Zero Trust SASE + Managed Security Operations

Netskope One – Sicherheit auf allen Wegen

Netskope One

- One Engine
- One Client
- One Network
- One Gateway

ERGEBNIS

Erhöhen der Agilität
Komplexität reduzieren
Risiken minimieren
Benutzererfahrung
Senkung der Kosten

Netskope NewEdge Private Cloud

Weltweite Abdeckung gewährleistet Sicherheit ohne Performance Einbußen

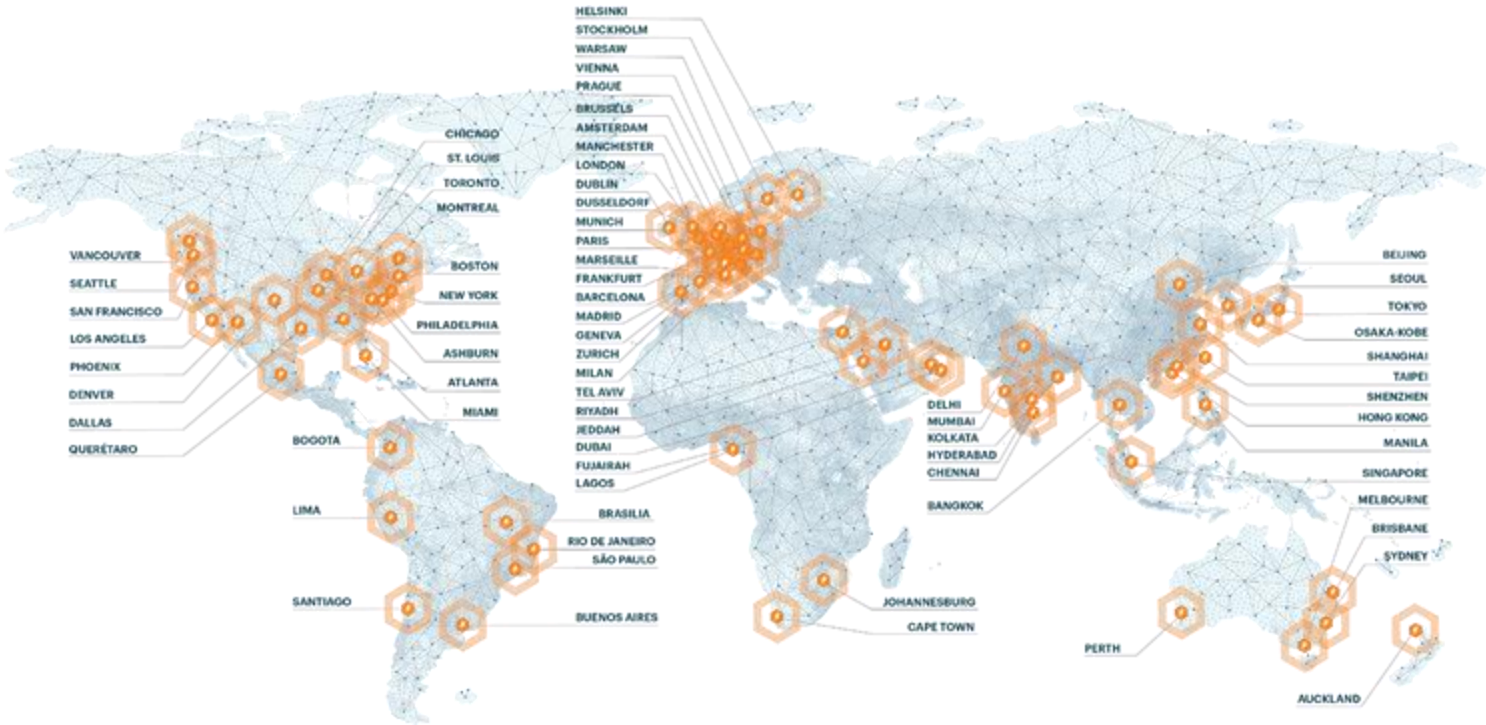
75+
Regionen

200+
Localization Zones

4K+
Network Adjacencies

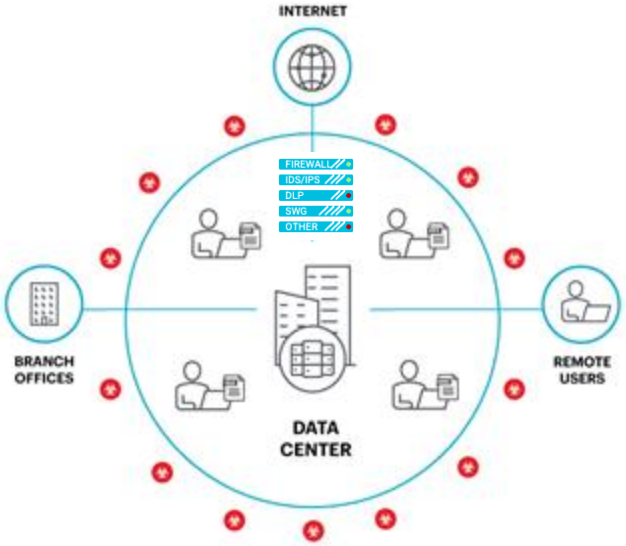
FULL
Compute

Industry's Best
SLAs



Die digitalen Infrastrukturen sind im Wandel

Früher – Perimeter Sicherheit



Connect + Authenticate

Heute – Zero Trust

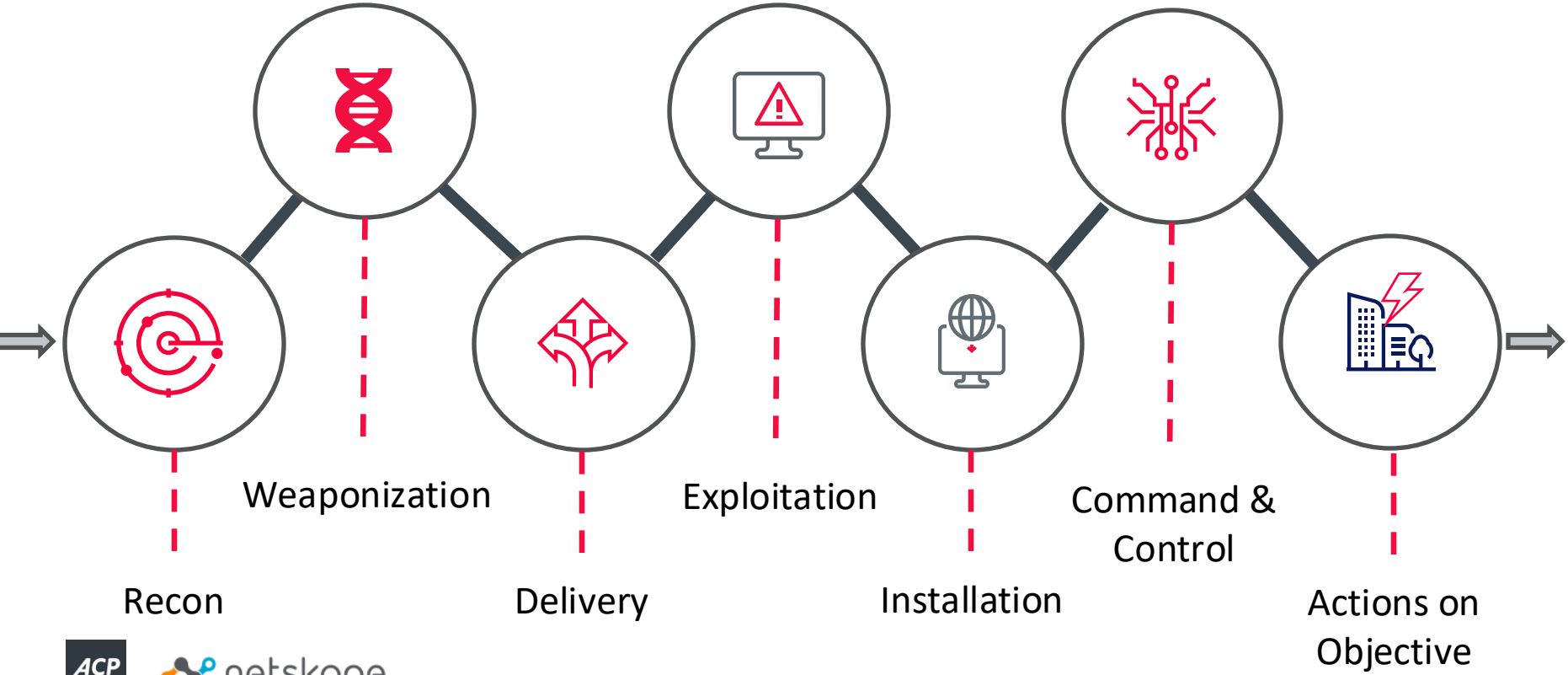
Authenticate + Connect

- **60%+** des Datenverkehrs sind SaaS und Cloud, welche 50 % der Bedrohungen verursachen
- **2.400+** SaaS-Anwendungen für durchschnittliche Unternehmen - die meisten Shadow-IT
- **95%** des Datenverkehrs ist verschlüsselt, in welchem sich Bedrohungen und Daten verstecken

ACP netskope

Ein Setup wie “früher” birgt gewisse Risiken…wir stellen vor:

Die Cyber Kill Chain



Reconnaissance – wer wird das Opfer…

- Das Opfer arbeitet beim Ziel des Angriffs
- Der Angreifer will über ihn das Unternehmen infiltrieren
- Die SASE Corp – Daniel M. 45 aus Wien

LSZ - Future Connections
8.159 Follower:innen
2 Wochen • Bearbeitet •

We are ready for #CyberSecurity - we are ready for you!

💙 Voller Power und neuer Ideen freuen wir uns auf den spannenden, Event-reichen Herbst! Wir freuen uns auf Euch liebe #ITSecurity Community!

❓ ...die 4 Affen der Weisheit 😅?
>>Nichts hören, nichts sehen, nichts sagen, keinen Spaß haben<<

‼️ In der Cyber-Security gilt bei uns: Alles hören. Alles sehen. Alles ansprechen. UND bei unseren Events gilt: Vernetzen, Austauschen und eine gute, gemeinsame Zeit habe!

Neben den thematischen Deep Dives, sind es die menschlichen Begegnungen, die unsere Cyber Crime Foren ausmachen. Zwischen den Sessions, beim Lunch oder beim Afterwork, denn genau dort entstehen oft die besten Synergien. #futureconnections

👉 Wann und wo?
Cyber Crime Salzburg, 18. September 2025
Cyber Crime Forum Graz, 29. September 2025
IT-Security Herbst Wien, 22. Oktober 2025
Cyber Crime Forum Rankweil, 20. November 2025

👉 hier gehts zu den Anmeldungen: https://lsz.at/

💙 Wir sehen uns!

Martin Pils, Jimmy Heschl, Sofie Mallinger, Anna Habenegg, Stefan Jakoubi, Lukas Wagner, Wolfgang Fasching, Siegfried "Ziggy" Schauer, Natalia Petrova-Korudzhiyski, Lukas Kulmitzer, Thomas Pfeiffer, Mag. Dzevad Mujezinovic, CIPP/E, CISM, Nicolas Petri uvm.

Sie und 33 weitere Personen
6 Kommentare • 2 Reposts

Reaktionen
+26

ACP netskope

360° Analyse - externe Sicht

Angreifer

Sammeln von Daten

- Data Leakage
- Darkweb
- Crawl Social Media

Scan der Infrastruktur

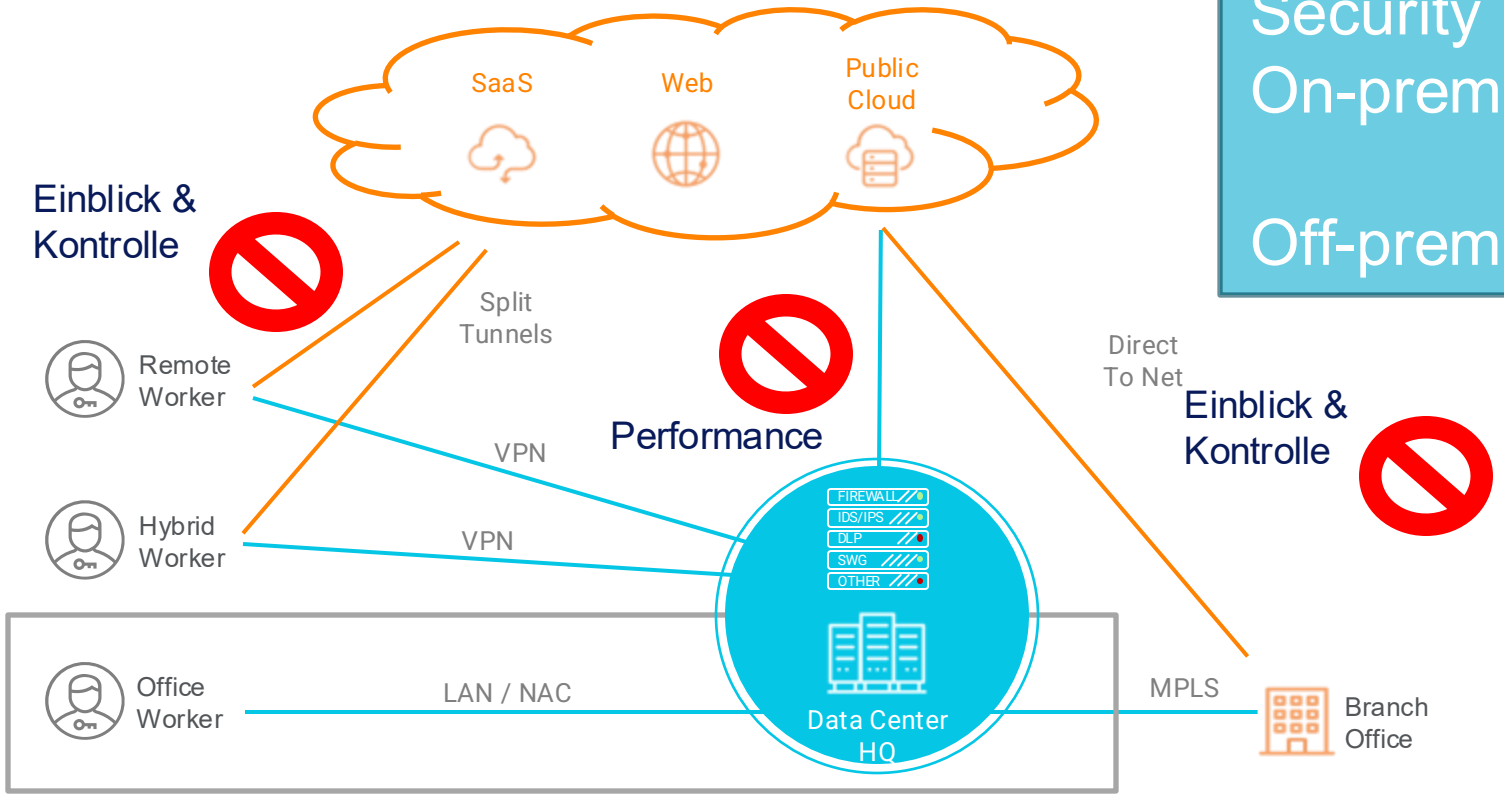
- Vulnerabilities
- External Surface

SOC-Observer

- Clear- / Deep- / Darknet Monitoring
- Threat Hunting
- External Attack Surface Management
- Vendor Vulnerability Alerting
- Nahtlose Daten-Integration

IT for innovators.

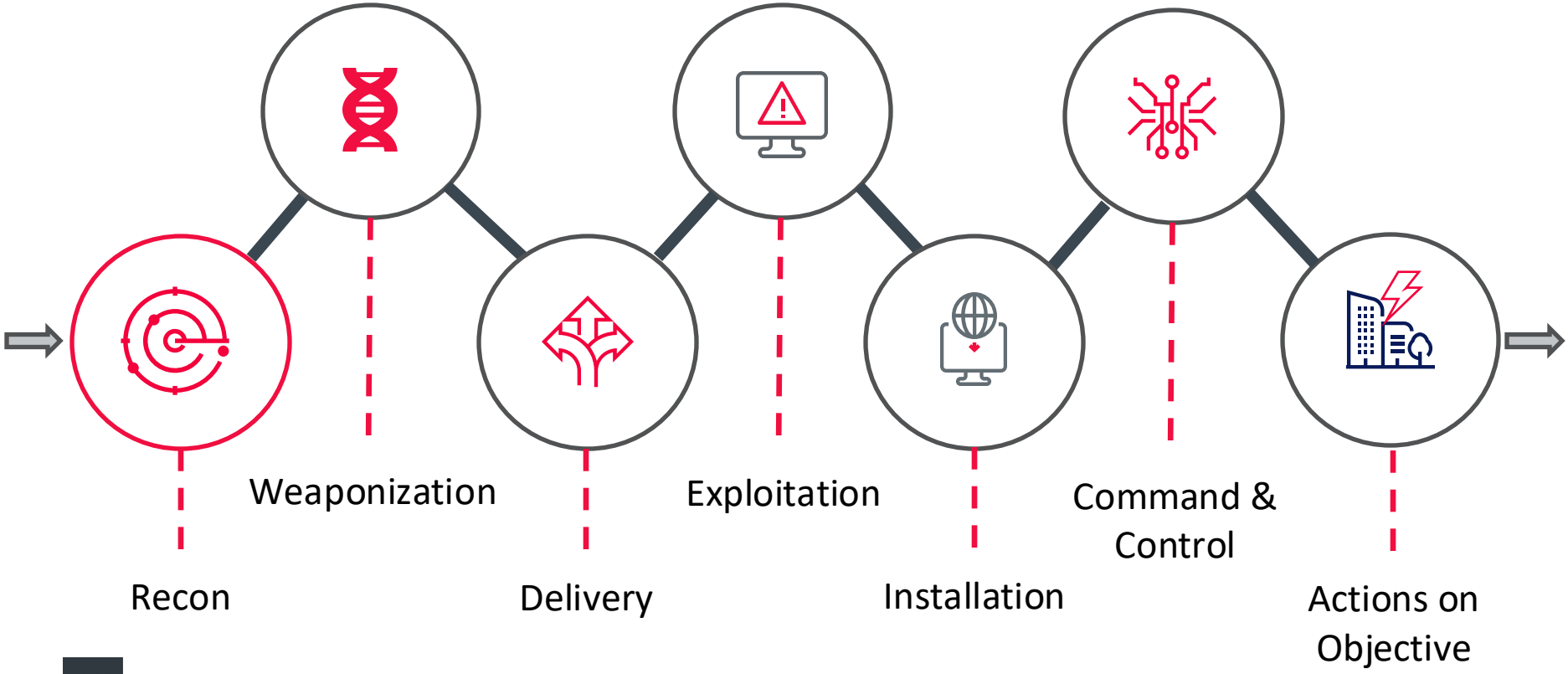
Ein oftmals angetroffenes Setup



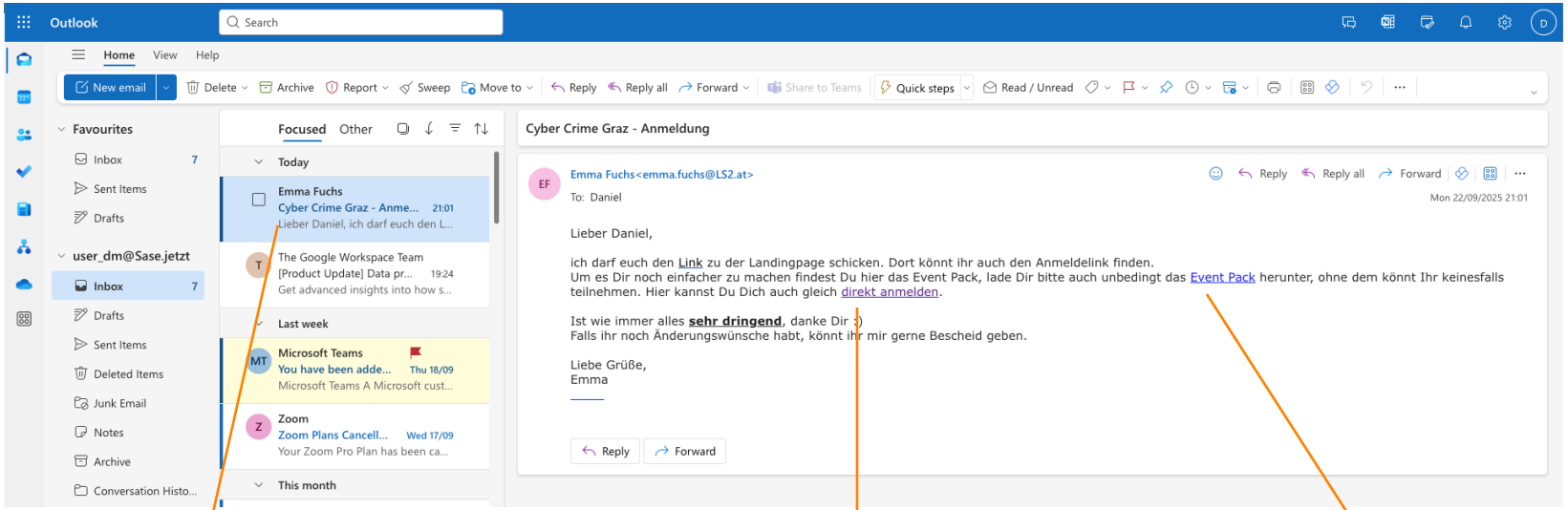
Security On-premises

Off-premises

Cyber Kill Chain



Delivery – jetzt nutzt der Angreifer sein Wissen

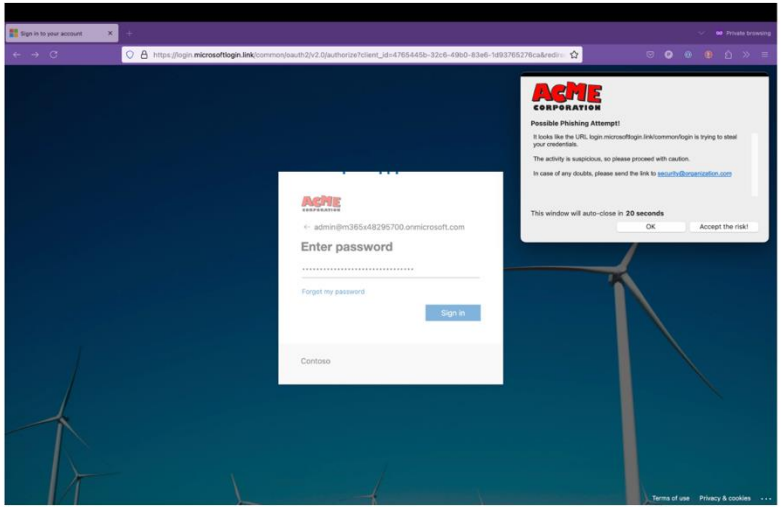


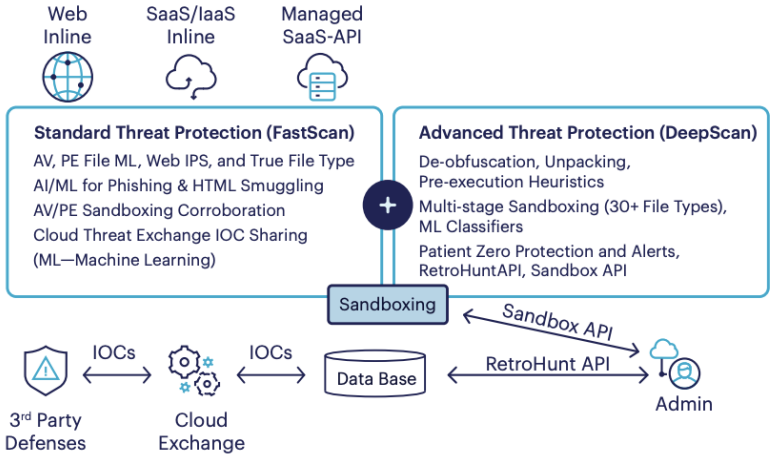
Wie immer muss man sich vor dem Event anmelden – Wie zu erwarten

Die Zeit drängt, aber Emma hat uns ja gleich einen Anmeldelink beigefügt

…und auch das Event Pack, so ein Service

Schützen Sie Ihre User vor Phishing und Malware

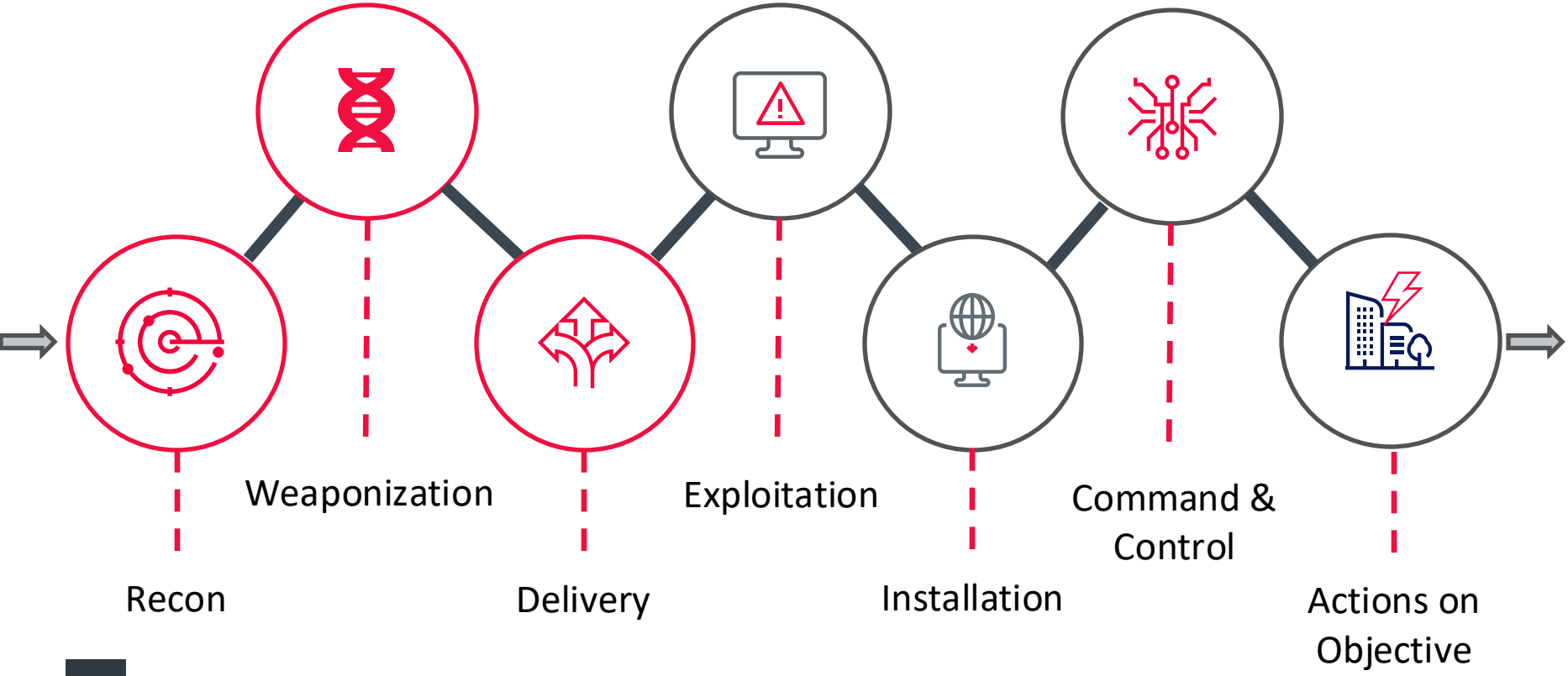




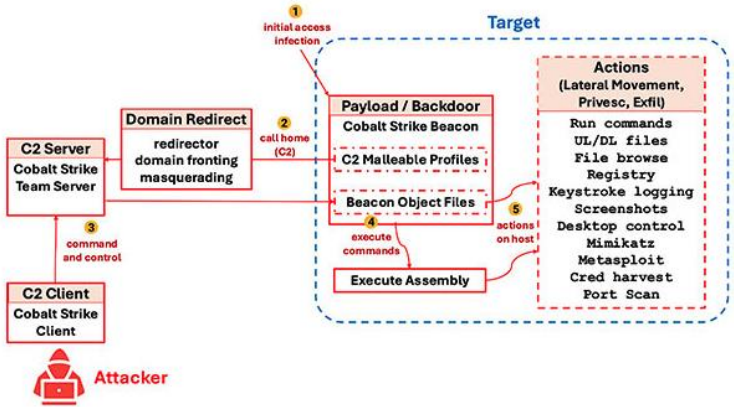
https://community.netskope.com/netskope-threat-protection-50/using-netskope-to-mitigate-the-risk-of-phishing-kits-7609

https://www.netskope.com/wp-content/uploads/2025/05/2025-06-Threat-Protection-DS-386-12.pdf

Cyber Kill Chain

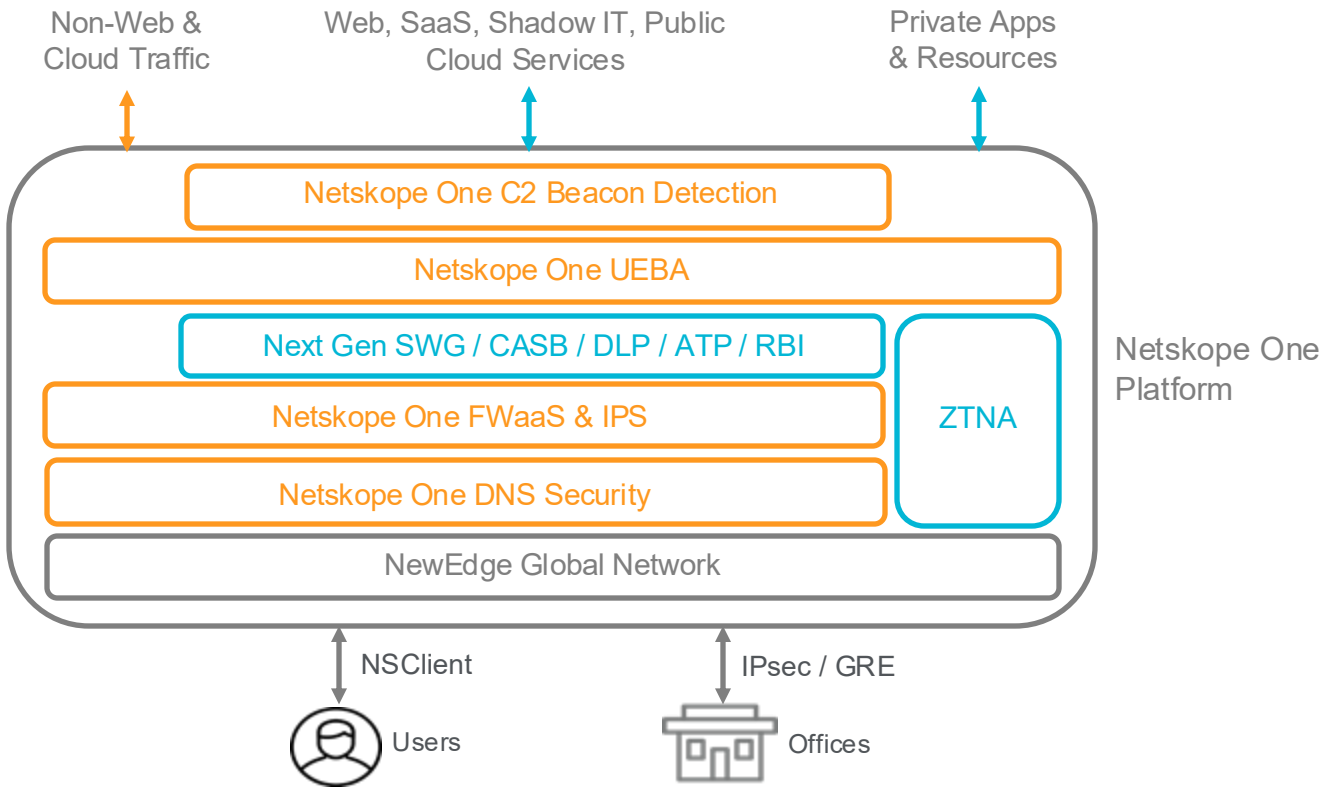


Command & Control – Kommunikation des Angreifers

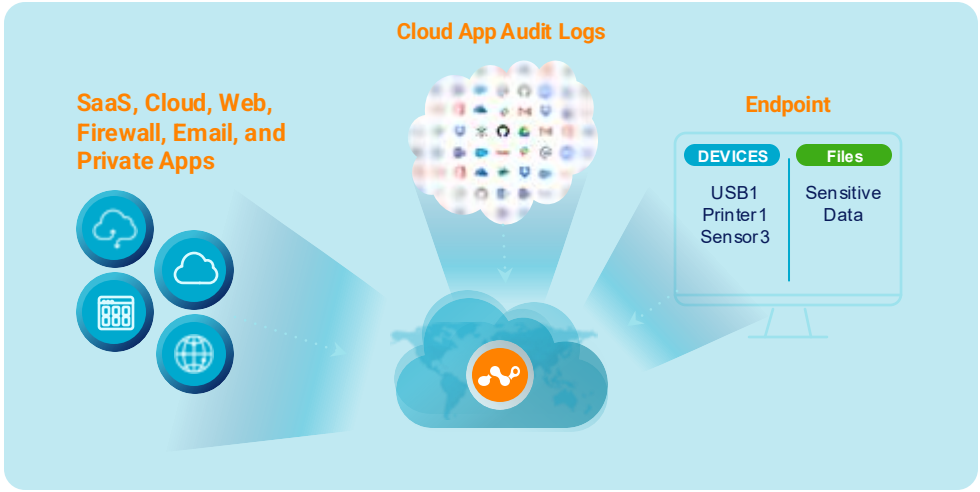


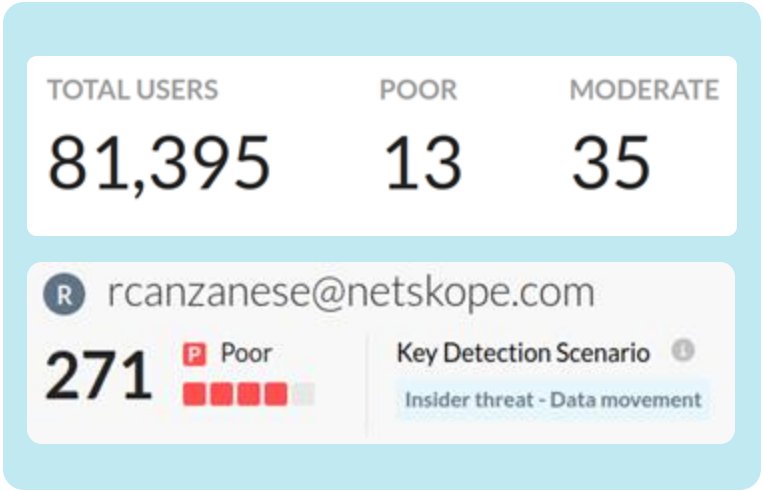
#	Attack Step	Description
1	Initial access / infection	Initial infection vector, including downloader and loader for the beacon payload.
2	Call home (C2)	Beacon calls home to Team Server utilizing HTTP/HTTPS/DNS typically. May utilize domain/IP obfuscation via redirectors such as proxies, domain fronting (e.g. CDNs) or domain masquerading. Beacons may also chain communications to bypass internal network segmentation.
3	Attacker command and control	Attacker controls Beacon, issuing various commands. May utilize Aggressor Scripts to automate/optimize workflow.
4	Execute commands	The Beacon may use Execute Assembly (.NET executables) in a separate process or Beacon Object Files within the Beacon session/process, extending post-exploit capabilities. Memory injection is used to evade detection from endpoint defenses focused on files and disk activity associated with malicious files.
5	Actions on host	Numerous built-in actions are provided for new capabilities via extensions as BOFs or Execute Assembly.

Command & Control Beacon Detection



KI unterstütztes aufdecken von Bedrohungen





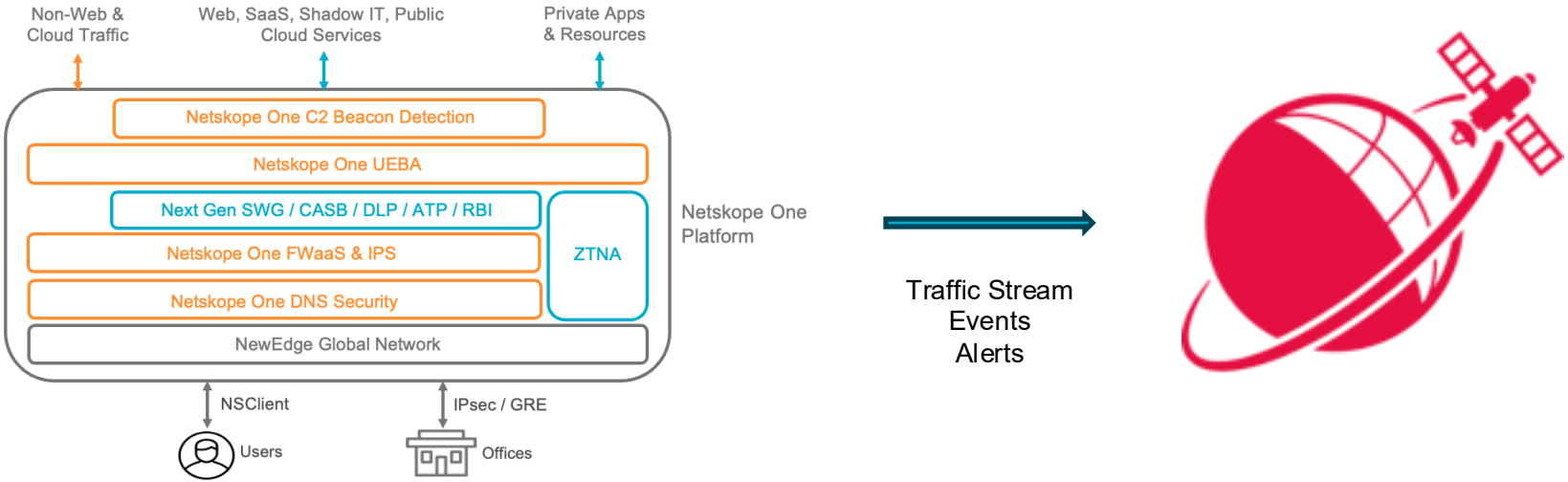
KI bewertet das Risiko jedes Nutzers kontinuierlich auf der Grundlage seines Verhaltens und seiner Bedrohungsprofile

KI-basierter User Confidence Index

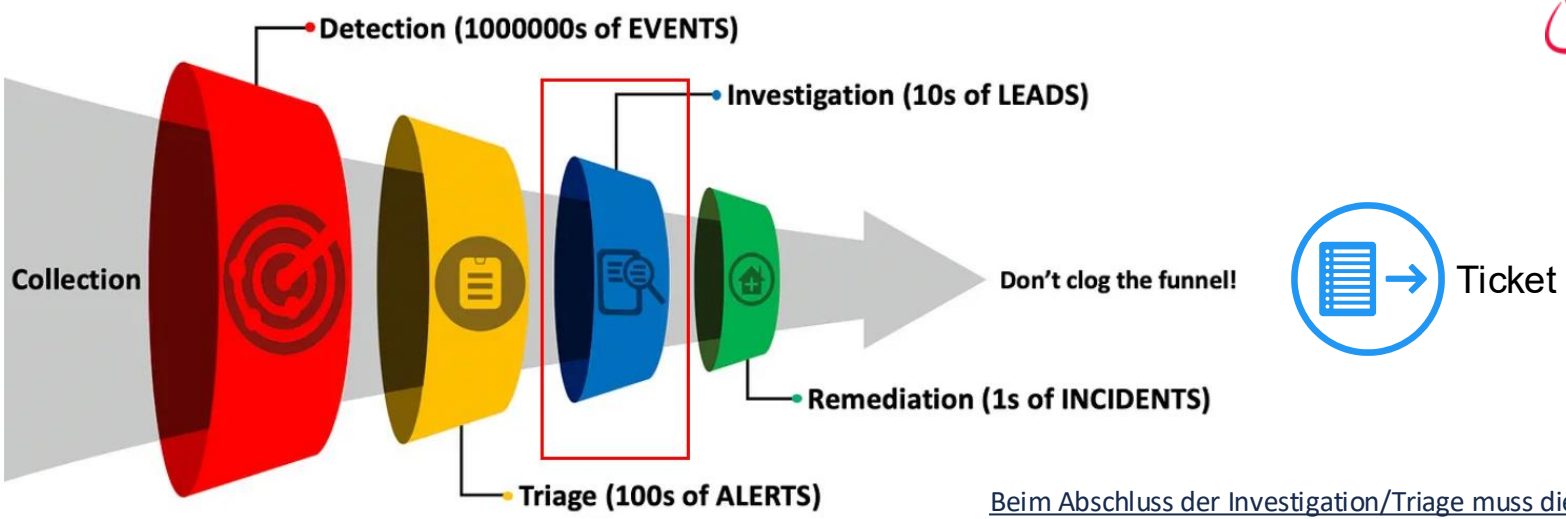
- Insider Risks
- Kompromittierte Geräte
- Kompromittierte Accounts
- C2 Beacon Detection

ACP netskope

Daten und Alarmierung an das SOC



ACP SOC Triage and Investigation

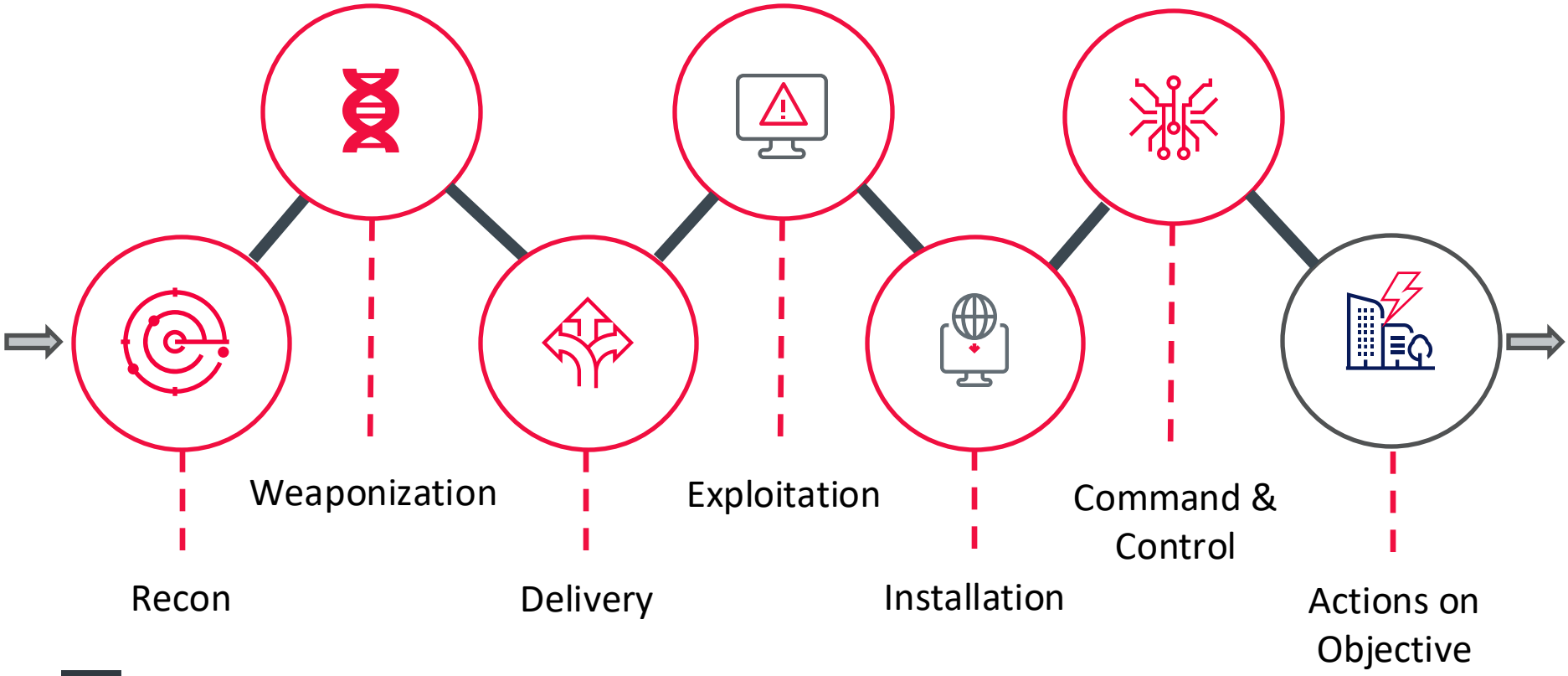


SOC DEATH Team - Detection **E**ngineering **A**nd **T**hreat **H**unting
> Use Case Entwicklung, System Training und Threat Hunting

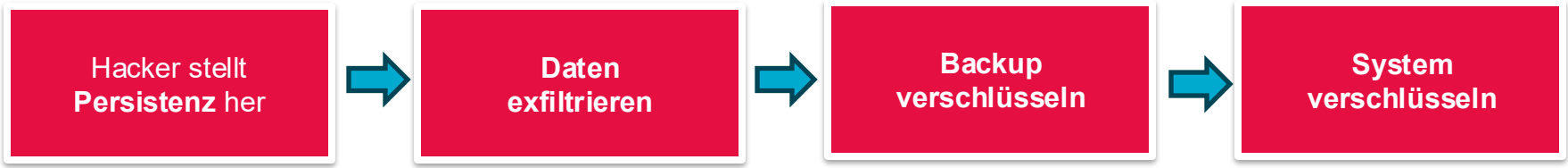
<u>Beim Abschluss der Investigation/Triage muss die Klassifizierung folgendermaßen erfolgen:</u>

- **True Positive** → Klassifizieren als True Positive
- **False Positive** / Benign Positive → Klassifizieren als False Positive
- True Negative → Nix zu tun
- False Negative → Nix möglich
- Suspicious → Darf niemals am Ende der Investigation stehen bleiben

Cyber Kill Chain



Was passiert nun ohne funktionierende Detection ?!!

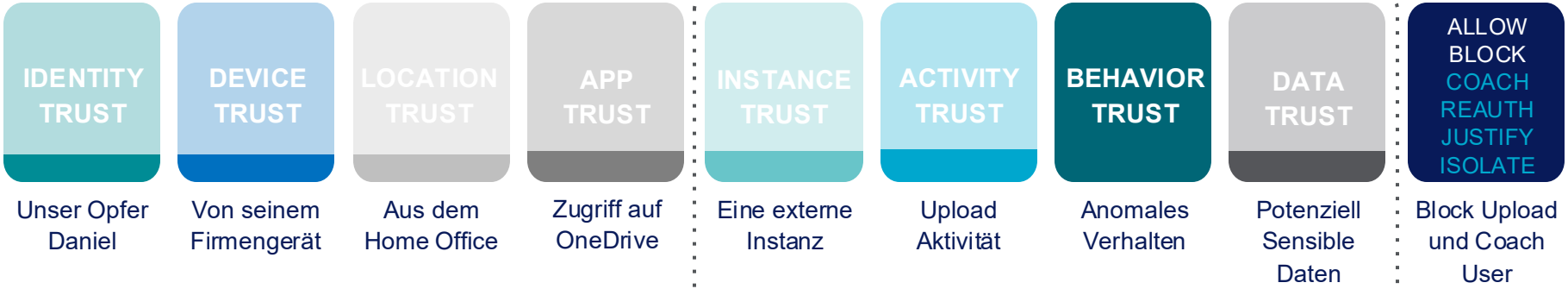


Exfiltration – Der Abzug von Daten

- meist über längeren Zeitraum – technisch unauffällig
- Oftmals über im Ziel-Unternehmen genutzte Plattformen
  - Microsoft 365 eignet sich besonders gut
    - Traffic ist encrypted
    - Oftmals über einen Split Tunnel direkt gesendet -> Performance
    - Wird selten decrypted und untersucht

Analyse und Bewertung: Netskope Zero Trust Engine

Kontinuierliche, adaptive Policy Entscheidungen in Echtzeit

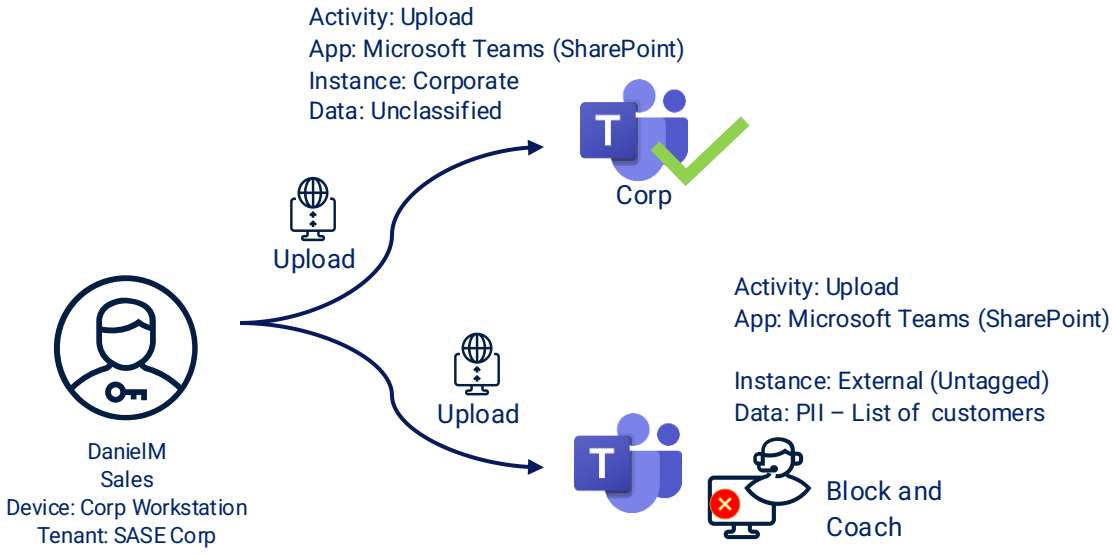


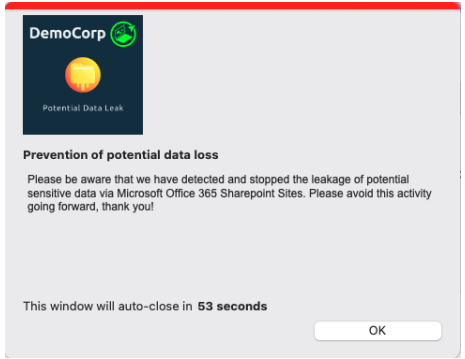
- Unterscheidung zwischen tausenden SaaS Tenants
- Einzigartige Data Protection & DLP Ansatz
- User Coaching in Echtzeit

60% des Internet Traffics geht Richtung SaaS/Cloud, 50% der Threats sind cloud-nativ

95% des Datenverkehrs ist SSL verschlüsselt gegenüber <40% in 2016

ACP netskope





User	Device	App	Instance	Risk	Category	Activity	Behavior	Content	Policy Action
Daniel M Sales	Corporate Compliant	Microsoft Teams	Partner DanielM@sase.jetzt Tenant: ExtCorp	App Risk User Risk UBA	Cloud App	Upload	Suspicious	DLP Labels **ML**	Allow **Block** **Warn/Coach** Encrypt Quarantine

ACP

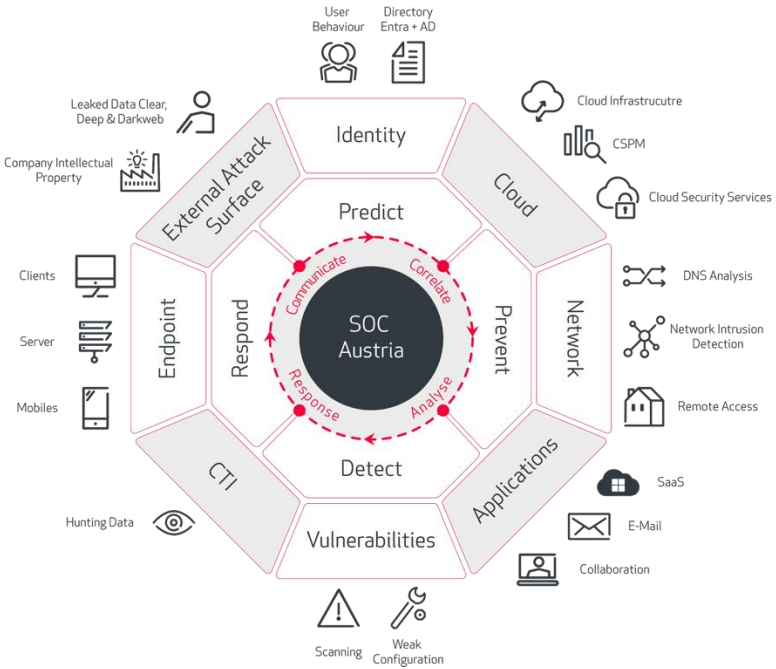
netskope

ACP Managed Service

ACP SOC

ACP NOC

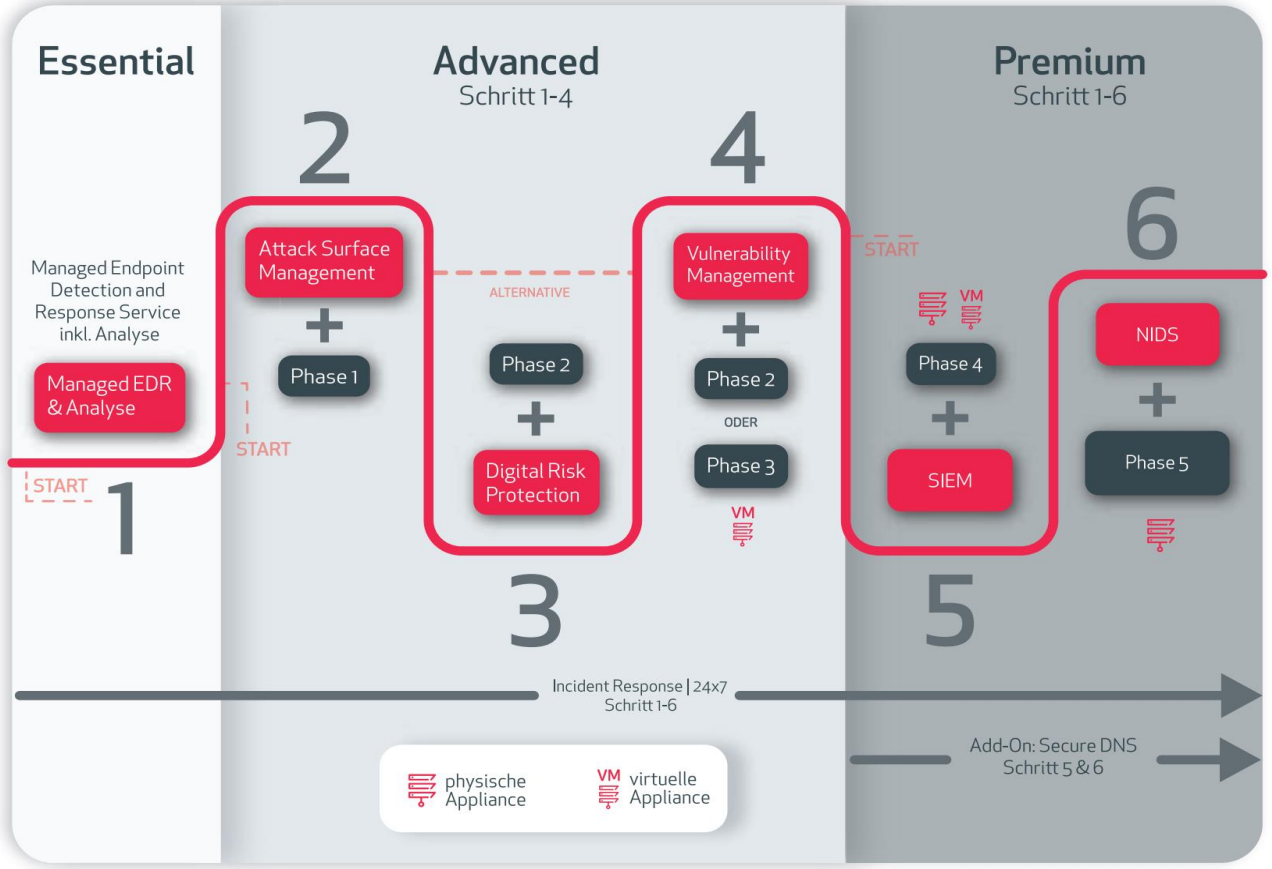
Log Daten

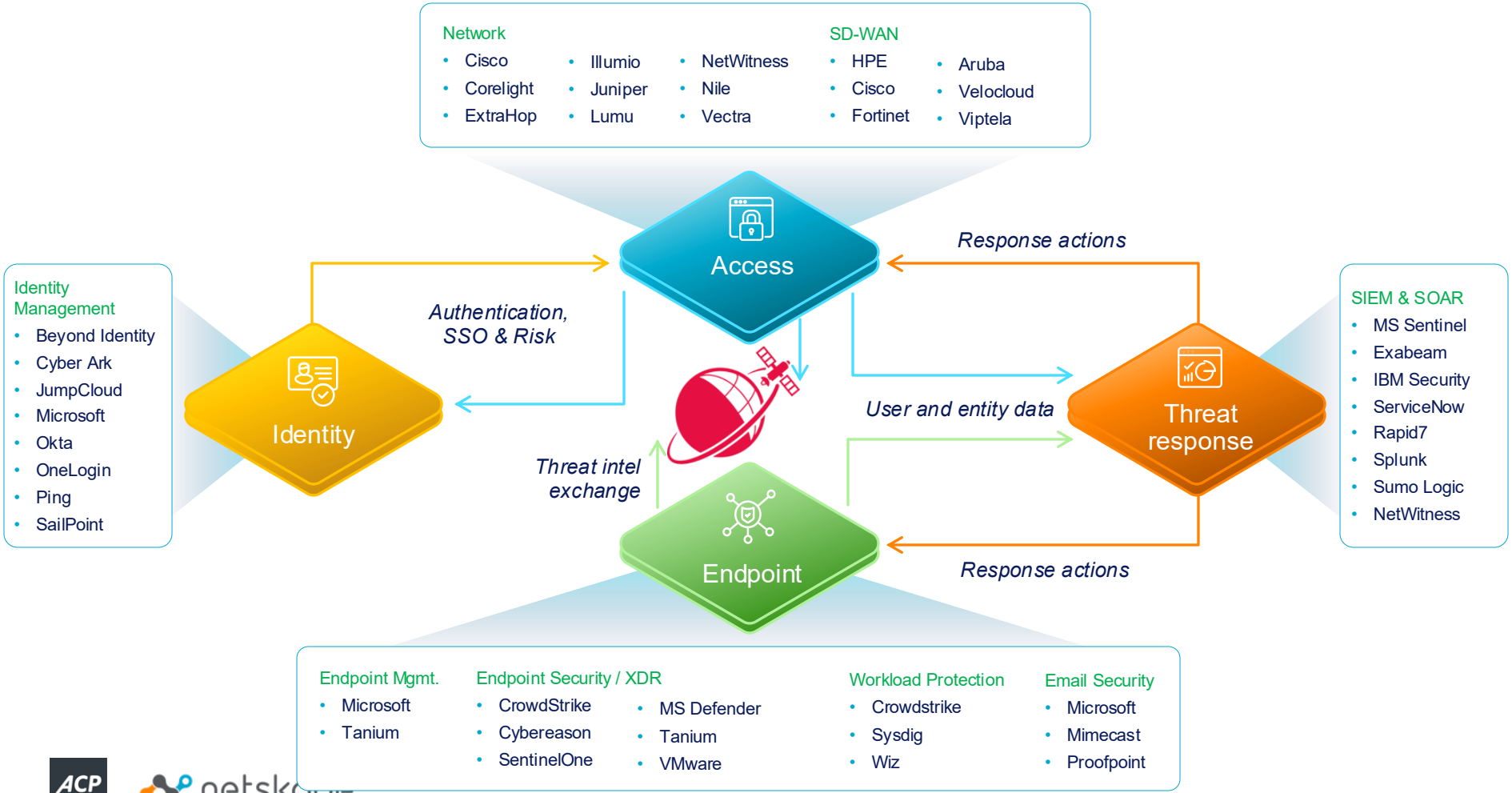


Ticket

NOC Ticket Beispiel : set user based Policy

SOC Journey





So werden Sie kein Opfer – mit Netskope und ACP

Danke!