CNLAB Herbsttagung: „Real Life - Nicht nur IT Architektur“

Thomas Fröhlich, 9.9.2020

inventx
BANK ON IT

Agenda

1. Vom traditionellen eBanking zu vernetzten Applikationen
2. Hybride Ansätze
3. Kapselung von Docker-Anwendungen
4. Angreifer-zentrisches Bedrohungsmodell
5. Moderne Security-Operation

Vom traditionellen eBanking zu vernetzten Applikationen

- Die moderne, vernetzte und digitalisierte Welt fördert neue und schnell wachsende «Geschäftsmodelle» …
- Gleichzeitig floriert das lukrative Geschäft mit Cyberkriminalität und Erpressungen …
- Cyberkriminelle werden immer raffinierter und die Verfolgung immer komplexer bis unmöglich …
- Attacken nehmen drastisch zu und werden sehr gezielt, sowie immer anspruchsvoller vollzogen …
- Gezielte Angriffe auf Institutionen oder Personen werden gekonnt genutzt …

- Die Verschiebung vom reinen Perimeterschutz zum vollumfänglichen Datenschutz bedingt neue Strategien/Konzepte …
- Es genügt nicht mehr nach Mustern zu suchen, es müssen bereits kleinste Anomalien erkannt werden …
- Der Datenschutz und der damit verbunden Klassifizierung von Daten bekommt eine ganz neue Bedeutung …

ZeroTrust ist nicht nur IT Architektur und auch nicht schwarz/weiss

Neues RZ in Gais: Stretched Availability-Zone 1

Inventx ergänzt die Availability-Zone 1 mit einem 3. Datacenter in Gais (Region Ost) und schafft für Kunden neue, innovative Möglichkeiten in der Umsetzung ihrer Workload-Strategien.

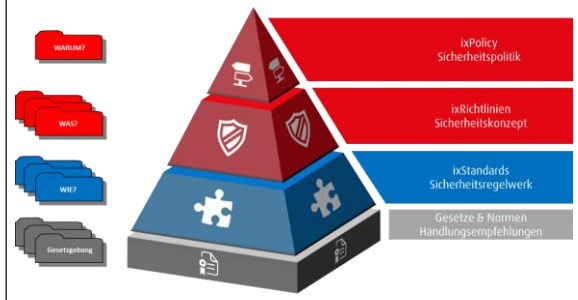
- **Nachhaltigkeit** – 25% höhere Energieeffizienz
- **Erfüllung gesetzlicher und regulatorischer Vorgaben** – Entspricht den Vorgaben der FINMA
- **99.995 %** – Uptime
- **1 x Tier 4[1] / 2 x Tier 3** – Zertifizierungs-Standards für die Rechenzentren
- **Kontrollierte Datenzugriffe** – Keine Datenzugriffe aus dem Ausland
- **< 30 km (Low Latency) > 70 km (Disaster Recovery)** – Distanz zwischen den RZ
- **Flexible Betriebsmodelle** – Lokaler, asynchroner oder synchroner Betrieb
- **Datenhaltung in der Schweiz** – Eigener RZ Verbund
- **ISAE 3402 Typ 2 ISO 27001 | 27017 | 27018** – Geprüfte Sicherheitsstandards

[1] Die offizielle Tier4-Zertifizierung durch Uptime-Institut wird per Ende Juni 2020 erwartet.

ISO Zertifizierungen & ISAE-Audit

Zertifizierungen/Prüfberichte

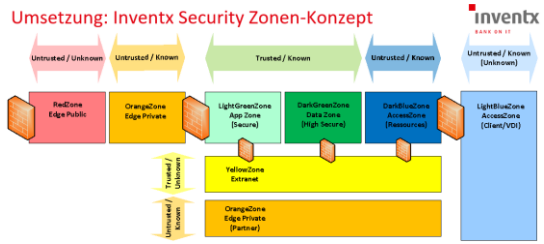
- **ISO 27001:2013** – Informationssicherheits-Managementsystem
- **ISO 27017:2015 und ISO 27018:2014** – Services und Datenschutz in der Cloud
- **ISAE 3402 Type 2 / finma Erläuterungsbericht** – Jährliche Prüfberichte durch PWC
- Alle ISO-Zertifizierungen werden über die gesamte Inventx mit allen Prozessen und über alle Controls durchgeführt

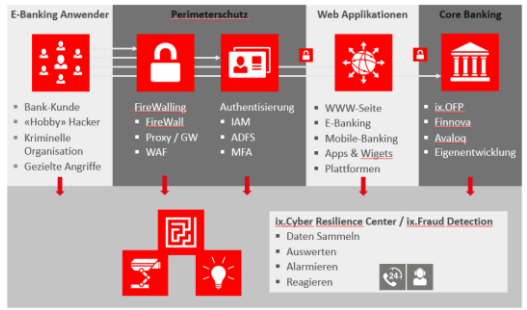


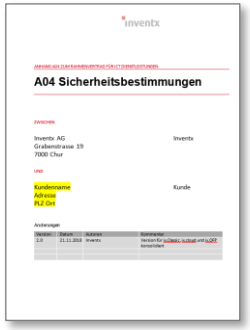
Einhaltung von gesetzlichen Grundlagen

- Bundesgesetz über den schweizerischen Datenschutz (DSG)
- Verordnung zum Datenschutzgesetz (VDSG)
- EU-Datenschutz-Grundverordnung (EU-DSGVO / GDPR - Inkraftsetzung neuer GV per 25. Mai 2018)
- Strafgesetzbuch (StGB)
- Bankengesetz (BankG)
- Urheberrechtsgesetz (URG)
- Obligationenrecht (OR - insbesondere Verträge mit Dritten, Arbeitsverträge, Kaufmännische Buchführung)
- Verordnung über die Führung und Aufbewahrung von Geschäftsbüchern (GeBüV)

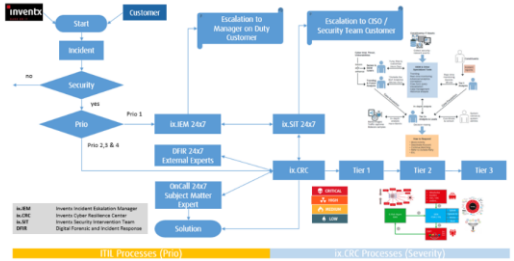
Umsetzung: Inventx Security Zonen-Konzept







Security Incident Management Prozess

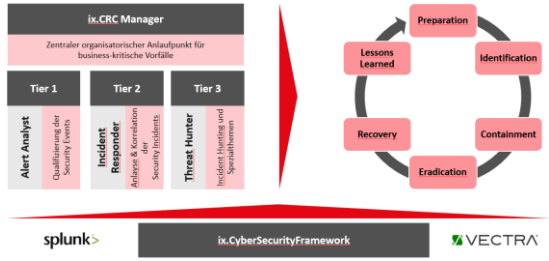


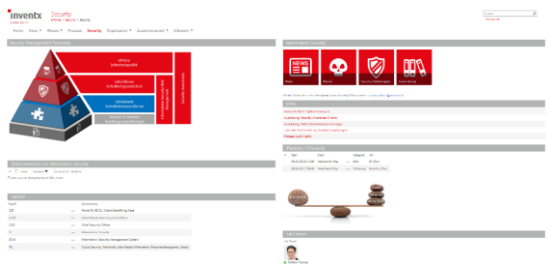
Einhaltung Aufsichtsrecht

- FINMA Rundschreiben 2018/03 "Outsourcing – Banken und Versicherer" (Inkraftsetzung per 1. April 2018)
- FINMA Rundschreiben 2008/21 Operationelle Risiken Banken
- FINMA Rundschreiben 2017/02 "Corporate Governance Versicherer" (Inkraftsetzung per 1. Januar 2017)
- FINMA Rundschreiben 2013/8 Marktverhaltensregeln
- FINMA Guidance 05/2020 -> Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA

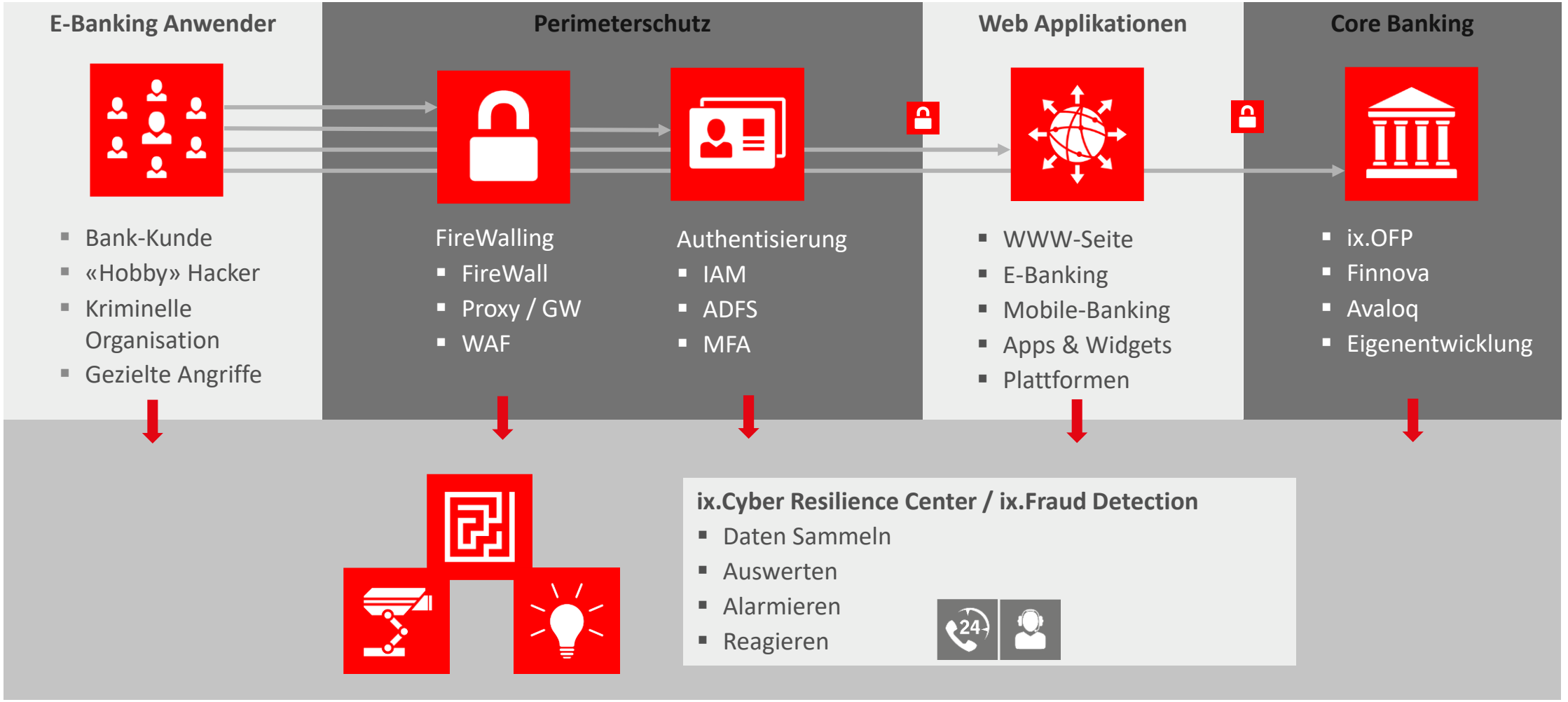
finma

ix.CRC: People, Prozesse & Technologie





Philosophie | Offene Zonen Architektur



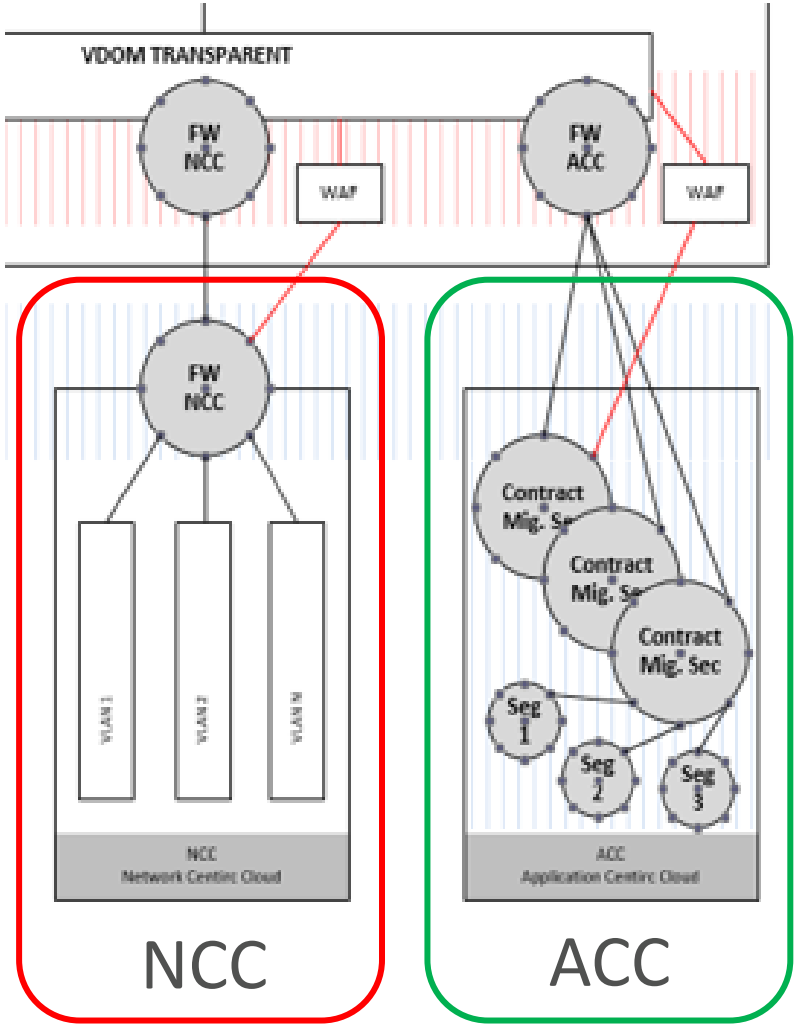
Vom Netzwerk Zonenkonzept zur Microsegmentierung

Network Centric Security oder Network Centric Cloud (NCC)

- Traditionelle Separierung von Security Zonen (Netzwerken) auf 2. FW Stufe
- Komplexes zentrales Regelwerk
- Zone = Subnetz = VLAN; Gateway (Routing) auf Firewall

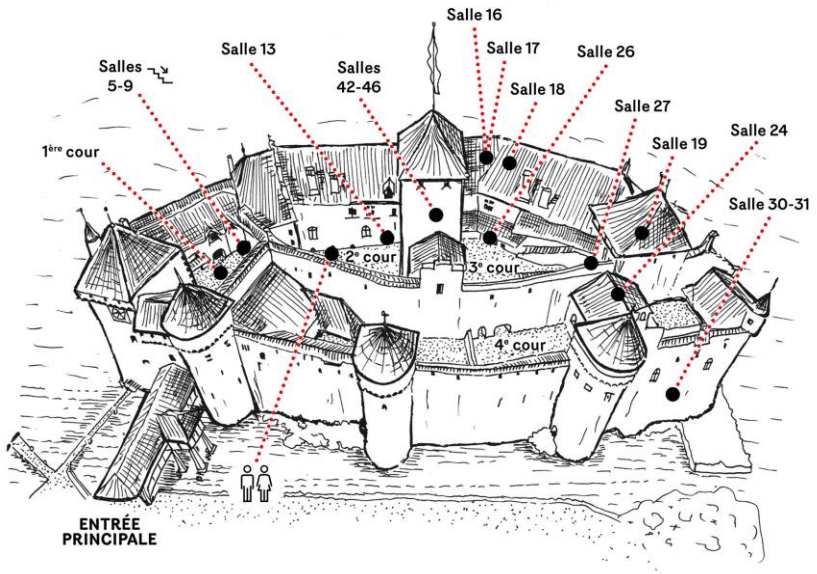
Data Centric Security oder Application Centric Cloud (ACC)

- Separierung von logischen Gruppen (Applikationselementen) mittels z.B. Cisco ACI Contracts
- Microsegmentation anhand von Attributen (IP Adressen, VM tags, OS, etc.)



Perimeter-Security zu Microsegmentierung

Perimeter Security



Security Zonen
Network Centric

Microsementation
Data Centric

Was bringt Microsegmentierung?

- …sehr effektiver Ansatz, um unbefugte seitliche Bewegungen (Ost-West) zu verhindern
- …zentralen Grundsatz eines Zero Trust-Frameworks
- …Schlüsselverteidigung zur Reduzierung der Angriffsfläche
- …ein Netzwerk auf einen einzelnen Host segmentieren
- …und somit die Angriffsfläche auf einen einzelnen Host verkleinern/isolieren

Schritte der Microsegmentierung:

- Network-Based
- Hypervisor-Based
- Host-Based
- Data/Application-Based

Microsegmentierung in der Praxis

- Microsegmentierung auf dem darunterliegenden Netzwerk kann helfen (z.B. mit CISCO ACI)
- Dockerisierung z.B. mit Kubernetes oder OpenShift bietet Microsegmentierung
- Virtuelle Clients inkl EDR (Endpoint Detection and Response) z.B. mit Citrix- oder Azure-Ansätzen

Herausforderungen:

- Kubernetes Cluster pro Umgebung und Kunde? -> Kosten / Risiken / Machbarkeit?
- Zusätzlicher Security Layer unter anderem für das Managen und eine aktiven Überwachung (z.B. Aqua, StackRox…) innerhalb Kubernetes
- Entwickler und standardisierte virtuelle Clients/Desktop sind meist nicht kompatibel…
- Architektur und damit verbundene Risiken müssen ganzheitlich (inkl. Containern) bekannt und dokumentiert sein

Ist Security Architektur einfach ein zusätzlicher Layer?

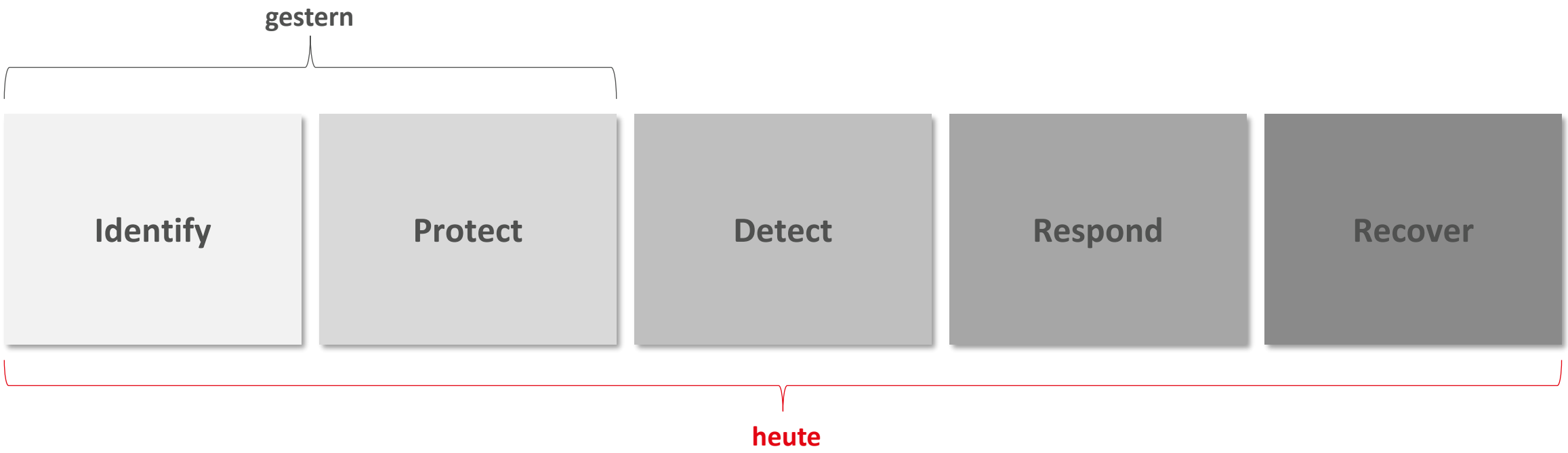
- Security Architekturen hin zu Zero Trust ist nicht etwas, das einer existierenden IT Architektur zugefügt werden kann, um Versäumnisse oder Mängel zu beseitigen
- **Nein, im Gegenteil**, es geht darum, dass der Sicherheits-Fokus ganz klar in jedem Design und der Entwicklung miteinbezogen wird, so unter anderem:
  - Netzwerk und Infrastruktur
  - Endpunkte (alles was eine IP hat)
  - Applikationen
  - Cloud: «MultiCloud is the new DataCenter»
- … ein «overall plan», wie Security in jedem Layer mit **Technologie, Prozessen und Menschen** ideal umgesetzt wird

Microsegmentierung löst nicht alles, was braucht es sonst noch?

- Verständnis für Infrastruktur-, Netzwerk-, Applikations-, Informations- und Business-Architekturen… und wie jeder dieser Layer mit Risiken beeinflusst wird
  - **Think Red:** Welche Bedrohungen (Threats) können Auswirkungen haben? -> **Attacker Centric**
  - **Act Blue:** Welche architektonischen Design und Technologien helfen, sich gegen diese Bedrohungen zu schützen/verteidigen?
- Geschäftliche und technische Kommunikation/Anforderungen müssen in Einklang sein
- Klare strategische und taktische Vision, ein roter Faden nach **Assume Breach & ZeroTrust**

Wo stehen Sie?

NIST Cyber Security Framework



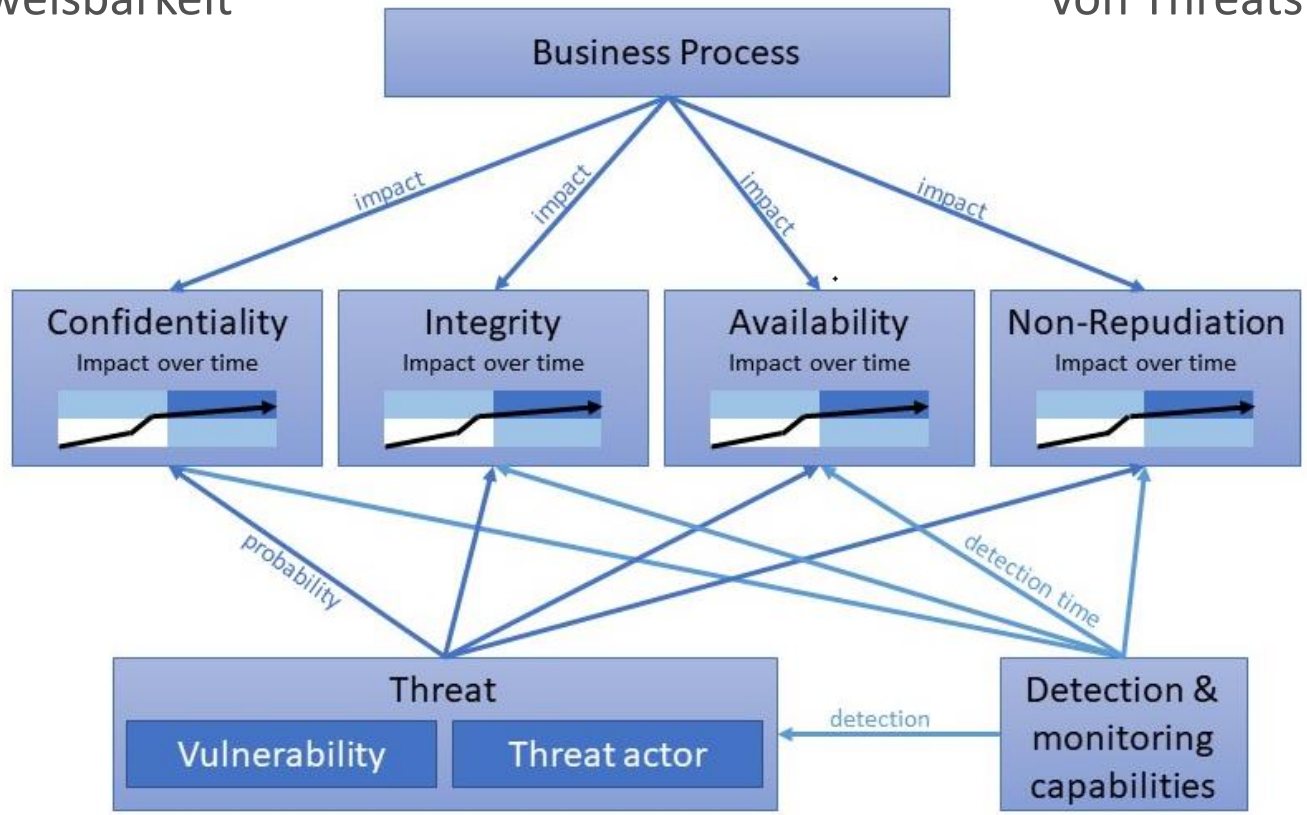
Zusätzlich zum klassischen Schutz[1] müssen Angreifer aufgespürt werden, denen es gelungen ist, in die Technologie-Plattform einzubrechen!

[1] Firewalls, Vulnerability-Scans, Malware-Protection etc.

Why threats and threat actors matters…

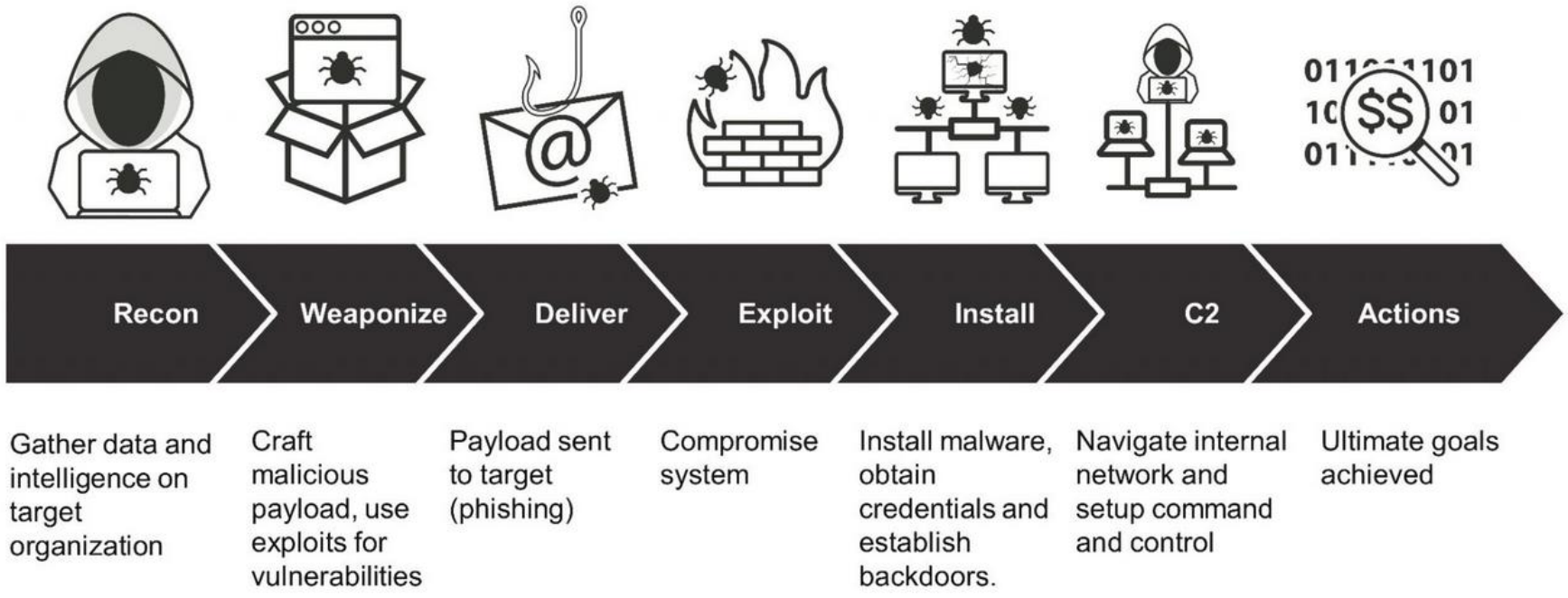
Threat-Actors nutzen **Schwachstellen** aus und gefährden Vertraulichkeit, Verfügbarkeit, Integrität und Nachweisbarkeit

Regelmässiges **«Threat modelling»** als Grundlage für **«Detections»** zur Erkennung von Threats



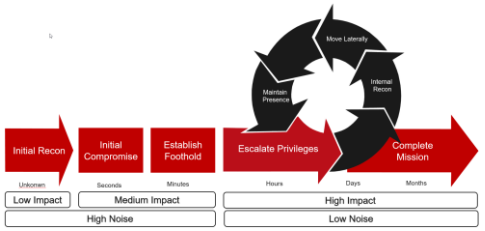
Kenne die Absicht deiner Angreifer!!

Core- Detections | Cyber Kill Chain – Threat Actor Activities

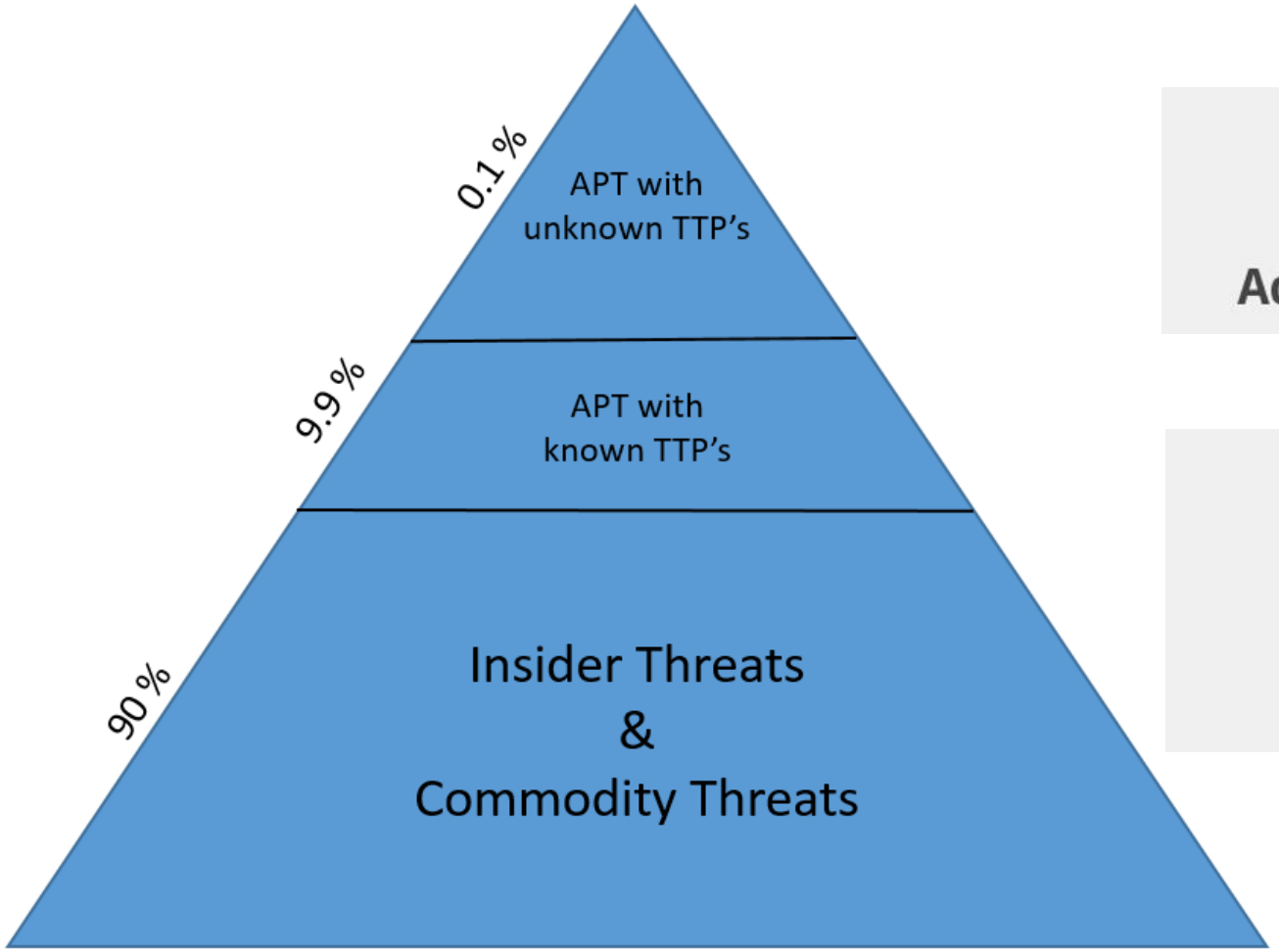


Attacker Centrics Threat modeling

- Detections definition im Abgleich mit Lockheed Martins «cyber kill chain»
- CoreDetections mit vordefinierten use cases
- Detections based im Netzwerkverkehr und Netzwerk Log-Analysen



Wahrscheinlichkeit von Angriffen | Pyramid of Pain



APT

stands for

Advanced Persistent Threat

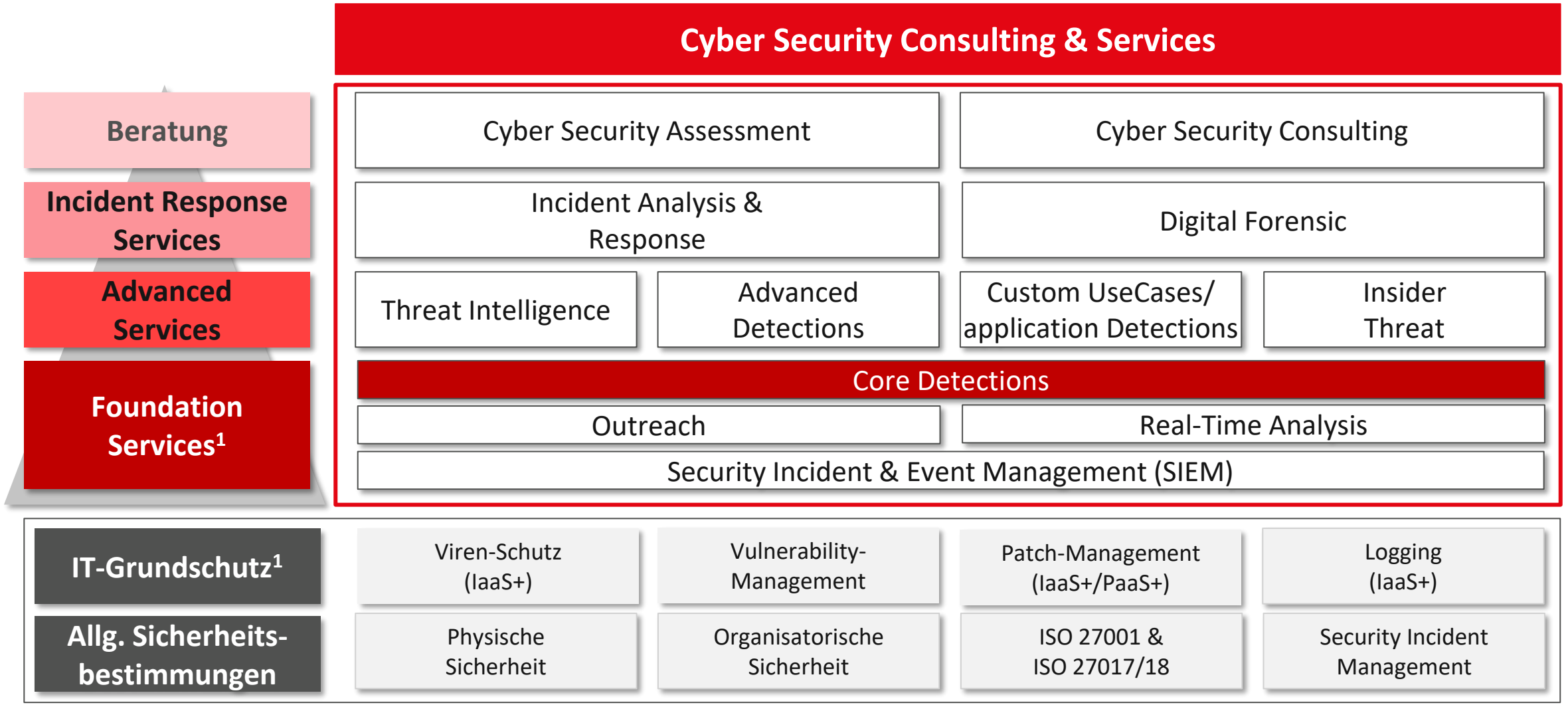
TTP

stands for

Tactics Techniques and Procedures

SOC: Mögliches/typisches Portfolio

IX.CyberResilienceCenter



[1] Nur im Package/Bundle verfügbar

Denkanstösse zum Mitnehmen…

- Haben wir die Flexibilität für Zero Trust Ansätze und ist die Architektur vorbereitet?
- Perimeter Security (wenige Zonen) -> Assume Breach (Microsegmentation)

- Wurde eine Cyber Philosophie etabliert und verinnerlicht?
- Risk based -> Kill Chain -> Attacker Centrics Threat modeling (wer ist der Angreifer -> Mensch)
- Risikominimierung durch aktives Security Operation z.B. durch Cyber Analysten in einem SOC

- Gute Zusammenfassung: Defensible Network Architecture 2.0 nach Richard Bejtlich
  - Überwachen, inventarisieren, kontrollieren (ingress und egress filtering), klarer System Owner, minimalisiert (attack surface), bewertet (Vulnerabilty Mgmt), aktuell (patched)

Inventx AG

Besten Dank für Dein Interesse. Bei Fragen stehen wir Dir jederzeit gerne zur Verfügung.

Thomas Fröhlich
Senior Security Solution Architect
thomas.froehlich@inventx.ch
T +41 81 287 1737

Ein Unternehmen der Esentica Holding.