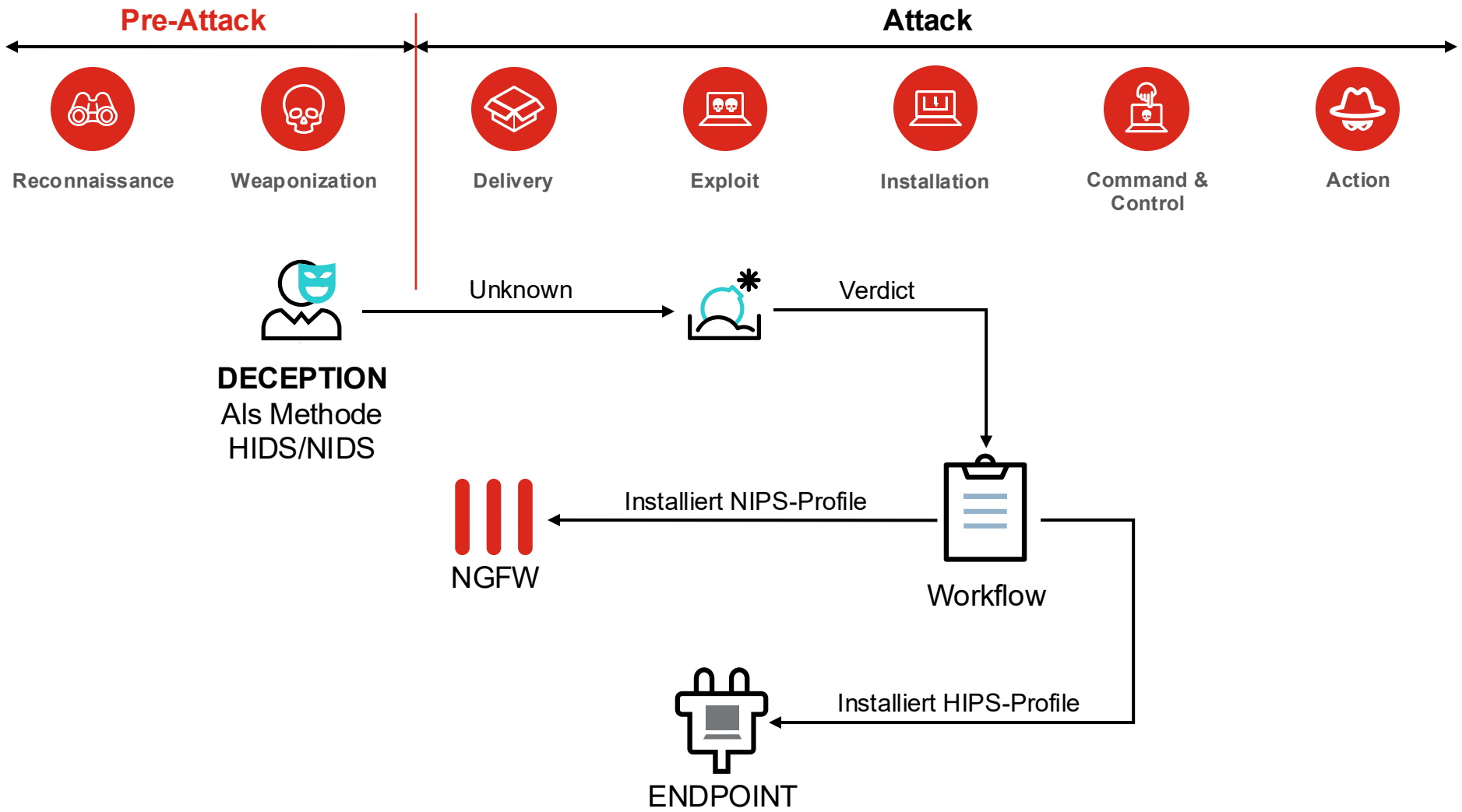


Cybernetics: Automatisieren



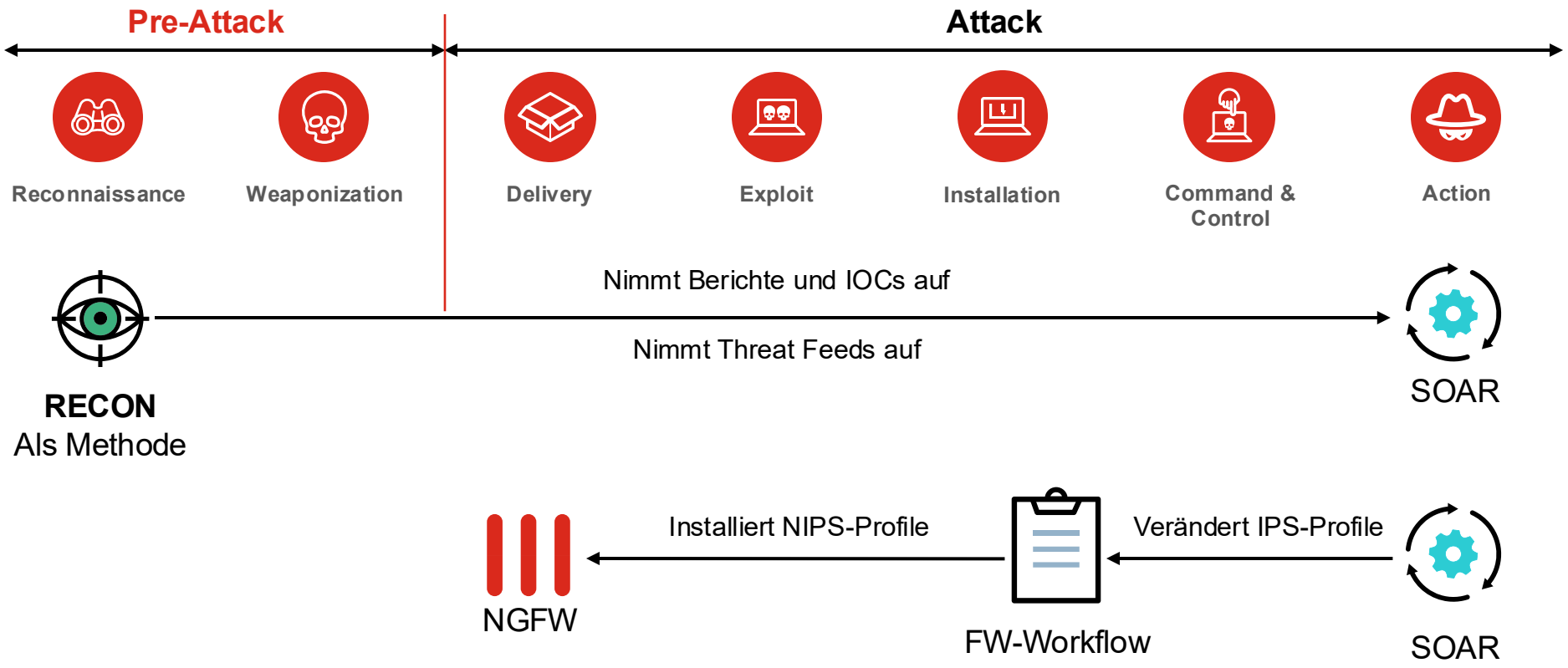
Shift Left

Erkennung verschieben



Shift Left: Cybernetics

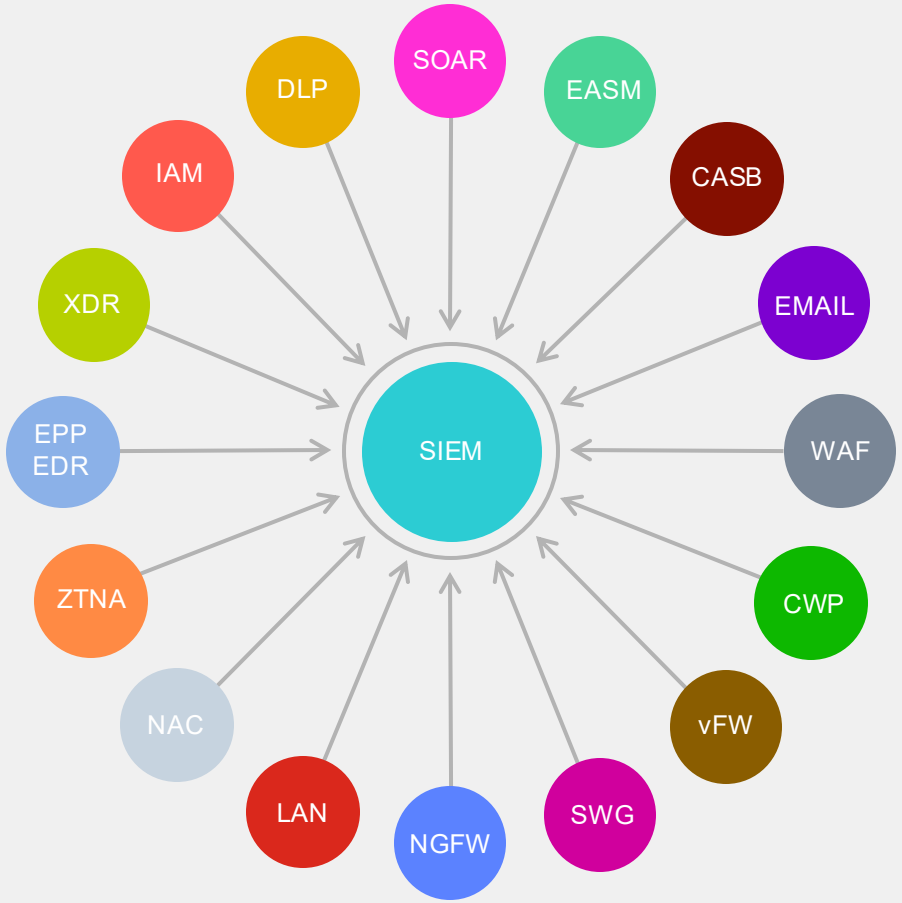
Wer sagt wem, was zu tun ist?



Consolidation of Security Point Product Vendors

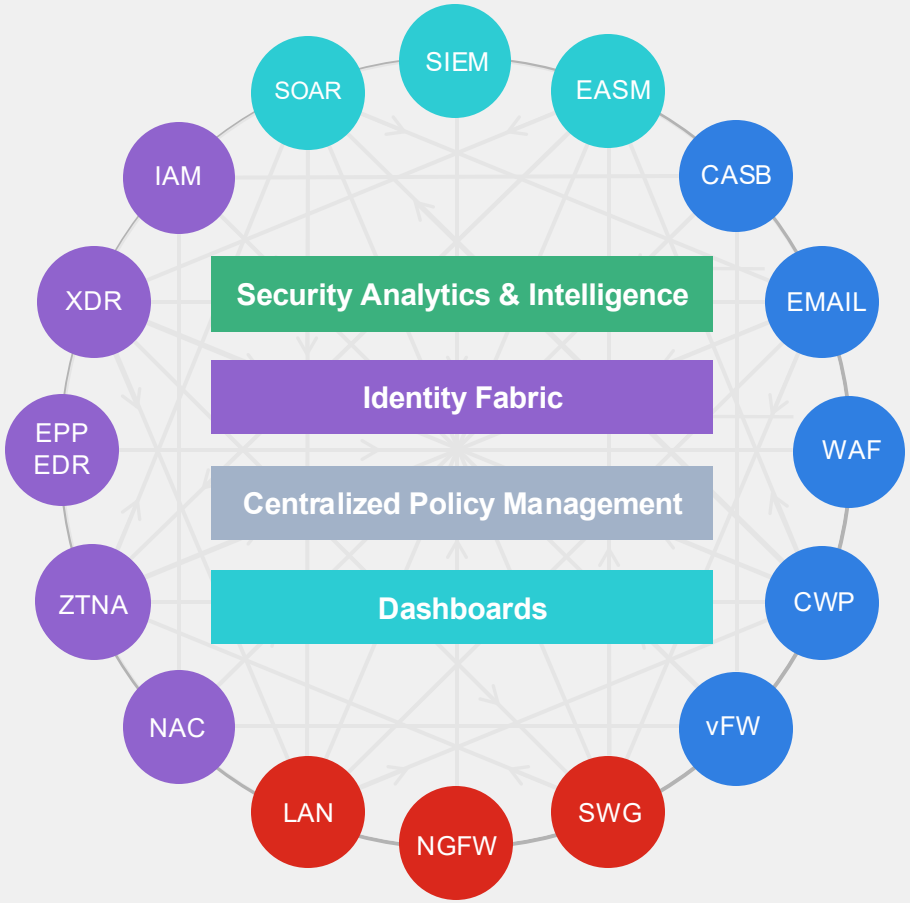
Gartner® Cybersecurity Mesh Architecture (CSMA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms

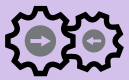
Open Ecosystem

500+ best-in-class integrated solutions for comprehensive protection

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

aws, aruba a Hewlett Packard Enterprise company, cisco, Google Cloud, IBM Cloud, Azure, ORACLE, servicenow, Symantec



Fabric APIs

Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

ARISTA, ASAVIE, DELL, DRAGOS, EQUINIX, intel, SIEMENS Ingenuity for life, splunk>, TIGERA, tufin

Fabric DevOps

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

aws, Google Cloud, HashiCorp, Azure, openstack, ORACLE, RED HAT ANSILE Tower, refactr, vmware

Extended Ecosystem

Integrations with threat sharing initiatives and other vendor technologies

CYBER THREAT ALLIANCE, MITRE, STIX, INTERPOL, OT CSA, Firewalls, Switching, Wireless, Endpoint Security

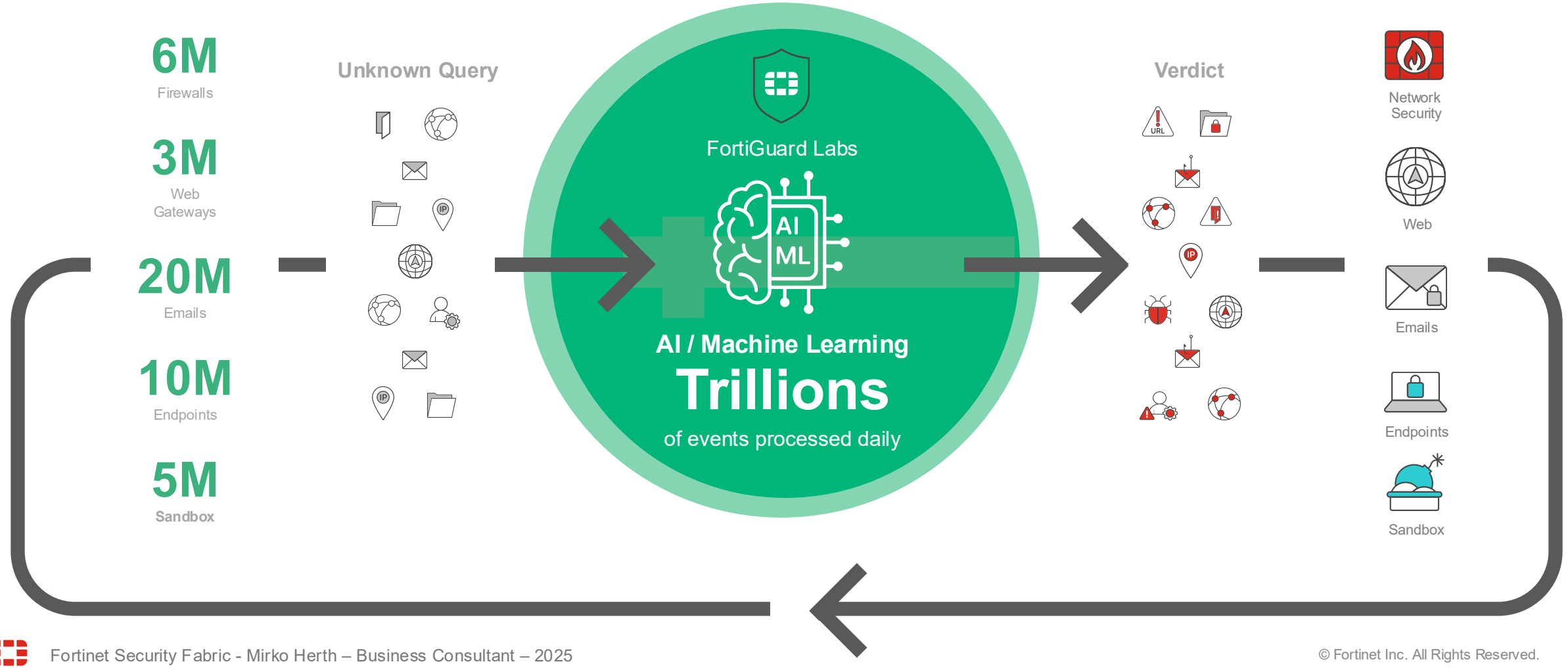
Figures as of March 31, 2021
Note: Logos are a representative subset of the Security Fabric Ecosystem

AI-Powered Security: FortiGuard

Broad Coverage
Telemetry across millions of Fortinet endpoints, networks and applications

Early Detection & Response

Broad Protection
across millions of Fortinet endpoints, networks and applications



Fortinet Security Fabric

Broad

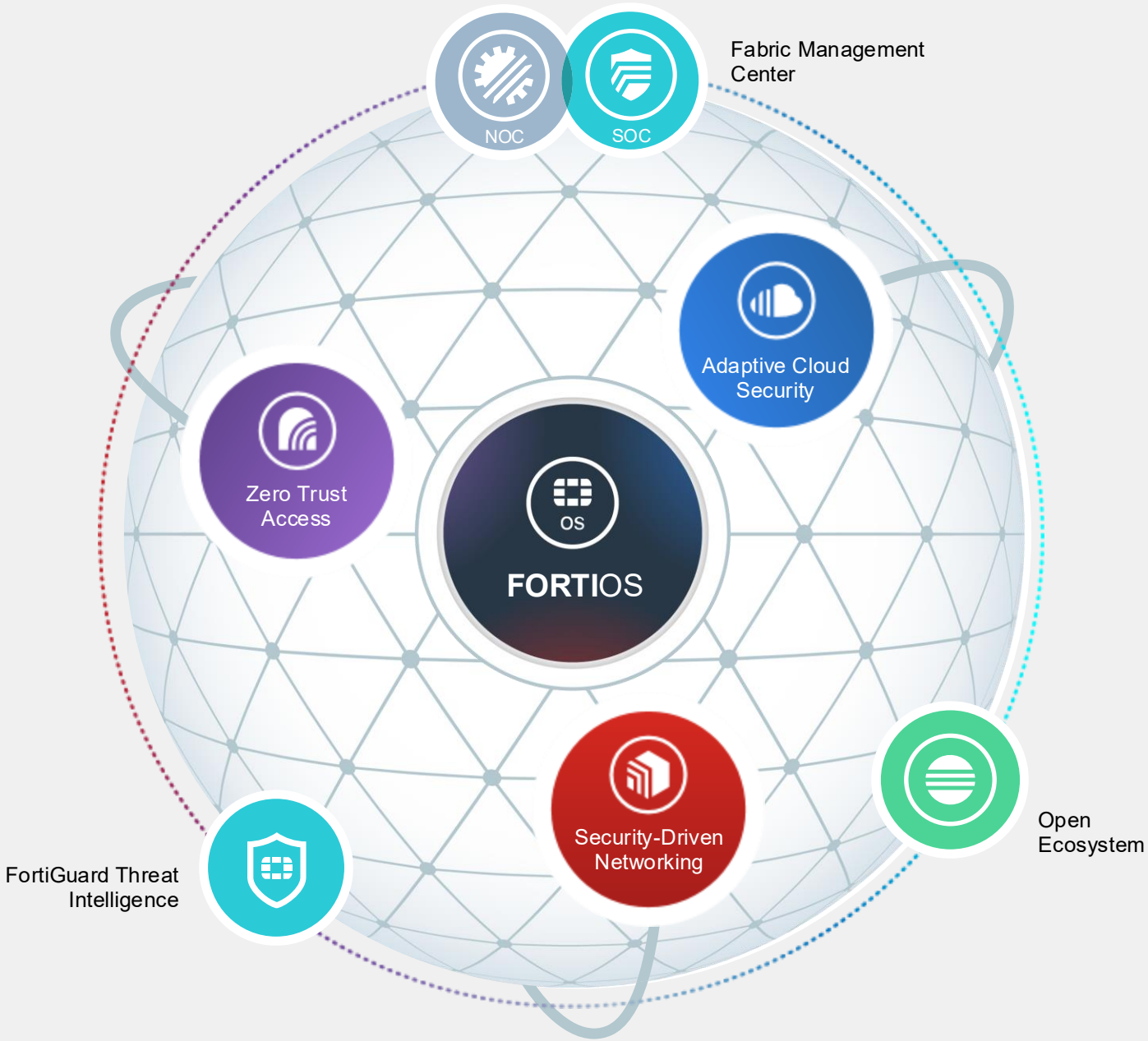
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

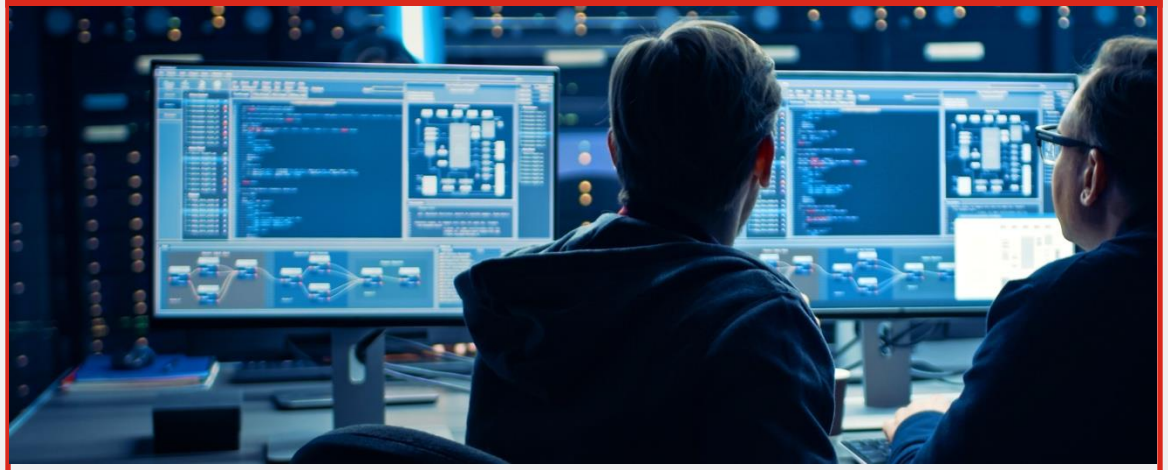
Automated

self-healing networks with AI-driven security for fast and efficient operations



Machine Learning & Künstliche Intelligenz

Analyse



- Analyse des Netzwerkverkehrs
- Analyse lokaler Prozesse
- Analyse von Taktiken
- Identifikation von Anomalien

Unterstützung

- Automatisierte Generierung von Sicherheitsregeln
- Anpassung von Sicherheitsregeln
- Optimierung der Sicherheitsrichtlinien
- Anpassung von Firewall-Regeln

AI at Fortinet

10+
Years Experience in AI/ML

6th
Generation of Machine Learning

59
AI Patents (Awarded & Pending)

100
Documented Applications of AI to Date

8
Number of Security Domains Utilizing AI

42
Number of Solutions Driven by AI Today

Mirko Herth

Business Consultant
mherth@fortinet.com


FORTINET