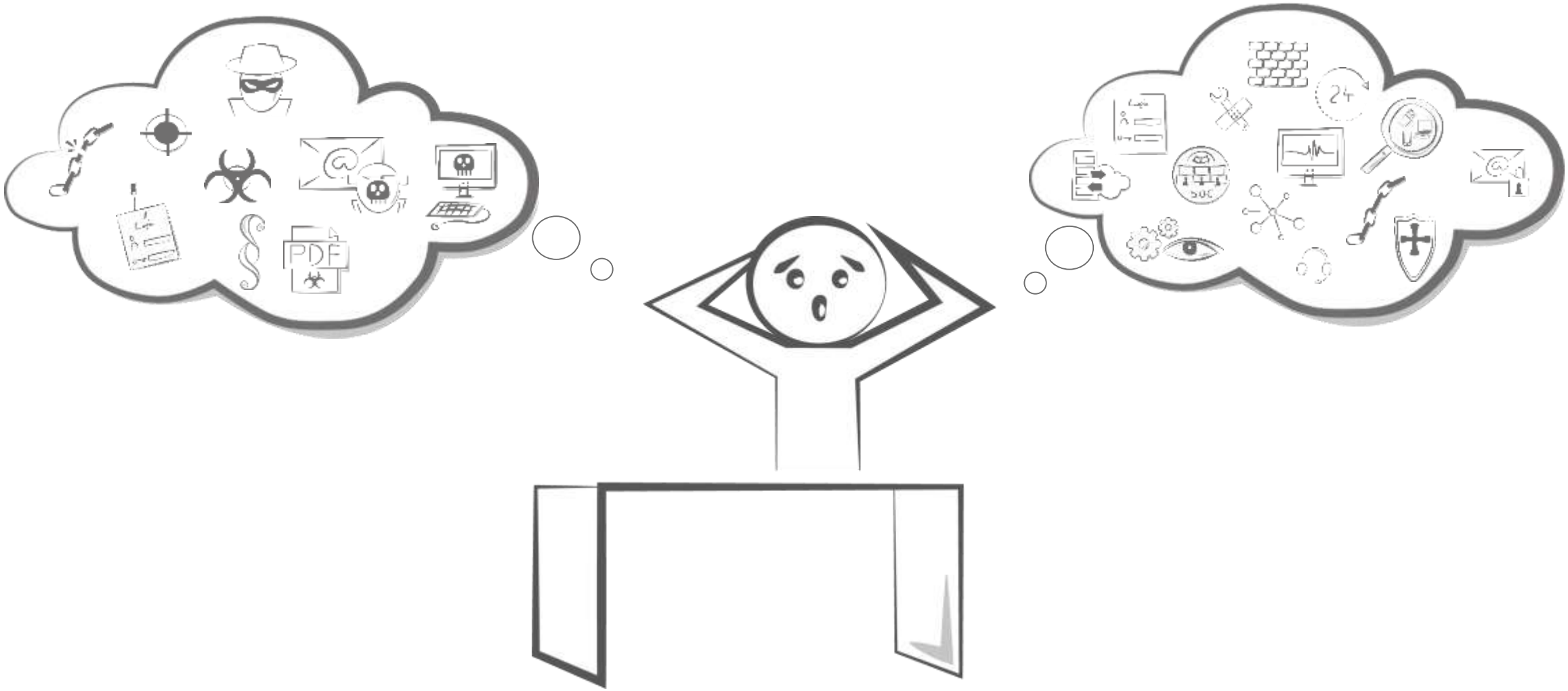
Aktuelle Cyber Security Herausforderungen

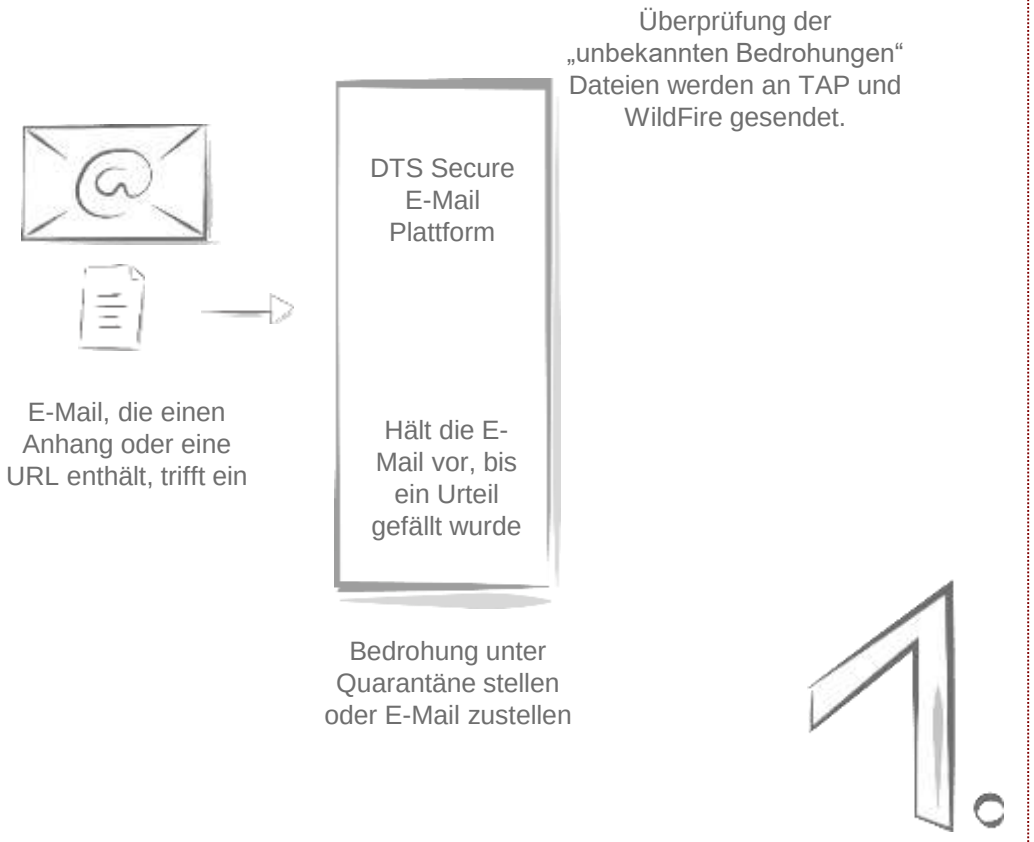
Jonas Schiffer & Timo Schulz

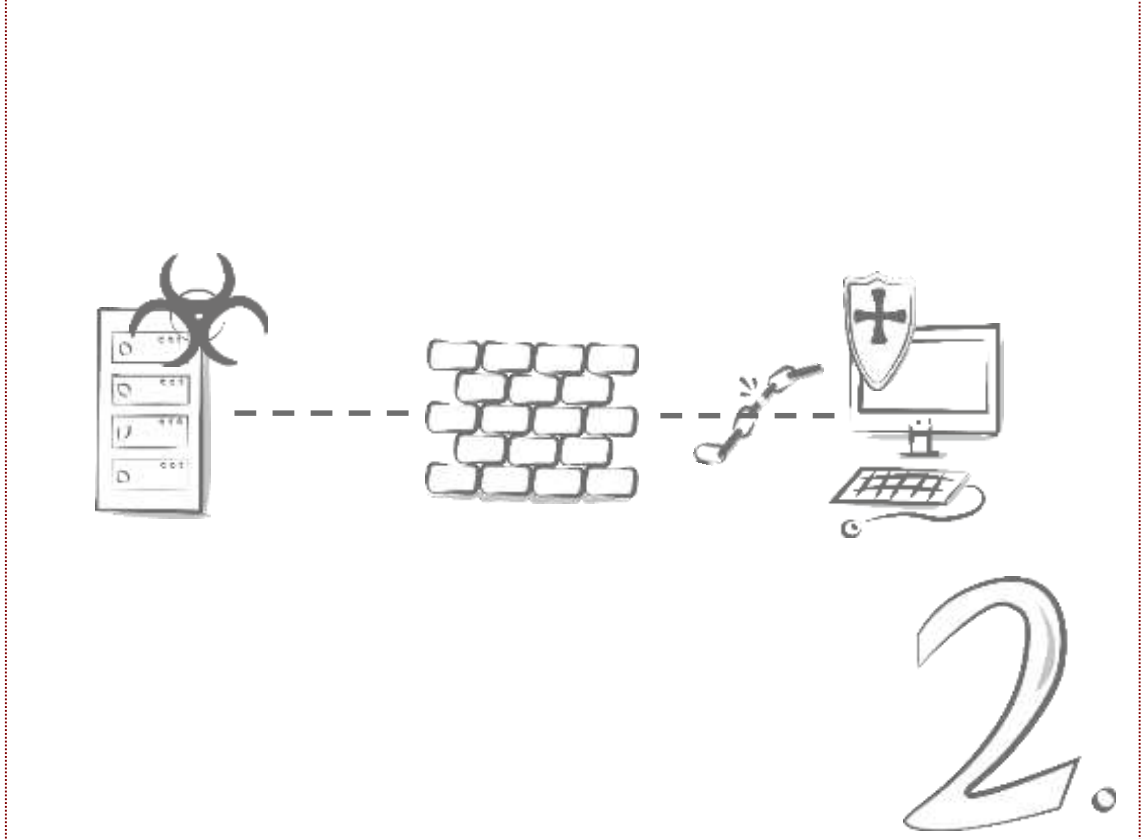
Produkte als Silos



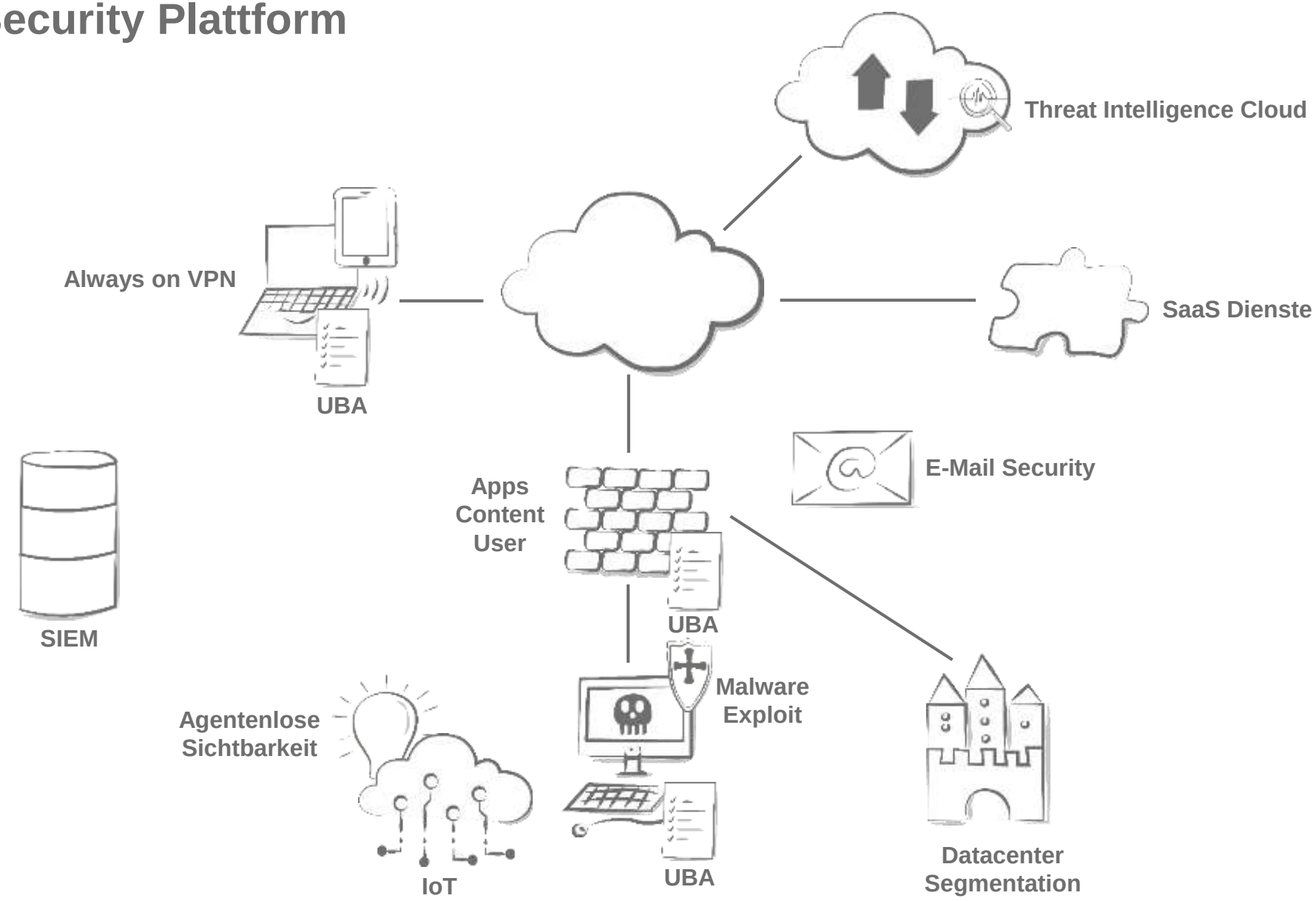
Use Cases

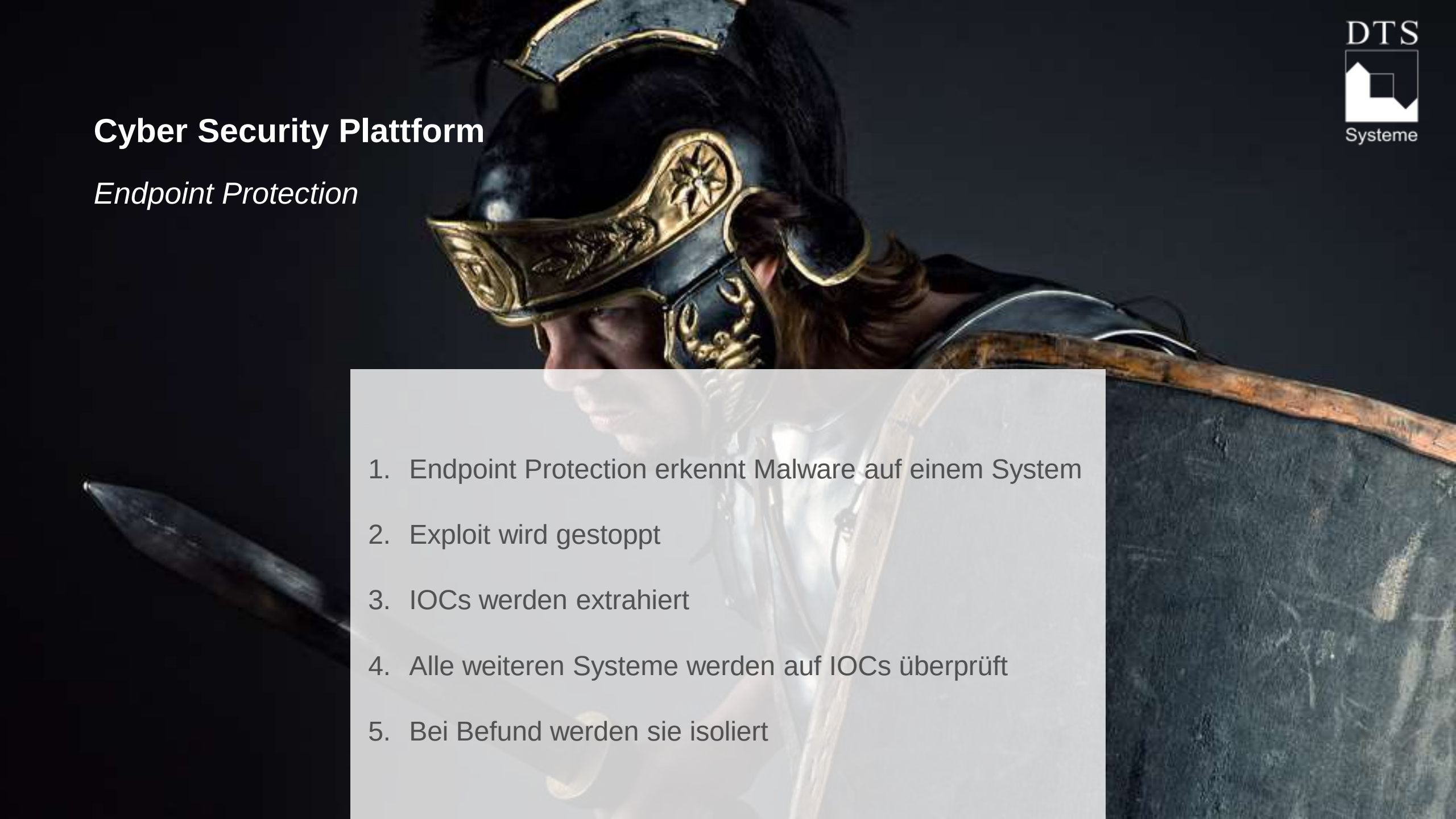
E-Mail Security, Endpoint Protection





Cyber Security Plattform





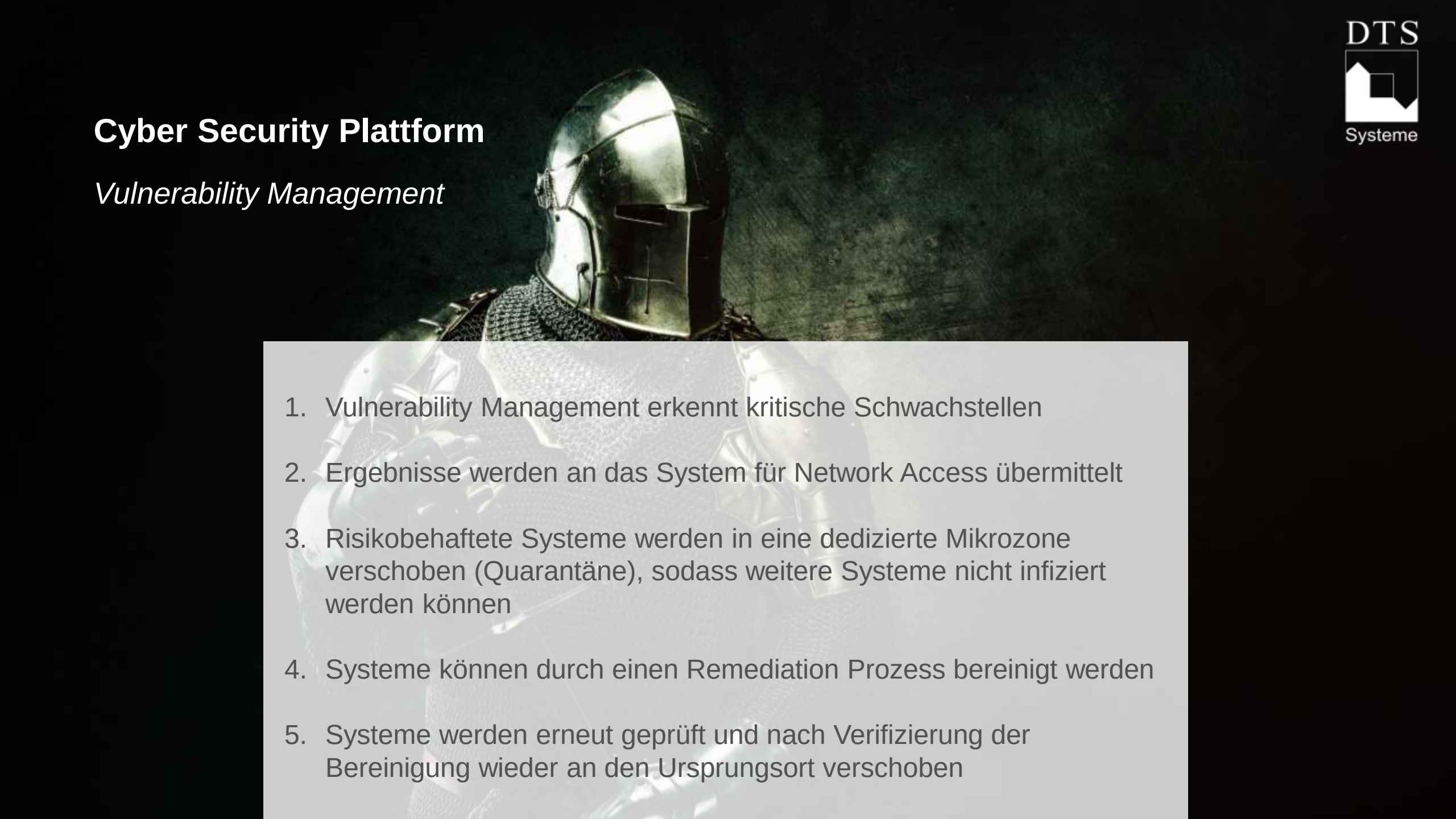
Cyber Security Plattform

Endpoint Protection

1. Endpoint Protection erkennt Malware auf einem System
2. Exploit wird gestoppt
3. IOCs werden extrahiert
4. Alle weiteren Systeme werden auf IOCs überprüft
5. Bei Befund werden sie isoliert

Cyber Security Plattform

Vulnerability Management



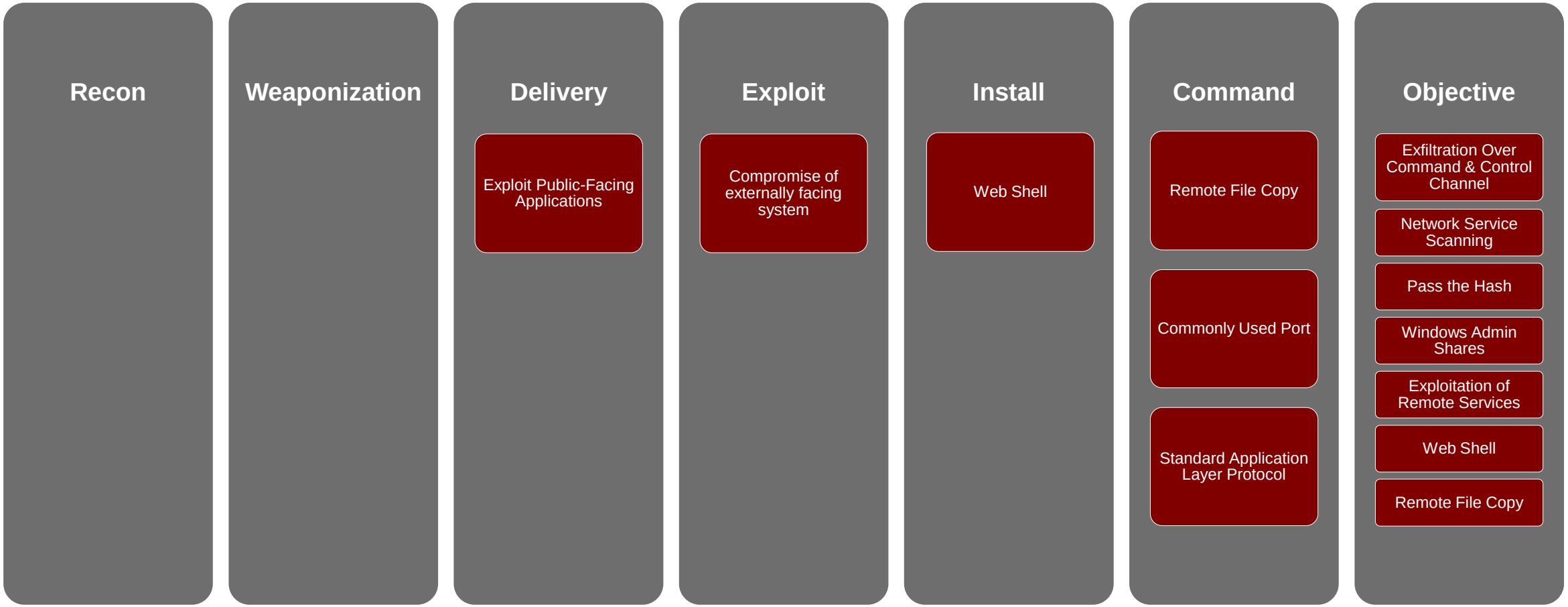
1. Vulnerability Management erkennt kritische Schwachstellen
2. Ergebnisse werden an das System für Network Access übermittelt
3. Risikobehaftete Systeme werden in eine dedizierte Mikrozone verschoben (Quarantäne), sodass weitere Systeme nicht infiziert werden können
4. Systeme können durch einen Remediation Prozess bereinigt werden
5. Systeme werden erneut geprüft und nach Verifizierung der Bereinigung wieder an den Ursprungsort verschoben

Cyber Security Plattform

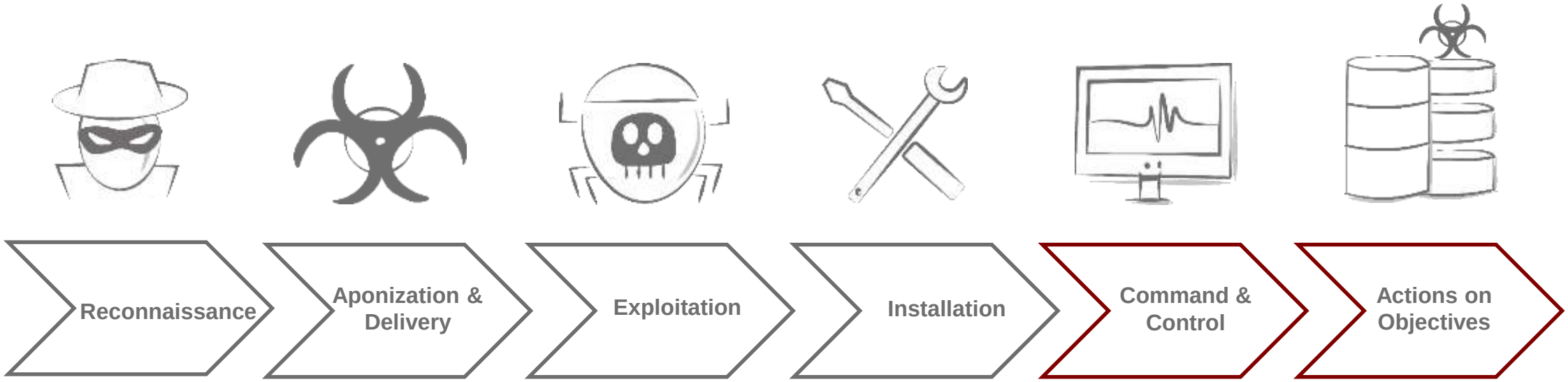
User Behavior Analysis

1. Endpoint & Netzwerk Logs werden korreliert
2. Aus den erhobenen Daten entsteht eine Baseline
3. User greift plötzlich auf Daten abseits seines Zuständigkeitsbereichs zu
4. User startet unverhältnismäßig große Uploads nach extern
5. Kommunikation zum Internet wird durch eine Firewall unterbunden
6. Client wird Isoliert durch die Endpoint Protection
7. Investigation wird durch die Security Analysten eingeleitet

Emissary Panda

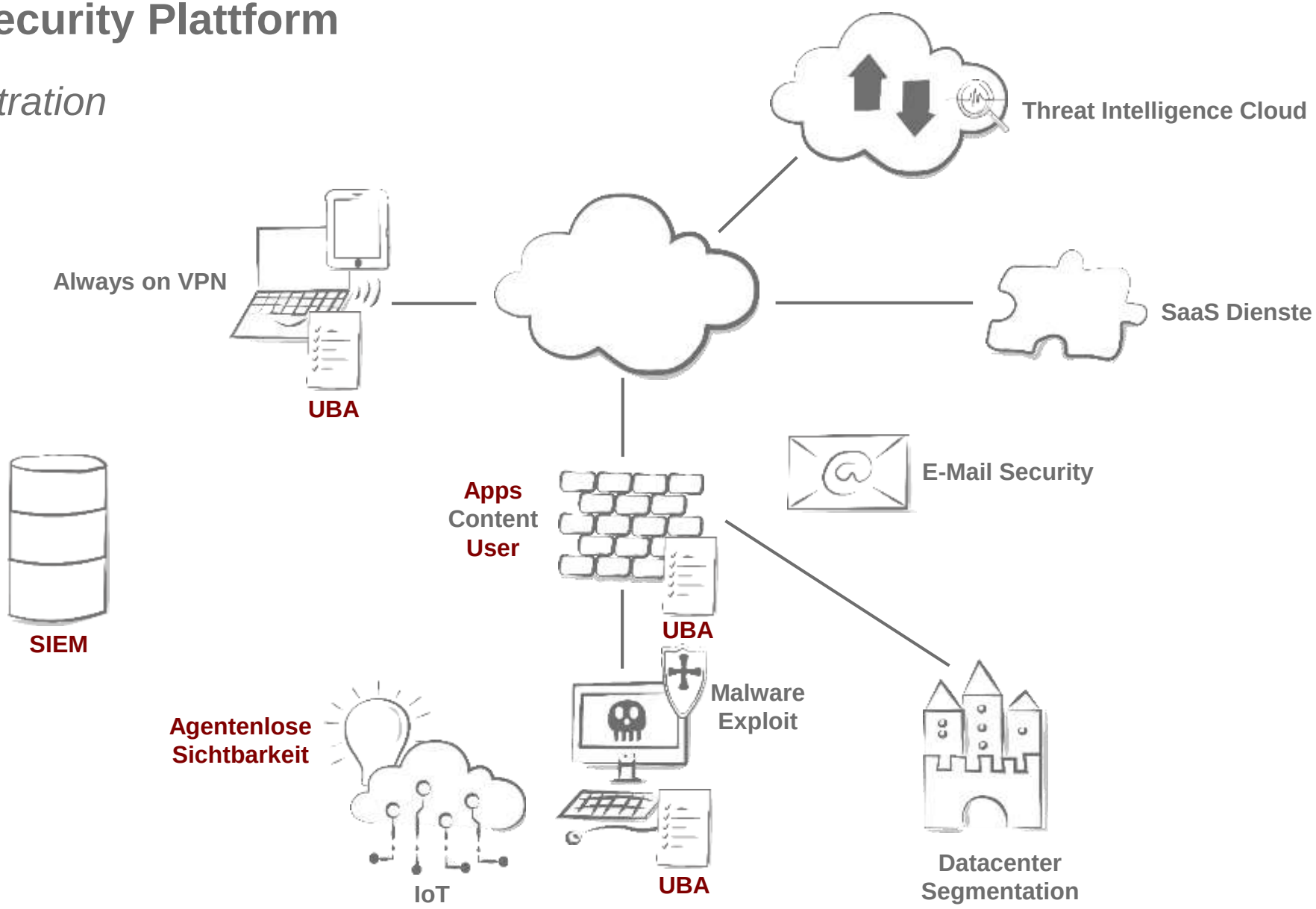


Cyber Attack Lifecycle



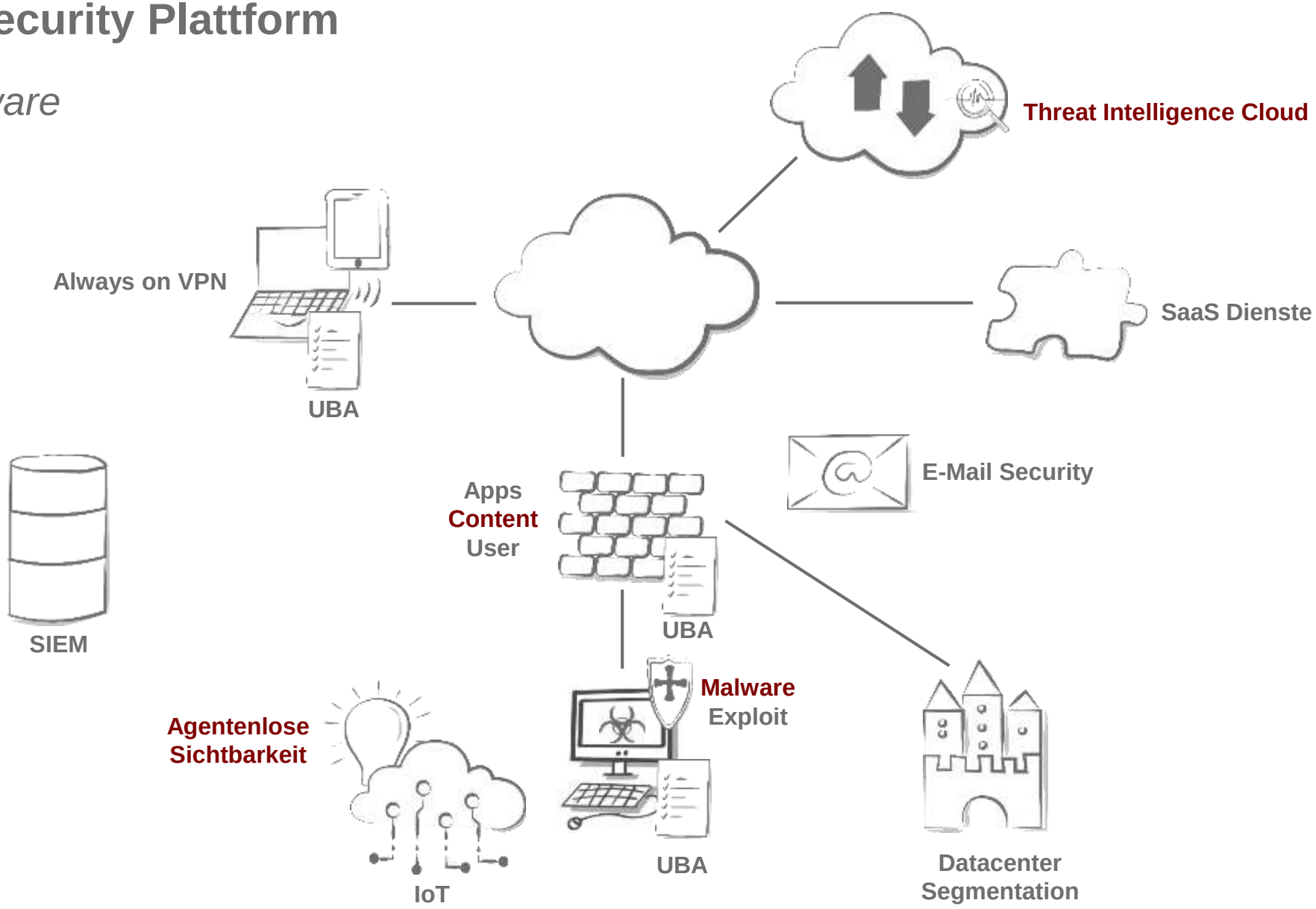
Cyber Security Plattform

Data Exfiltration



Cyber Security Plattform

Ransomware




DTS
Systeme
DTS Security Operations Center (SOC)

Sind Sie ausreichend abgesichert?

Und erstens kommt es anders….

Reporter: *„Auch Nashorn Babys sind nicht ungefährlich“*

… und zweitens als man denkt

Quelle: !VARA
Referenz: Linux Neuman, CCC

Wie sieht die Lösung aus?

Alle externen Kommunikationswege blockieren?

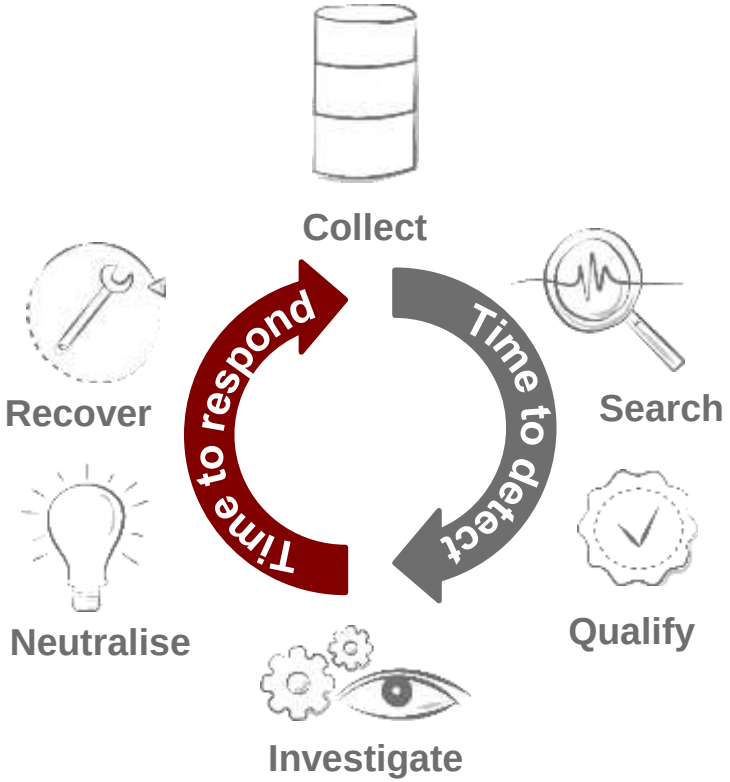
-> Leider Nein

Wie sieht die Lösung aus?

2.

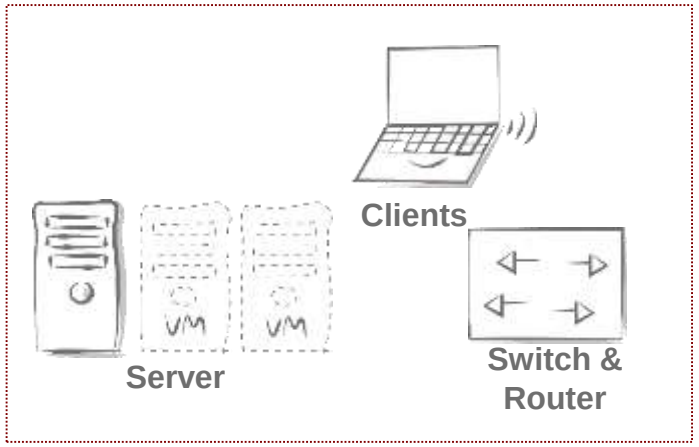
Welche anderen Möglichkeiten gibt es?

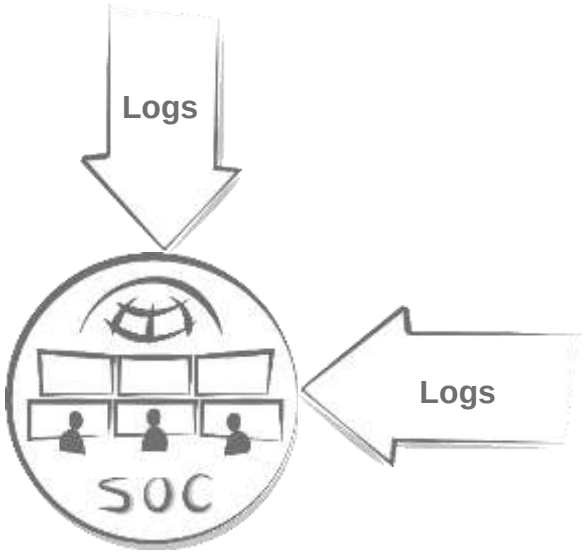
-> Zeit des Befundes sowie die Zeit der Gegenmaßnahmen möglichst gering halten

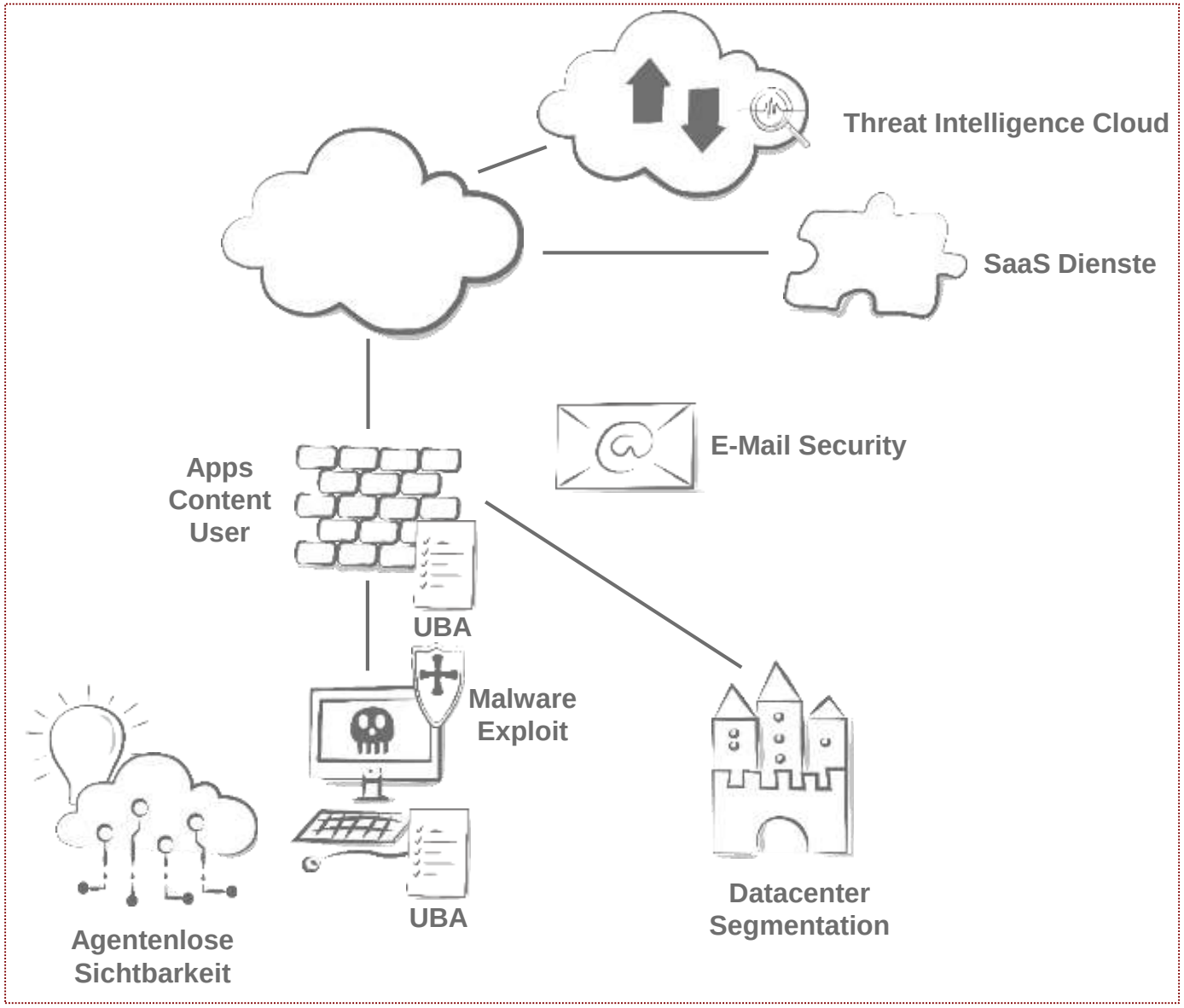


1. Sammeln von Log-Daten
2. Durchsuchen der Log-Daten
3. Anomalien erkennen / Threats ausfindig machen
4. Auswirkung auf IT-Landschaft bewerten / feststellen
5. Passende Gegenmaßnahmen einleiten
6. Betroffene Systeme / User wiederherstellen

Cyber Security Plattform - Erweitert

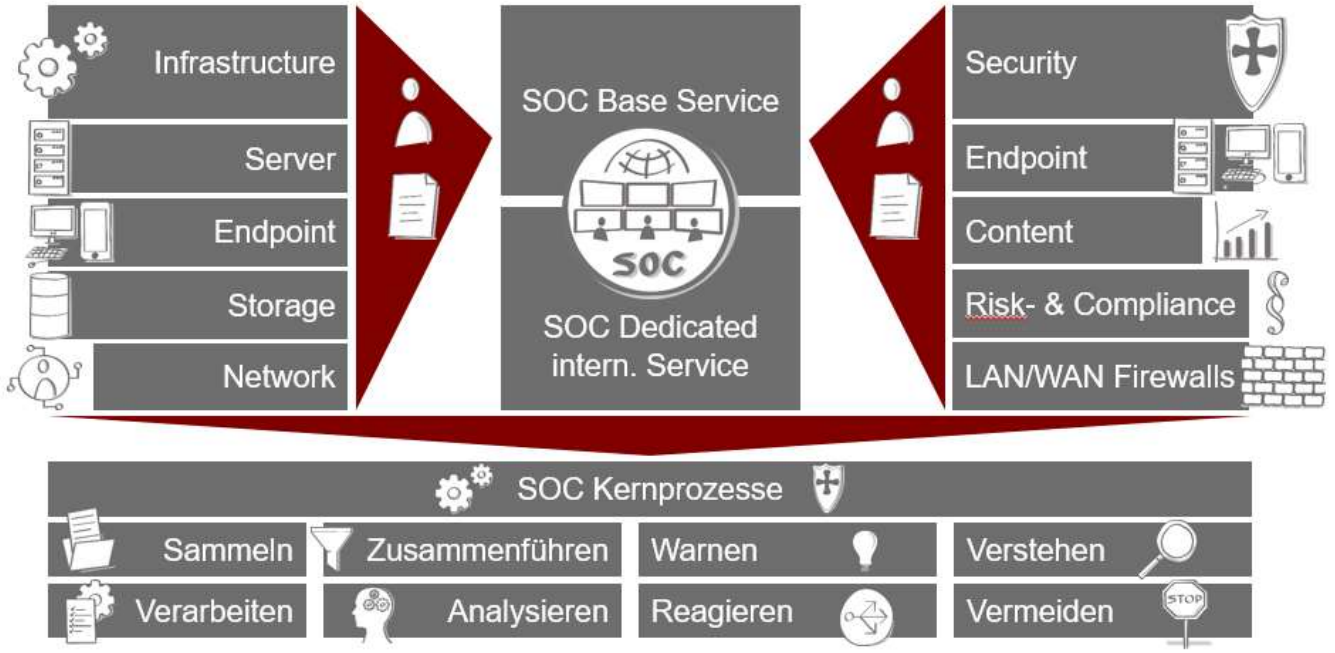






DTS Security Operations Center (SOC)

- Zentrale Sicherheitsleitstelle zum Schutz von IT-Infrastruktur und Daten
- 24/7 Schichtbetrieb
- Analyse **aller** Log-Nachrichten (Forensische Analyse) aus den Bereichen *„Infrastructure“* & *„Security“*
- Proaktive/präventive Suche nach Schwachstellen und Angriffsreaktion (Erkennung von Anomalien)
- Alarmierung & Einleitung von Abwehrmaßnahmen




DTS
Systeme
Offene Fragen?
Besuchen Sie uns gerne in
Halle 9, Stand 530!


Vielen Dank für Ihre Aufmerksamkeit!