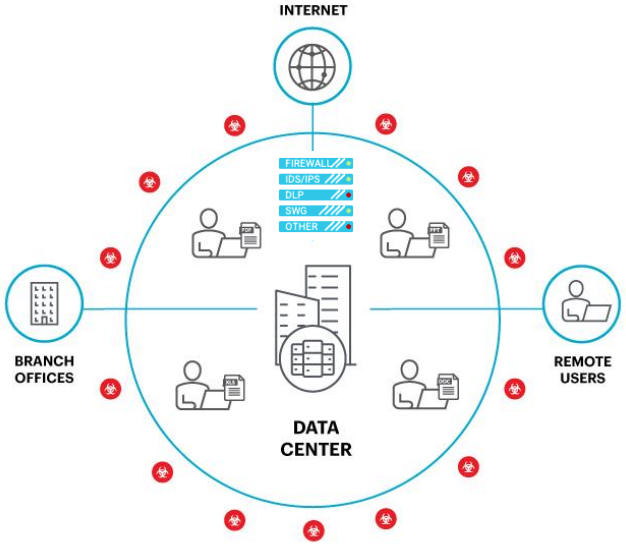
Mit SASE und Zero Trust zu gesteigerter Cyberresilienz

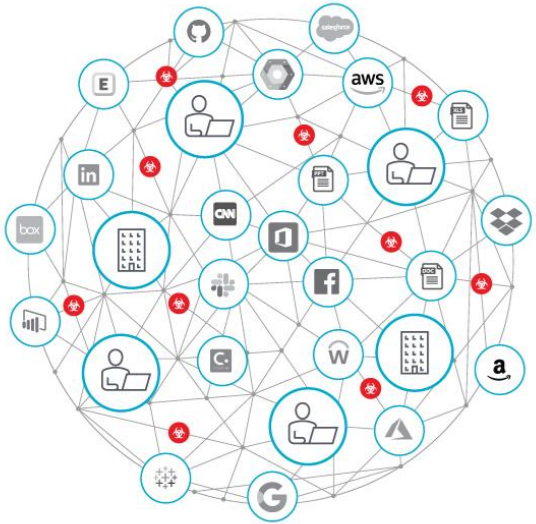
Die digitalen Infrastrukturen sind im Wandel

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

netskope

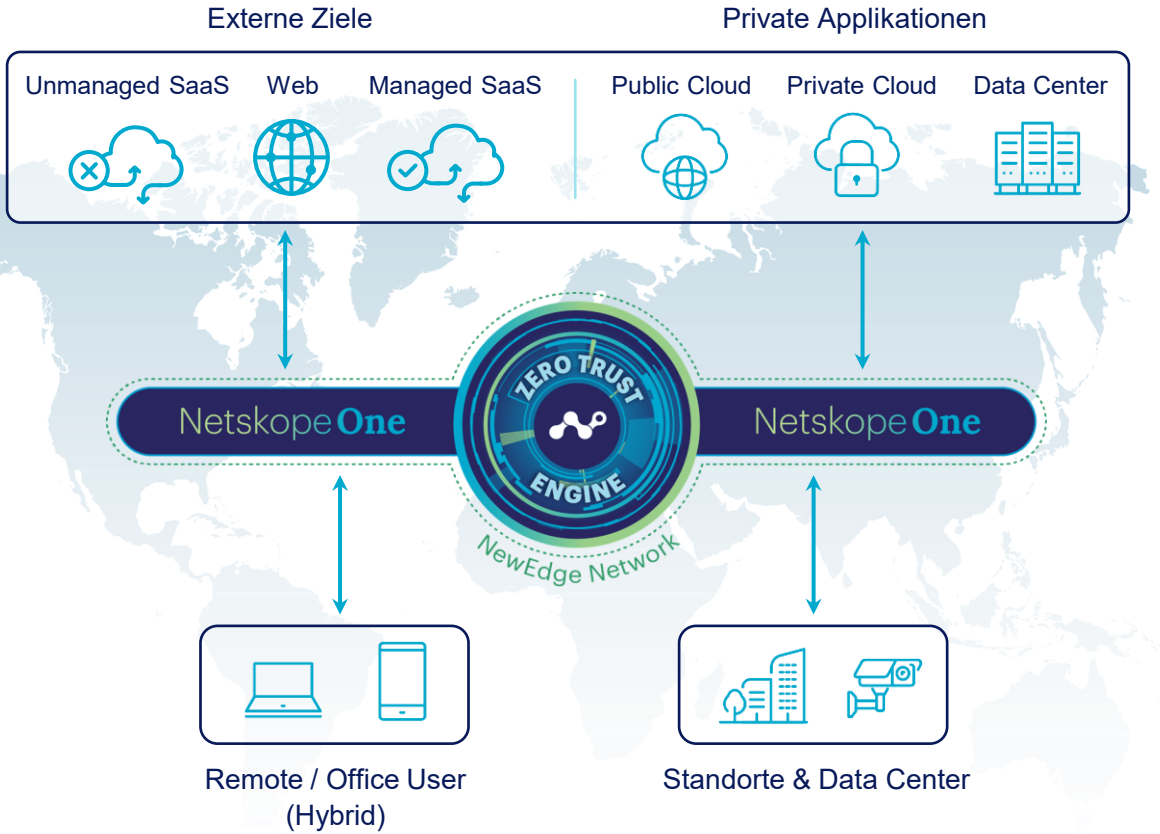
Netskope One – Sicherheit auf allen Wegen

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

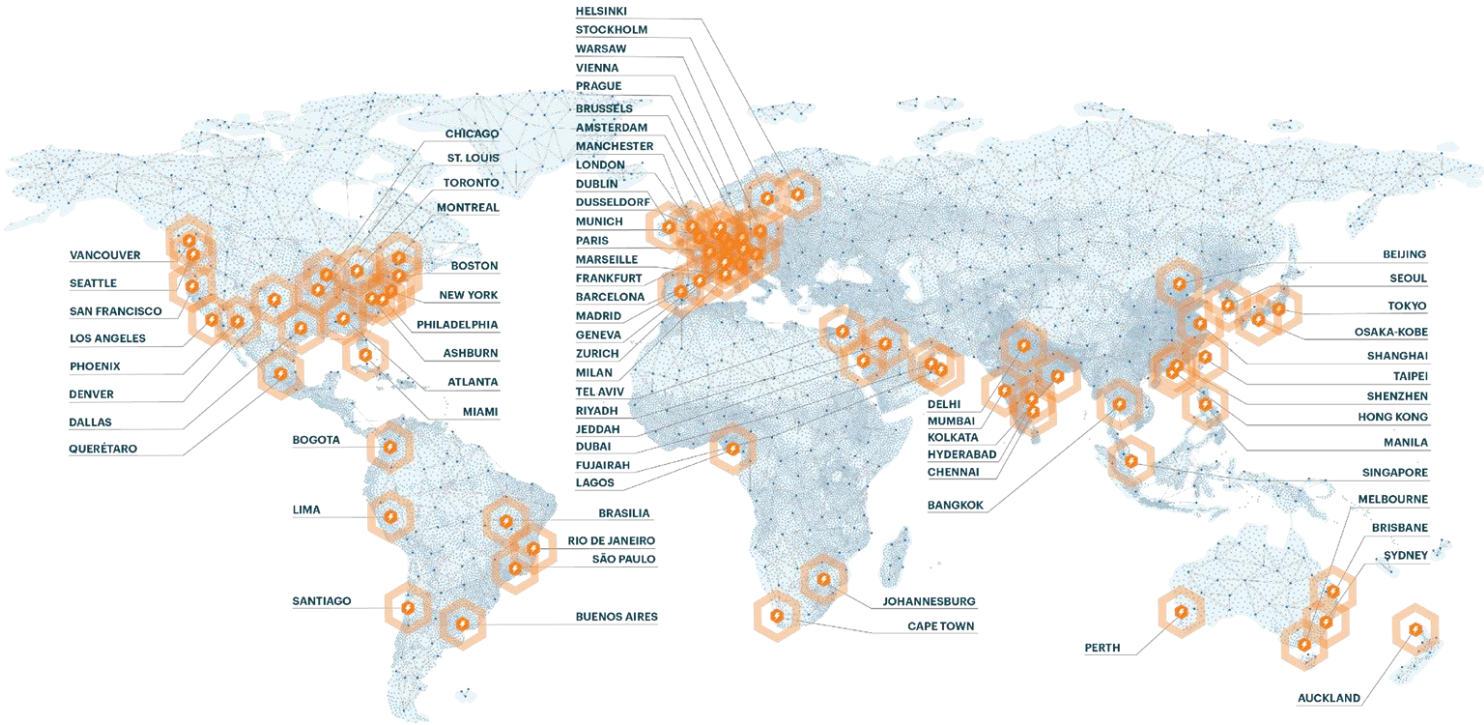
75+
Regionen

200+
Localization Zones

4K+
Network Adjacencies

FULL
Compute

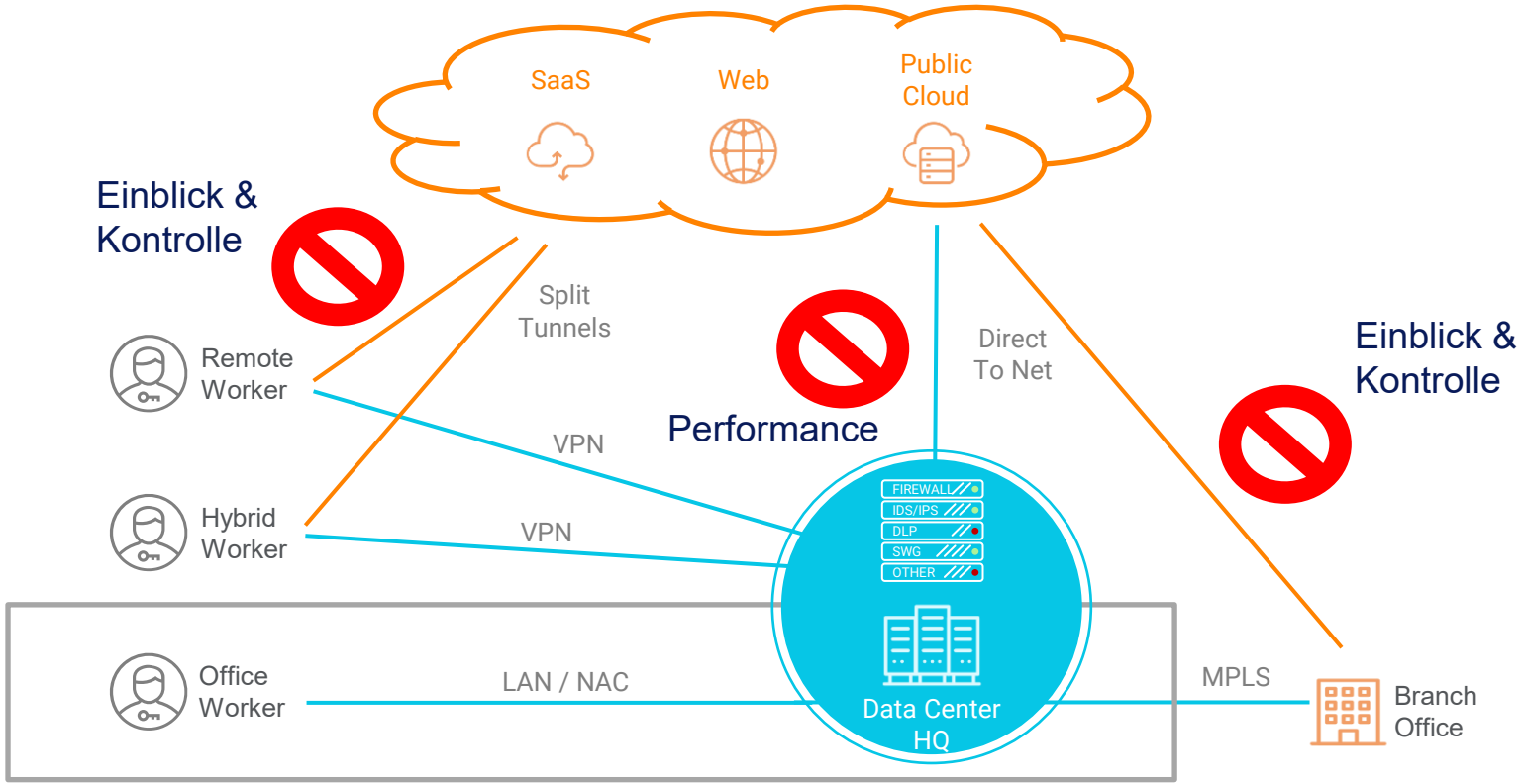
Industry's Best
SLAs



Government of Canada · FedRAMP · HIPAA COMPLIANT · ISO · irap · SSAE 18 SOC 2 · C5 · IEC · STAR LEVEL TWO · TRUSTe Certified Privacy · The EU - U.S. Privacy Shield

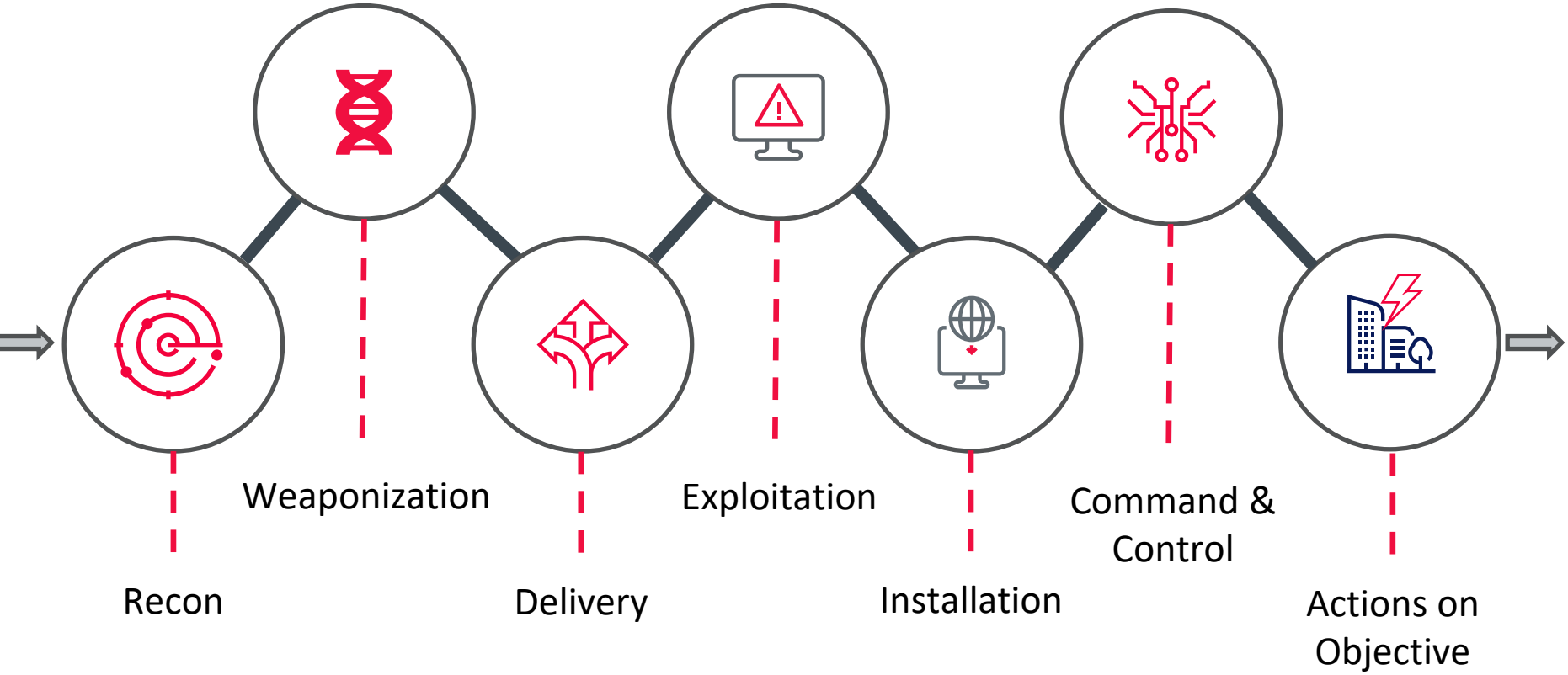
netskope

Ein oftmals angetroffenes Setup…



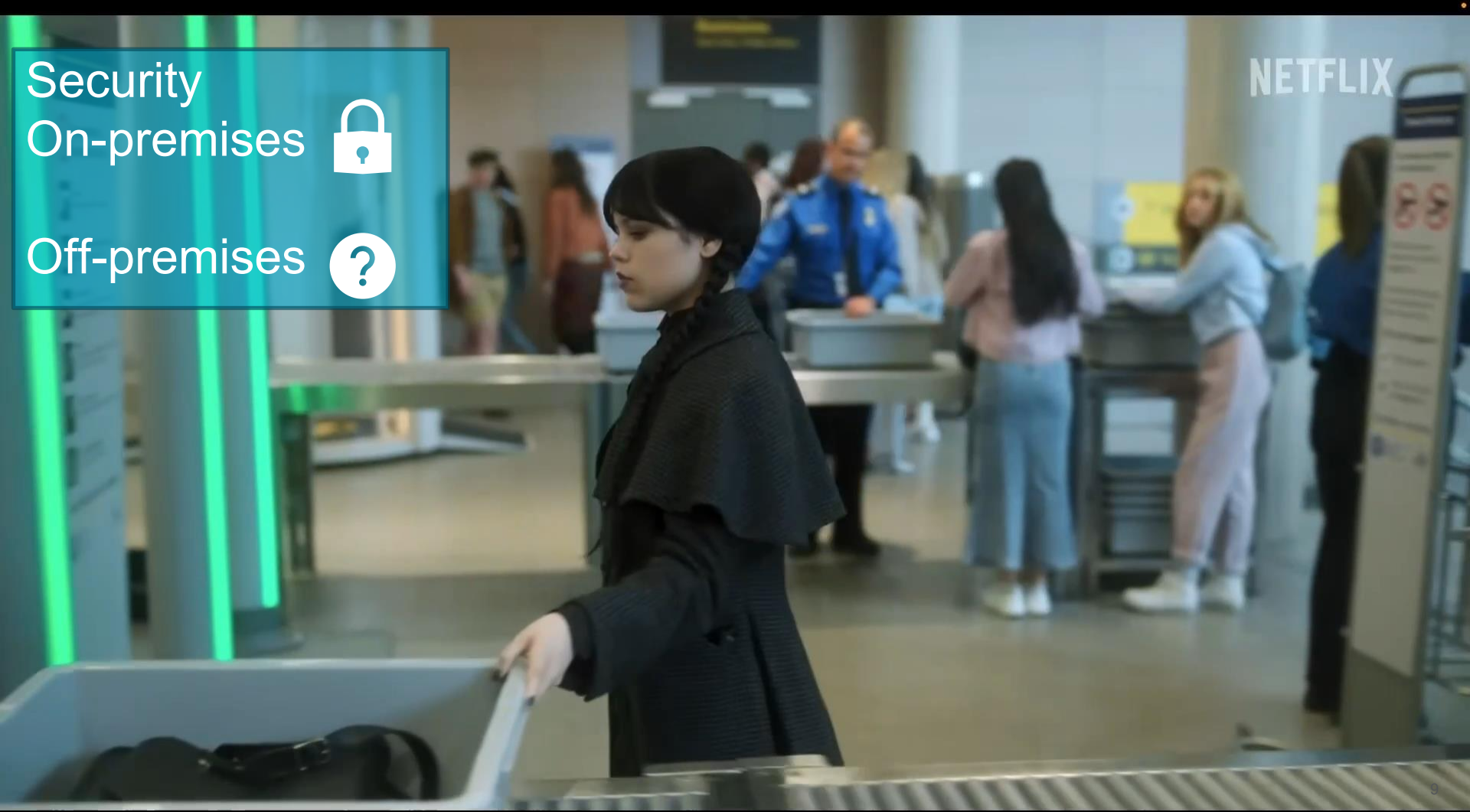

…birgt gewisse Risiken…
NETFLIX

Cyber Kill Chain

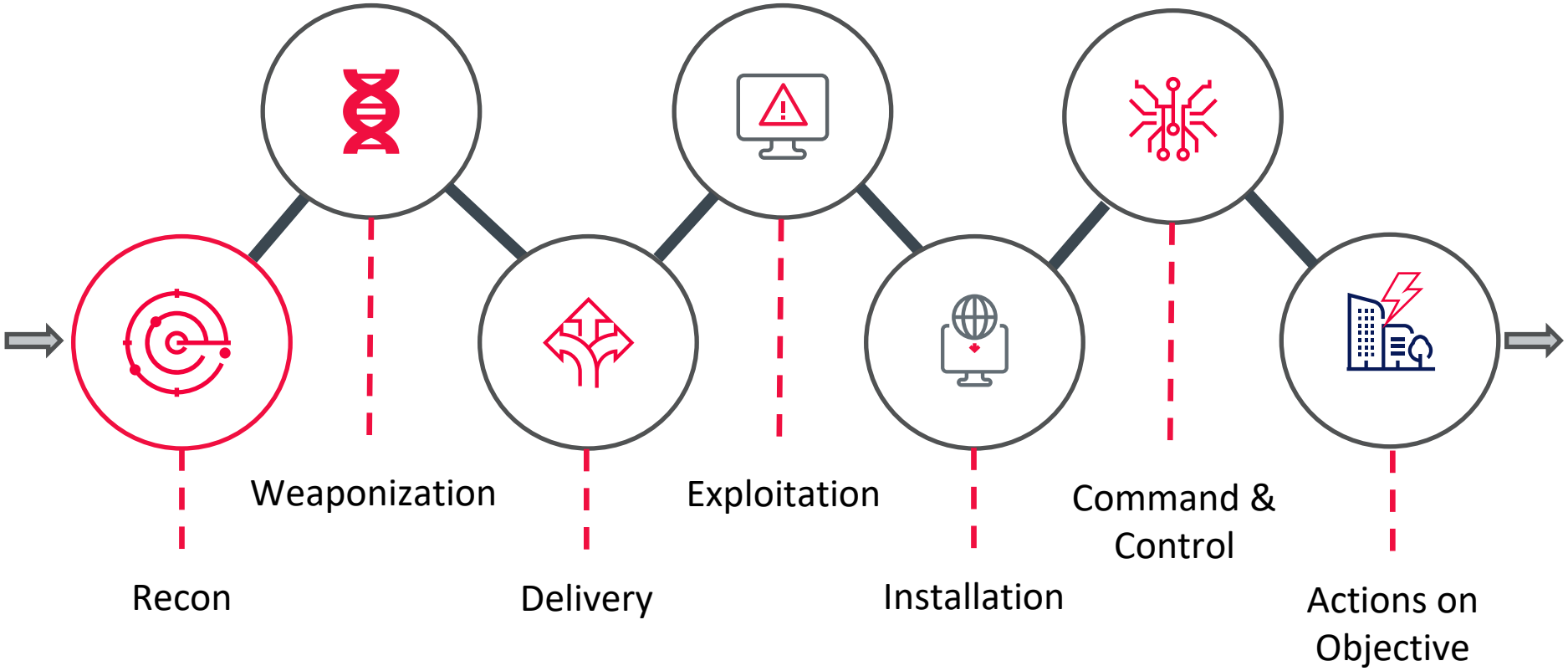


Reconnaissance – wer wird das Opfer…

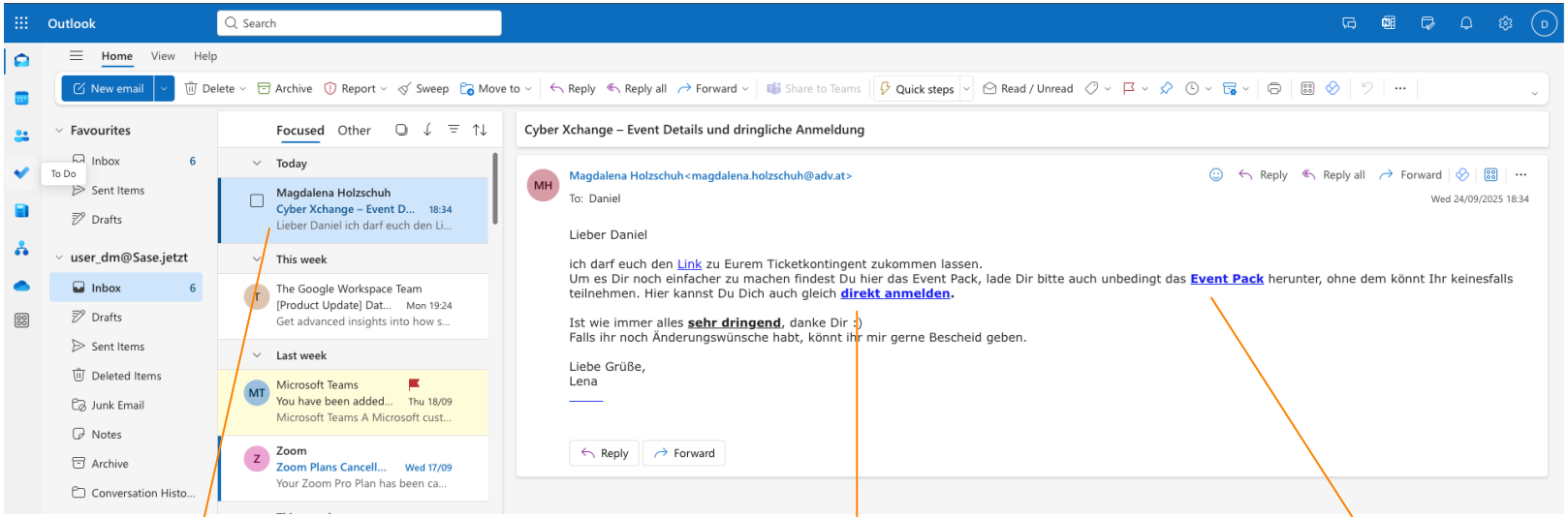
- Das Opfer arbeitet beim Ziel unseres Angriffs
- Der Angreifer will über ihn das Unternehmen infiltrieren
- Die SASE Corp – Daniel M. 45 aus Wien


Security
On-premises
Off-premises
?
NETFLIX

Cyber Kill Chain



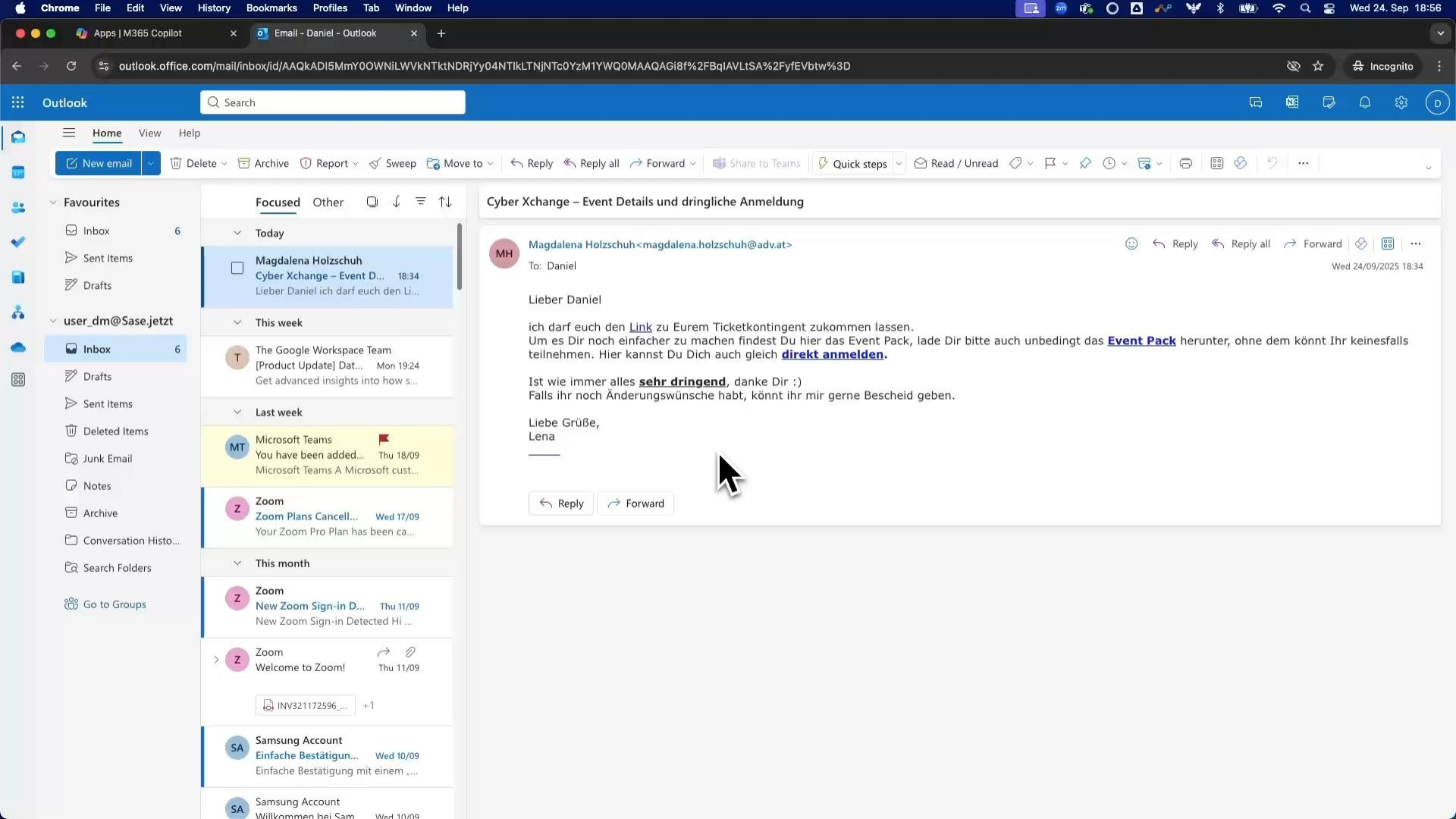
Delivery – jetzt nutzt der Angreifer sein Wissen



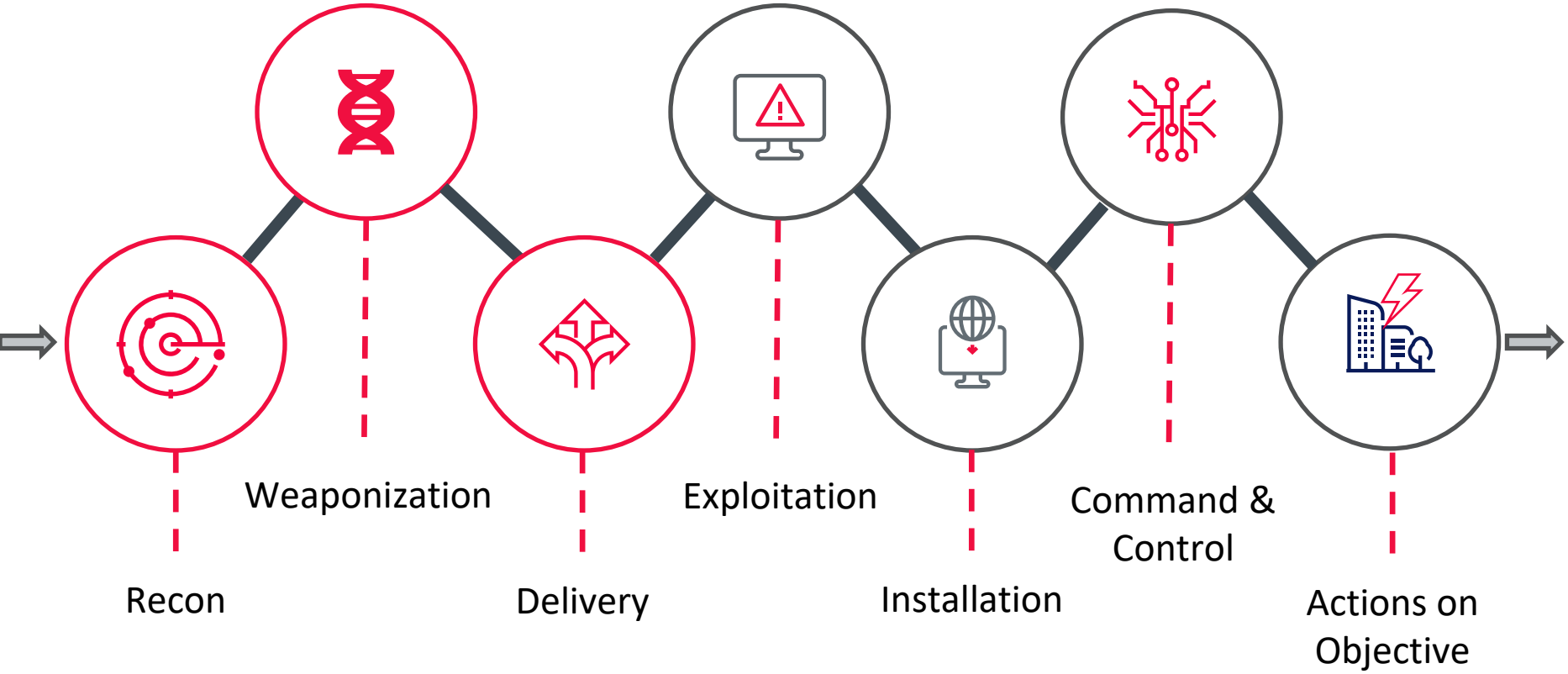
Wie immer muss man sich vor dem Event anmelden – Wie zu erwarten

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

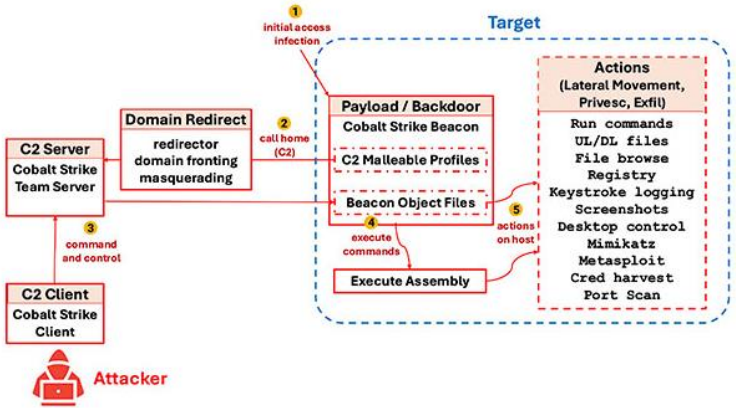
…und auch das Event Pack, so ein Service


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed 24. Sep 18:56
Apps | M365 Copilot
Email - Daniel - Outlook
outlook.office.com/mail/inbox/id/AAQkADI5MmY0OWNiLWVkNTktNDRjYy04NTlkLTNjNTc0YzM1YWQ0MAAQAGi8f%2FBqIAVLtSA%2FyfEVbtw%3D
Incognito
Outlook
Search
Home View Help
New email Delete Archive Report Sweep Move to Reply Reply all Forward Share to Teams Quick steps Read / Unread
Favourites
Inbox 6
Sent Items
Drafts
user_dm@Sase.jetzt
Inbox 6
Drafts
Sent Items
Deleted Items
Junk Email
Notes
Archive
Conversation Histo...
Search Folders
Go to Groups
Focused Other
Today
Magdalena Holzschuh
Cyber Xchange – Event D... 18:34
Lieber Daniel ich darf euch den Li...
This week
The Google Workspace Team
[Product Update] Dat... Mon 19:24
Get advanced insights into how s...
Last week
Microsoft Teams
You have been added... Thu 18/09
Microsoft Teams A Microsoft cust...
Zoom
Zoom Plans Cancell... Wed 17/09
Your Zoom Pro Plan has been ca...
This month
Zoom
New Zoom Sign-in D... Thu 11/09
New Zoom Sign-in Detected Hi ...
Zoom
Welcome to Zoom! Thu 11/09
INV321172596_... +1
Samsung Account
Einfache Bestätigun... Wed 10/09
Einfache Bestätigung mit einem „...
Samsung Account
Willkommen bei Sam... Wed 10/09
Cyber Xchange – Event Details und dringliche Anmeldung
Magdalena Holzschuh<magdalena.holzschuh@adv.at>
To: Daniel
Reply Reply all Forward
Wed 24/09/2025 18:34
Lieber Daniel
ich darf euch den Link zu Eurem Ticketkontingent zukommen lassen.
Um es Dir noch einfacher zu machen findest Du hier das Event Pack, lade Dir bitte auch unbedingt das Event Pack herunter, ohne dem könnt Ihr keinesfalls teilnehmen. Hier kannst Du Dich auch gleich direkt anmelden.
Ist wie immer alles sehr dringend, danke Dir :)
Falls ihr noch Änderungswünsche habt, könnt ihr mir gerne Bescheid geben.
Liebe Grüße,
Lena
Reply Forward

Cyber Kill Chain

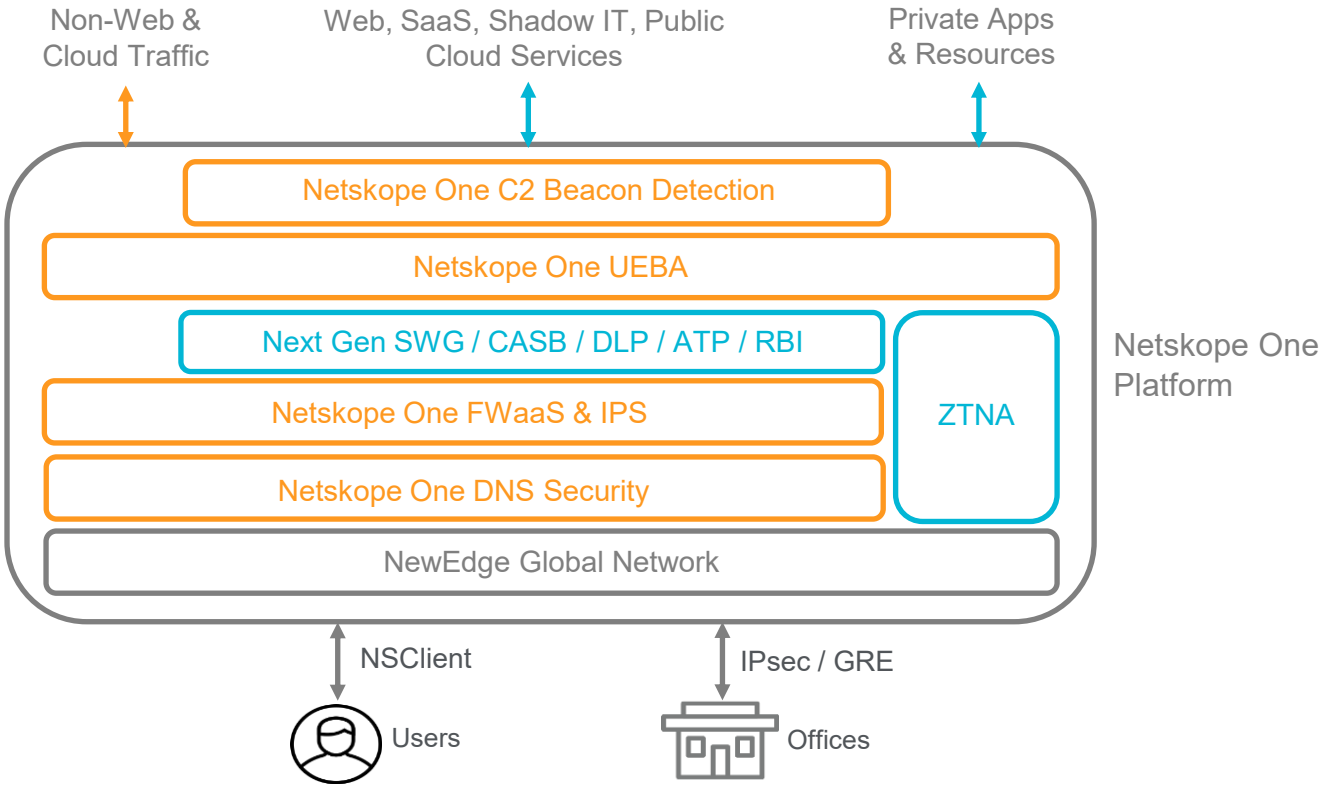


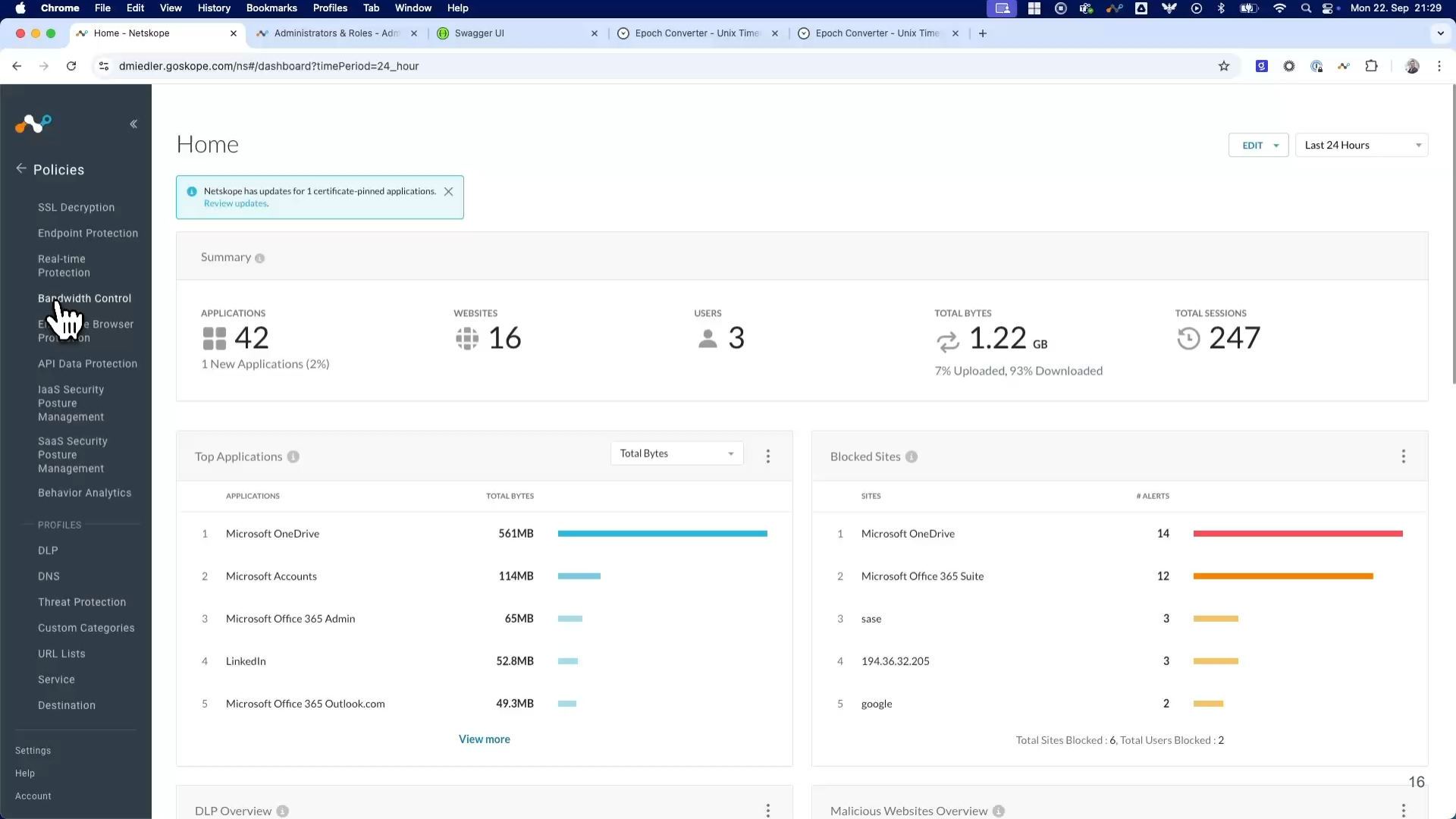
Command & Control – Kommunikation des Angreifers



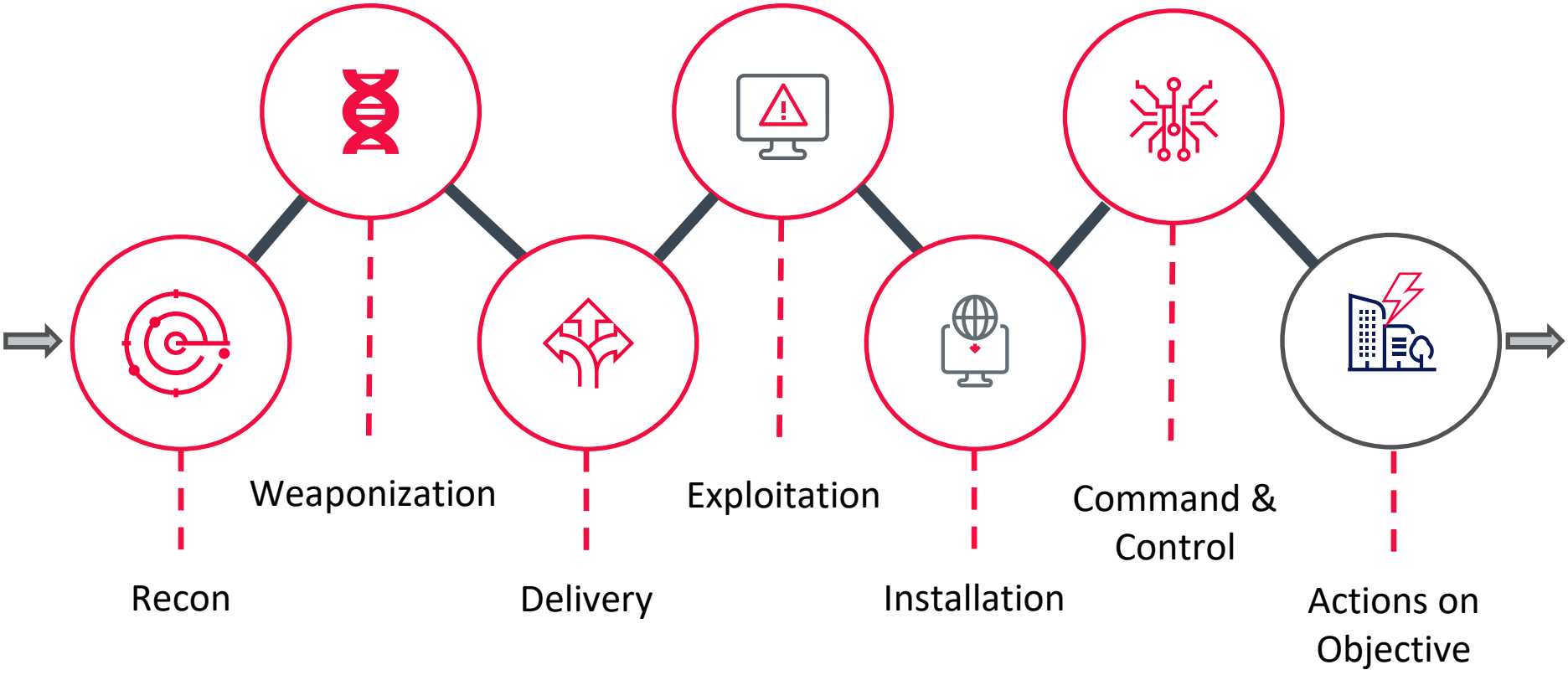
#	Attack Step	Description
1	Initial access / infection	Initial infection vector, including downloader and loader for the beacon payload.
2	Call home (C2)	Beacon calls home to Team Server utilizing HTTP/HTTPS/DNS typically. May utilize domain/IP obfuscation via redirectors such as proxies, domain fronting (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



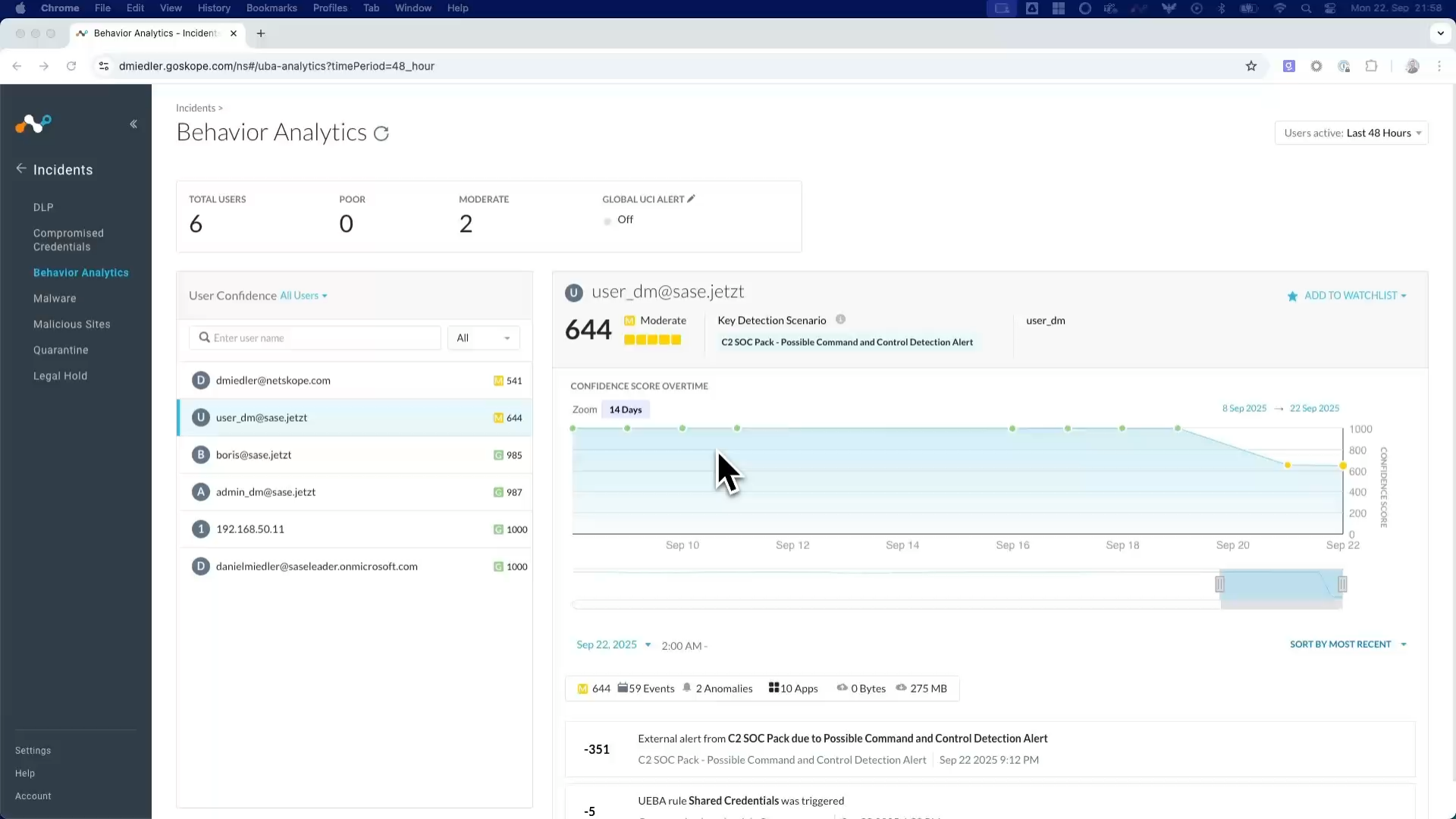

Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 22. Sep 21:29
Home - Netskope
Administrators & Roles - Adm
Swagger UI
Epoch Converter - Unix Time
Epoch Converter - Unix Time
dmiedler.goskope.com/ns#/dashboard?timePeriod=24_hour
Policies
SSL Decryption
Endpoint Protection
Real-time Protection
Bandwidth Control
Browser Isolation
API Data Protection
IaaS Security Posture Management
SaaS Security Posture Management
Behavior Analytics
PROFILES
DLP
DNS
Threat Protection
Custom Categories
URL Lists
Service
Destination
Settings
Help
Account
Home
EDIT
Last 24 Hours
Netskope has updates for 1 certificate-pinned applications.
Review updates.
Summary
APPLICATIONS
42
1 New Applications (2%)
WEBSITES
16
USERS
3
TOTAL BYTES
1.22 GB
7% Uploaded, 93% Downloaded
TOTAL SESSIONS
247
Top Applications
Total Bytes
APPLICATIONS
TOTAL BYTES
1 Microsoft OneDrive 561MB
2 Microsoft Accounts 114MB
3 Microsoft Office 365 Admin 65MB
4 LinkedIn 52.8MB
5 Microsoft Office 365 Outlook.com 49.3MB
View more
Blocked Sites
SITES
ALERTS
1 Microsoft OneDrive 14
2 Microsoft Office 365 Suite 12
3 sase 3
4 194.36.32.205 3
5 google 2
Total Sites Blocked : 6, Total Users Blocked : 2
DLP Overview
Malicious Websites Overview
16

Cyber Kill Chain



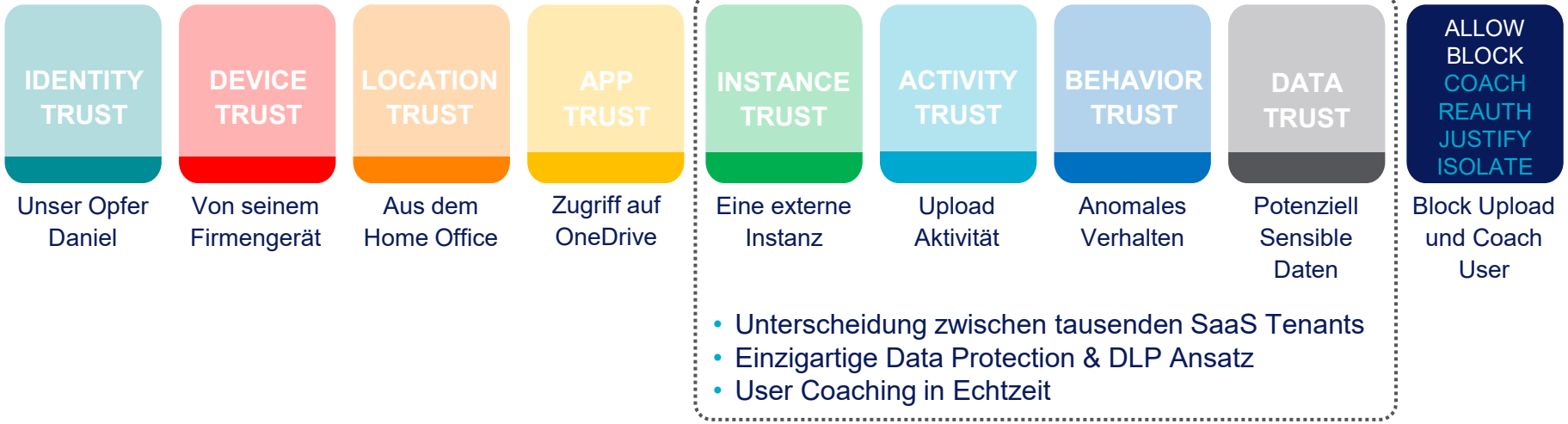
Exfiltration – Der Abzug von Daten

- 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


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon 22. Sep 21:58
Behavior Analytics - Incident
dmiedler.goskope.com/ns#/uba-analytics?timePeriod=48_hour
Incidents
DLP
Compromised Credentials
Behavior Analytics
Malware
Malicious Sites
Quarantine
Legal Hold
Settings
Help
Account
Incidents >
Behavior Analytics
Users active: Last 48 Hours
TOTAL USERS
6
POOR
0
MODERATE
2
GLOBAL UCI ALERT
Off
User Confidence All Users
Enter user name
All
dmiedler@netskope.com 541
user_dm@sase.jetzt 644
boris@sase.jetzt 985
admin_dm@sase.jetzt 987
192.168.50.11 1000
danielmiedler@saseleader.onmicrosoft.com 1000
user_dm@sase.jetzt
ADD TO WATCHLIST
644
Moderate
Key Detection Scenario
C2 SOC Pack - Possible Command and Control Detection Alert
user_dm
CONFIDENCE SCORE OVERTIME
Zoom 14 Days
8 Sep 2025 → 22 Sep 2025
1000
800
600
400
200
0
CONFIDENCE SCORE
Sep 10
Sep 12
Sep 14
Sep 16
Sep 18
Sep 20
Sep 22
Sep 22, 2025
2:00 AM -
SORT BY MOST RECENT
644
59 Events
2 Anomalies
10 Apps
0 Bytes
275 MB
-351
External alert from C2 SOC Pack due to Possible Command and Control Detection Alert
C2 SOC Pack - Possible Command and Control Detection Alert | Sep 22 2025 9:12 PM
-5
UEBA rule Shared Credentials was triggered

Analyse und Bewertung: Netskope Zero Trust Engine

Kontinuierliche, adaptive Policy Entscheidungen 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

Zero Trust in Aktion

Ständige Verifizierung

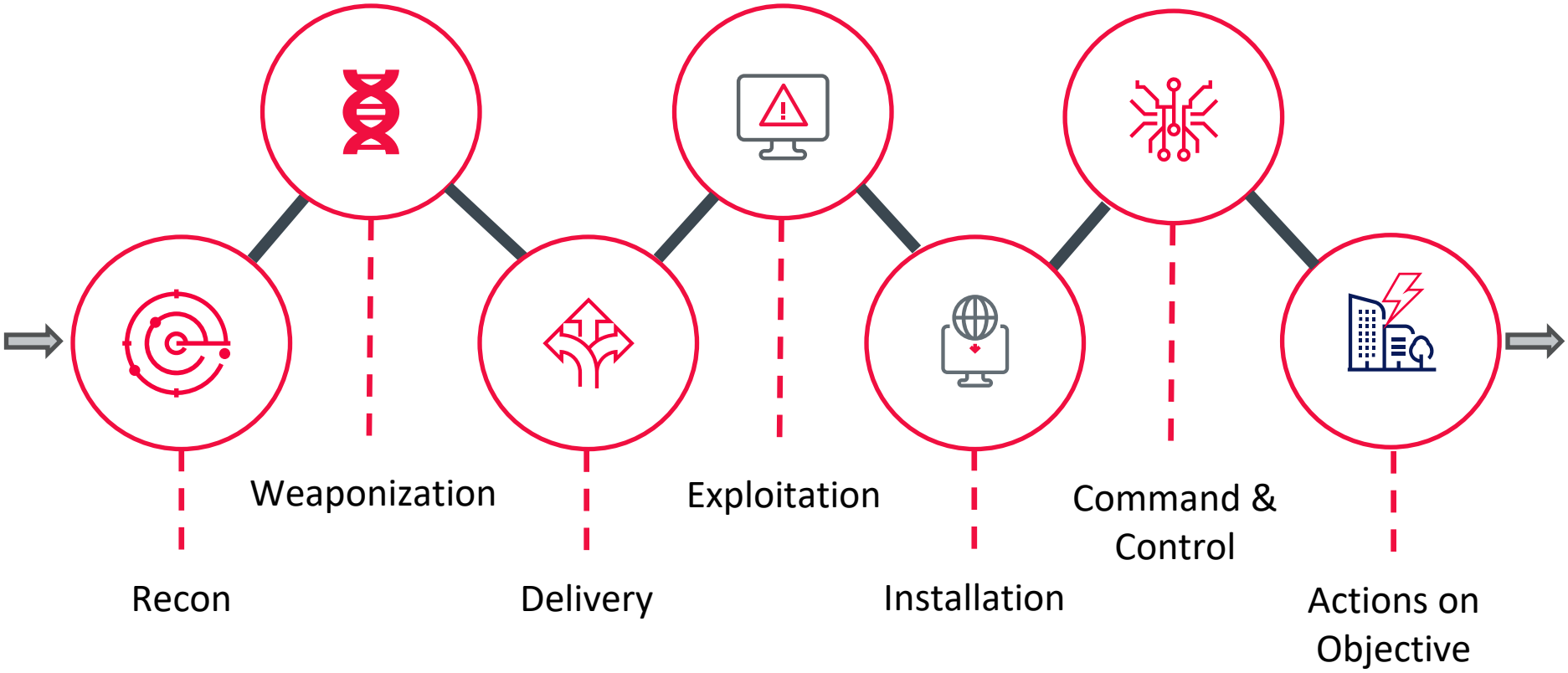
Least Privilege

Assume Breach

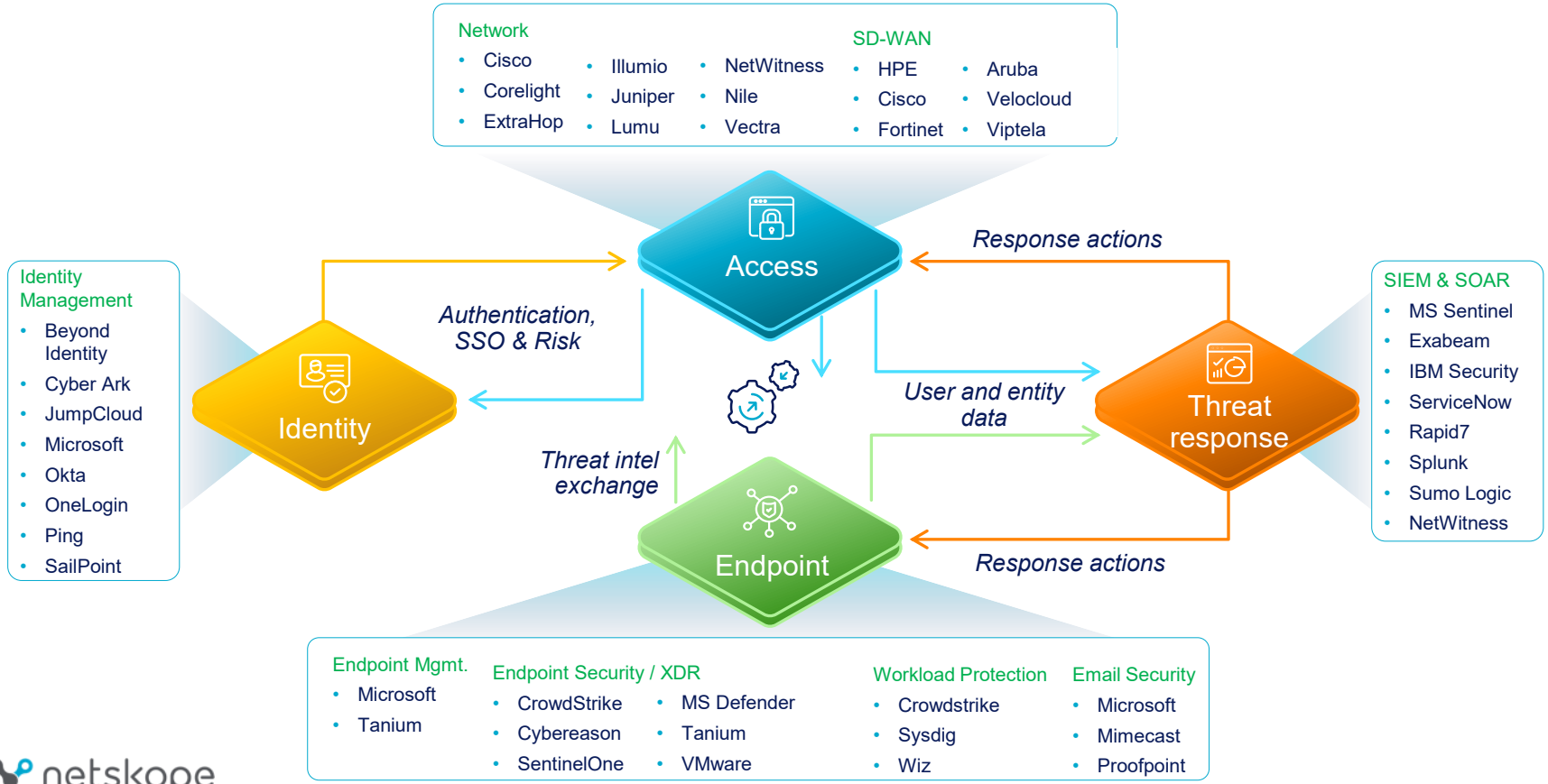
Risiko Minimierung

netskope

Cyberresilienz entlang der Cyber Kill Chain braucht…



…die Integration aller Security Layer - Netskope Cloud Exchange



Gesteigerte Cyberresilienz– mit Netskope Zero Trust SASE

Danke!

netskope