Controlware Security Day 2022

proofpoint.

controlware

proofpoint®

Cyberangriffe an der Quelle stoppen:

Verringern Sie das Risiko durch Microsoft 365 mit angemessenem Schutz

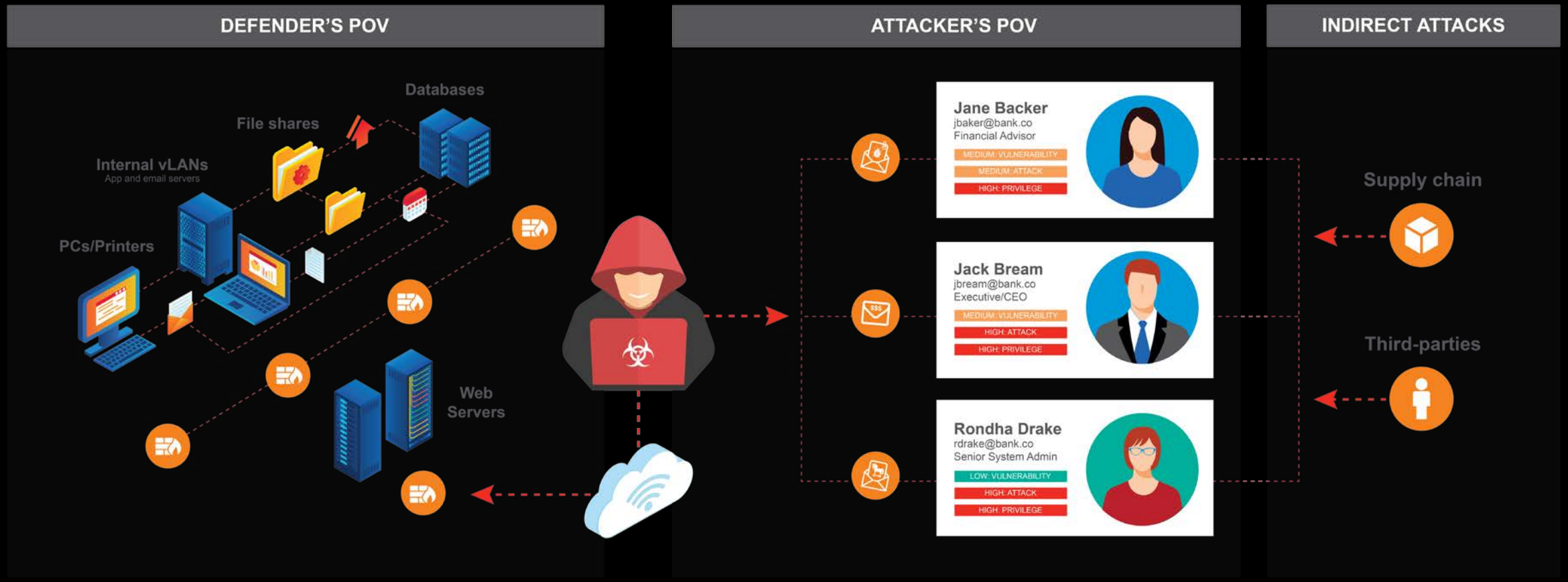
Presenter: Oliver Adam – Staff Systems Engineer – oadam@proofpoint.com

Ziel und Ursprung von Angriffen in 2022

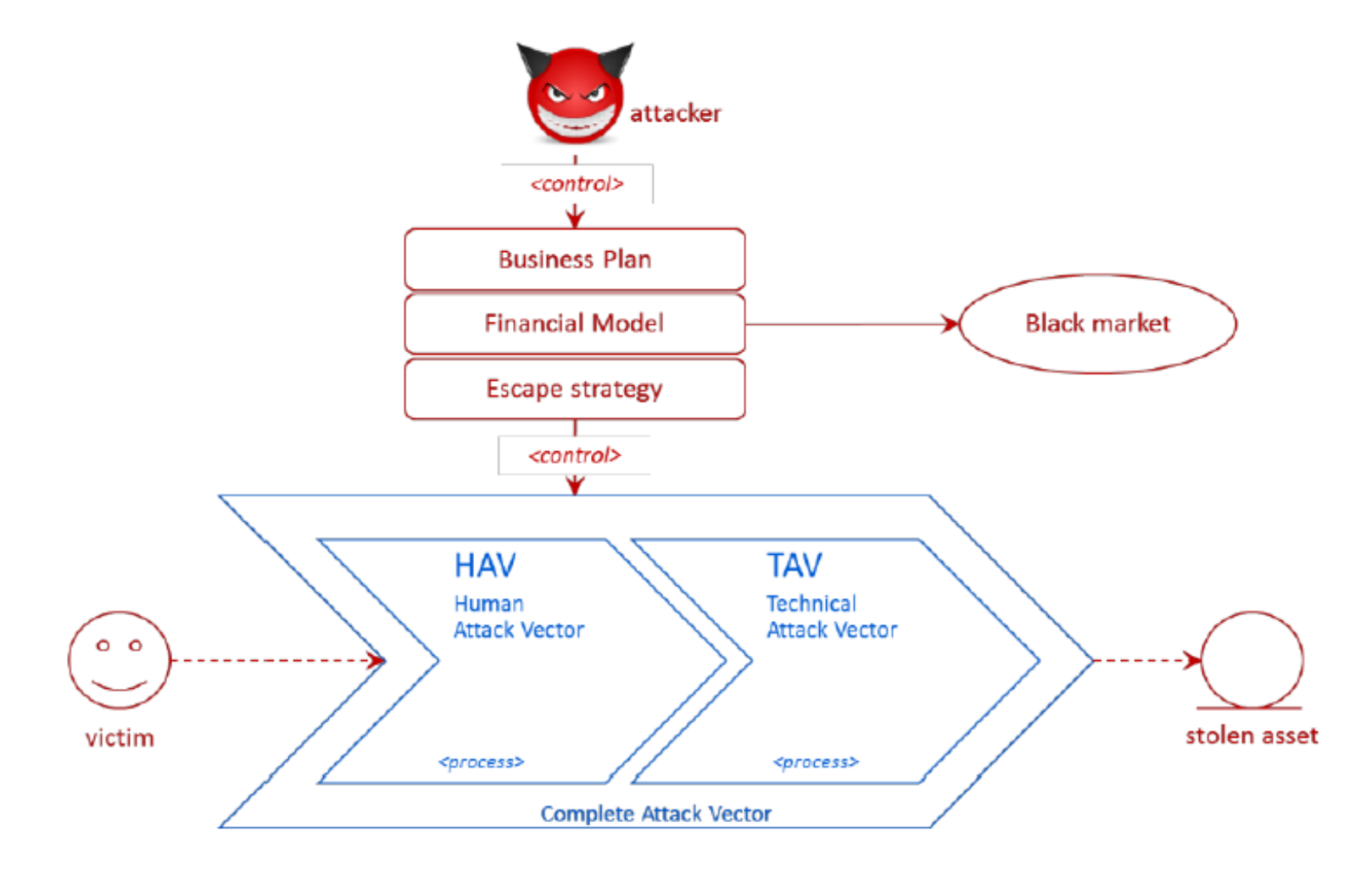
- Phishing
- Malware
- BEC

- Ransomware
- File Sharing Abuse
- Supply Chain Attacks

Angreifer fokussieren auf den Menschen als Sicherheitslücke

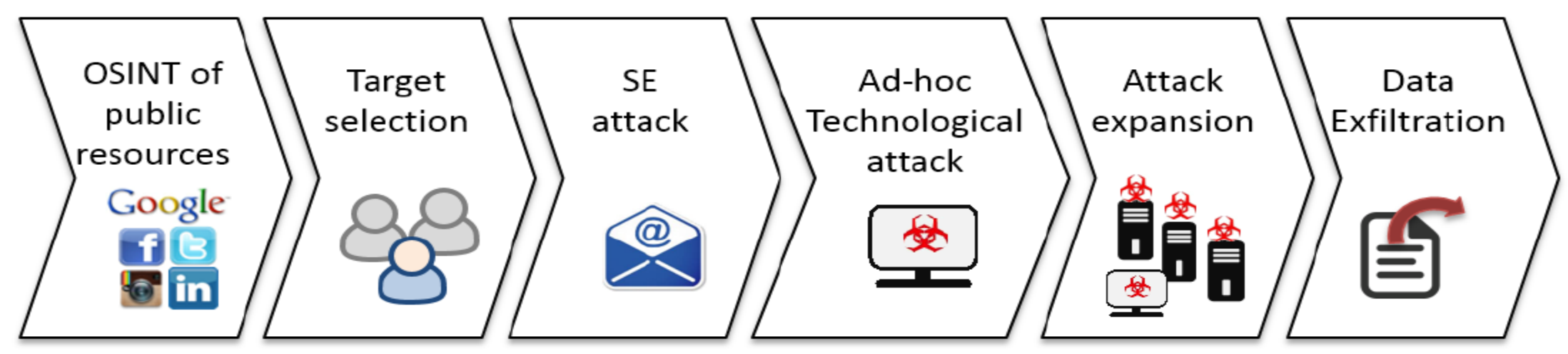


Moderne Angriffe: Human Attack Vector + Technical Attack Vector



Quelle: https://www.dogana-project.eu/

Social Engineered Attack: “Kill-Chain”



Quelle: https://www.dogana-project.eu/

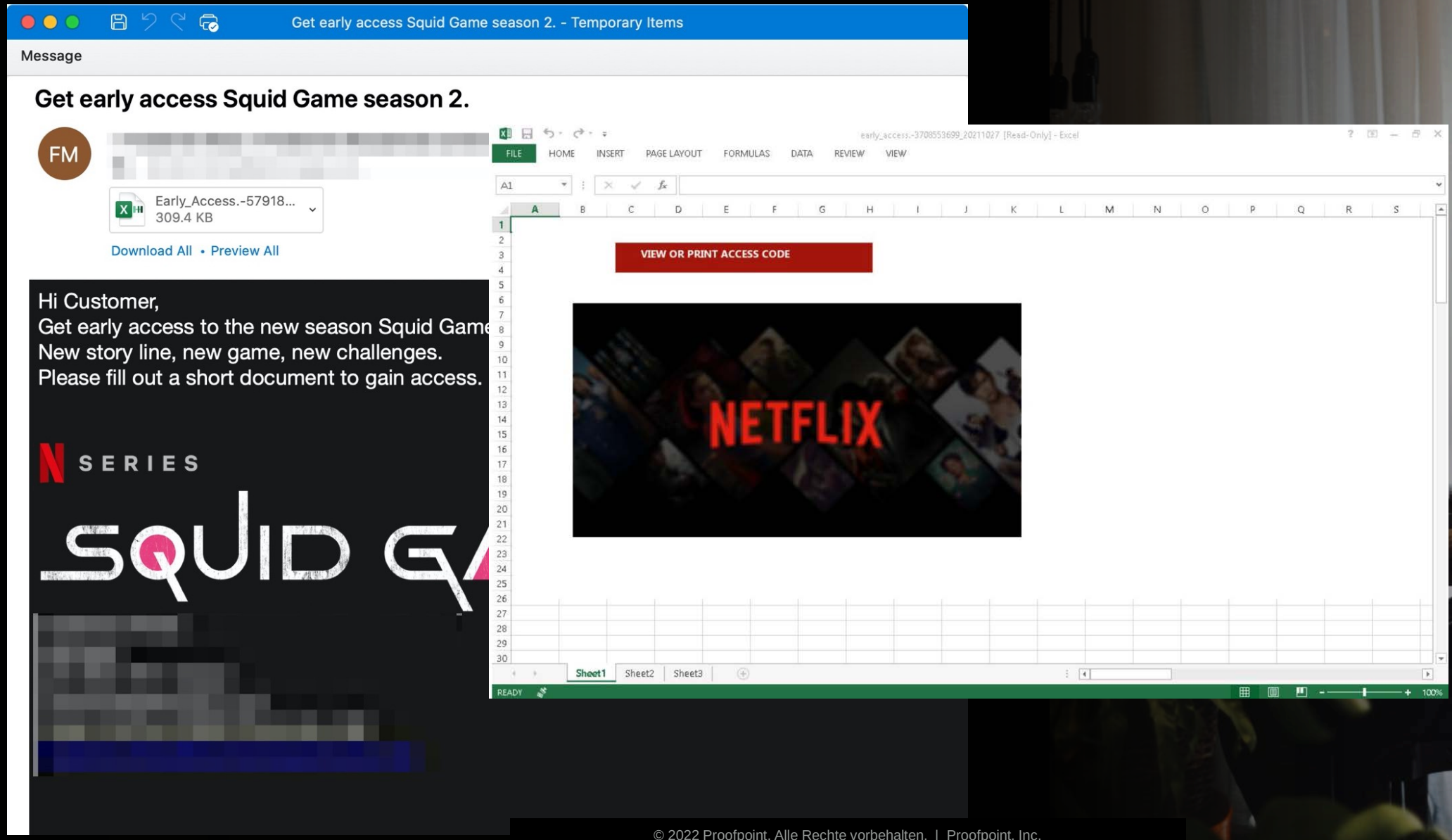
Häufige Social Engineering Taktiken:

RUNNING ATTACKER’S CODE FOR THEM

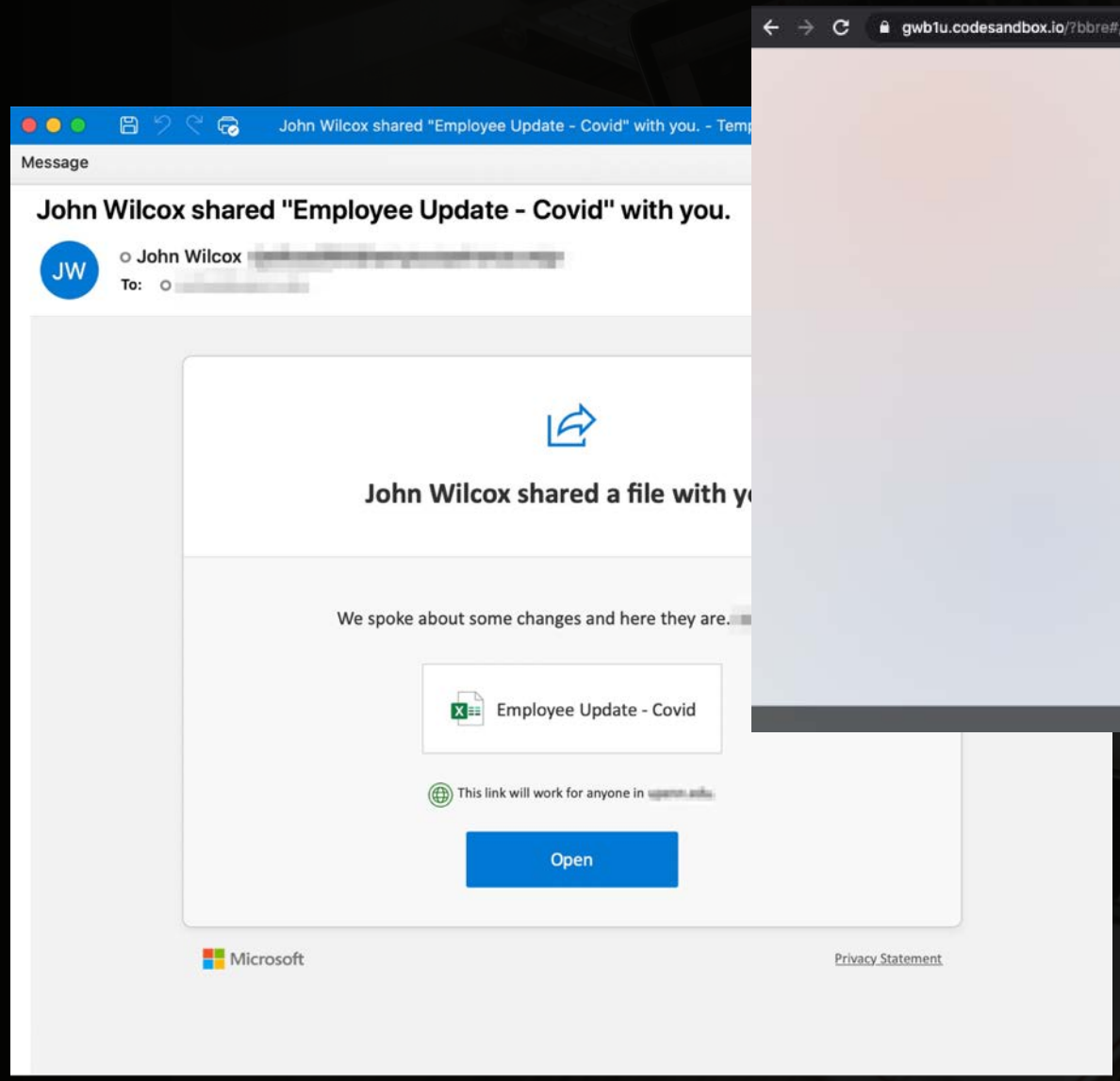
HANDING OVER CREDENTIALS TO THEM

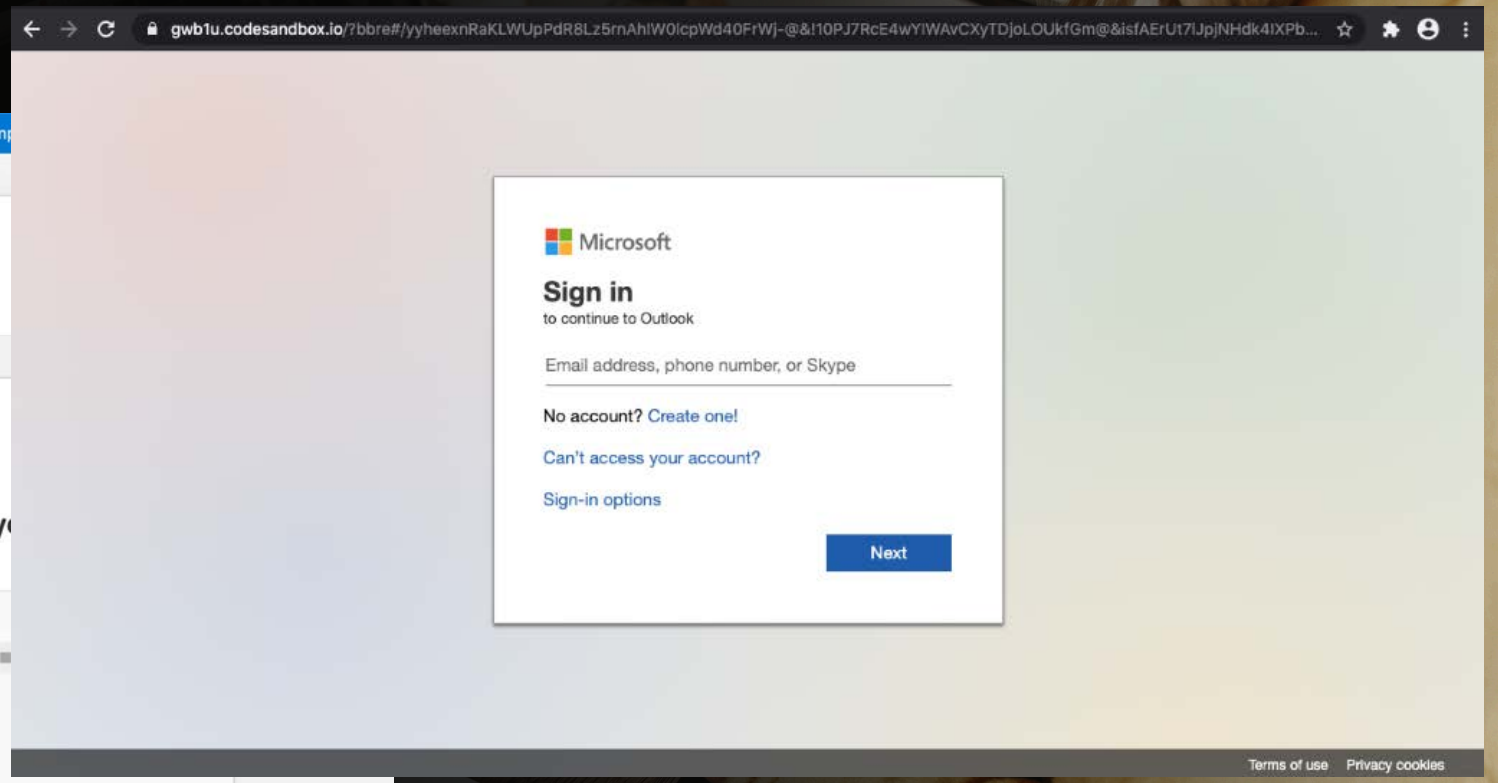
TRANSFER FUNDS OR DATA TO THEM

Starten des Schadcodes



Weitergabe von Anmeldedaten





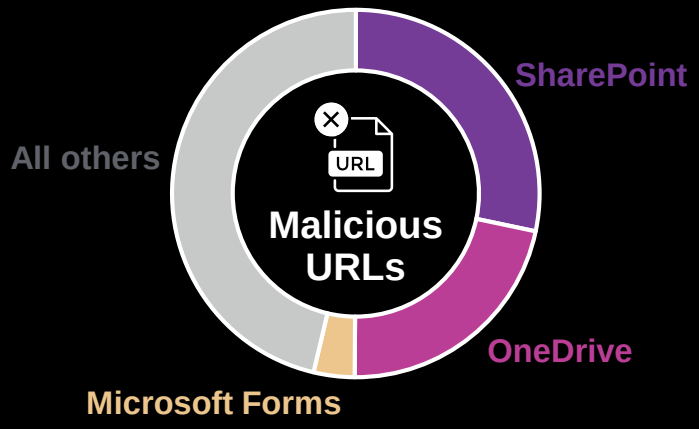
“Gut genug” ist nicht immer gut genug

Weaponizing the Cloud

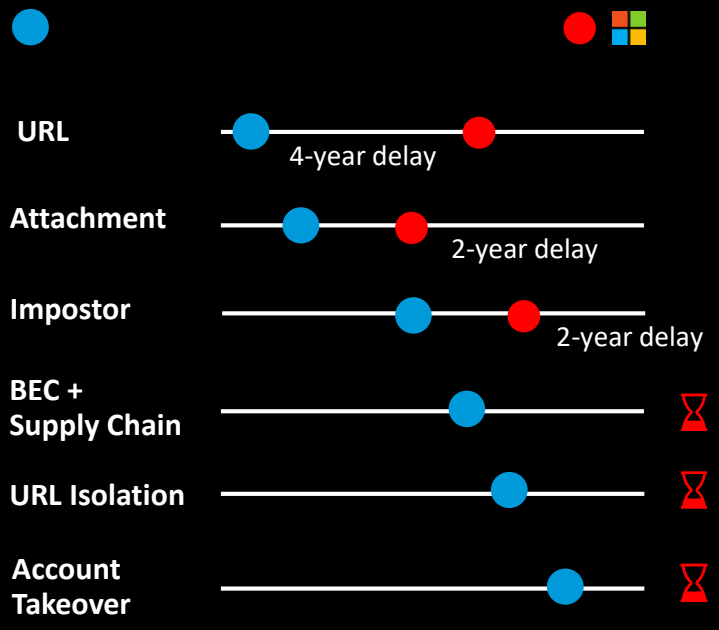
Office 365

~110M

malicious messages targeted at Proofpoint customers sent or hosted by MS Office 365 in 2020 & 2021



Microsoft Core Gaps



Security Vulnerabilities

2022:
CVE-2022-30190
aka “Follina”

RCE / ACE vulnerability in MSDT allowing to circumvent protected view. Known since March 2021.

Noch früherer Ansatz in der Angriffskette – mit E-Mail-Sicherheit

Wir sind durch **Phishing** in Ihr Netzwerk gelangt. Die E-Mail mit dem schädlichen Anhang wurde von einem Mitarbeiter geöffnet... Er wurde gebeten, das Makro im Dokument zu aktivieren, den Inhalt anzuzeigen, auf den Link zu klicken usw. #Lösung: Verhindern Sie einen solchen Angriff!
#Wie? Das überlassen wir Ihnen...

Ransomware-Gruppe Clop

Proofpoint hilft Ihnen bei der Abwehr

Die Proofpoint Threat Protection-Plattform

Echtzeit-Prävention und proaktive Maßnahmen:
Vorbereitung, Verhinderung und Erkennung der Erstinfektion

Sicheres E-Mail-Gateway

Proofpoint Email Protection

Sandbox-Analyse

Proofpoint Targeted Attack Protection (TAP)

Sensibilisierung für Sicherheit und Schulungen

Proofpoint Security Awareness Training

Behebung nach der Zustellung:
Behebung und Wiederherstellung nach lateralen Bewegungen und Persistenz

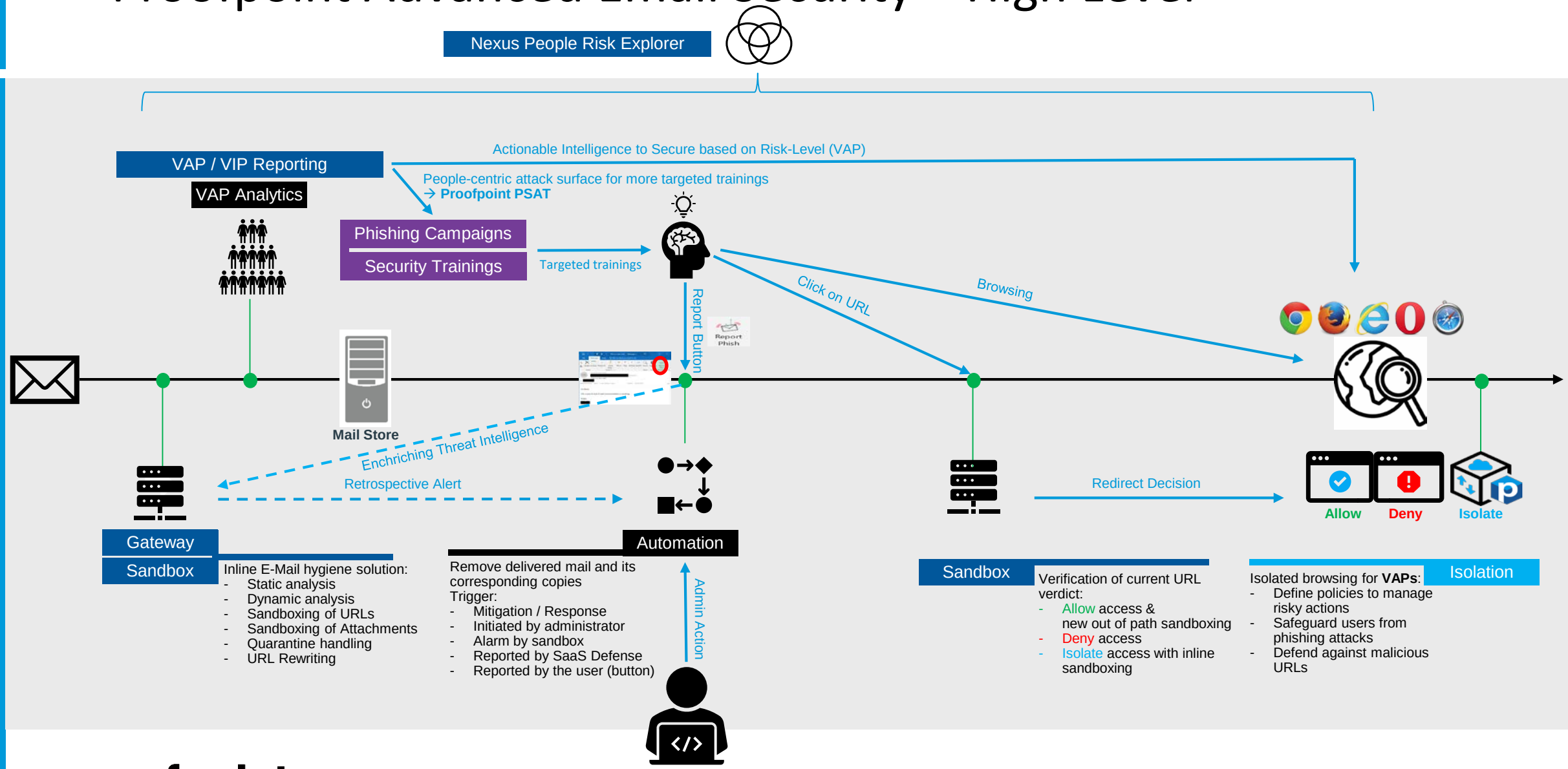
Isolierung

Proofpoint Browser Isolation

Reaktion

Proofpoint Threat Response Auto-Pull

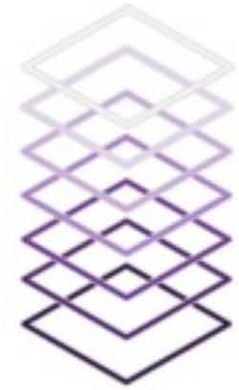
Proofpoint Advanced Email Security – High Level



proofpoint.

Proofpoint AI & ML Detection Engines vs Microsoft

Proofpoint URL Defense

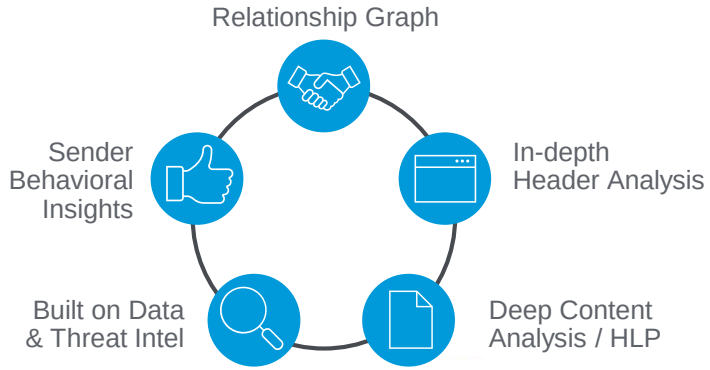


- Reputation Analysis
- Predictive Sandbox Engine
- Static Analysis
- Dynamic Analysis (URLs & files)
- ML Feedback Loop
- Automated Expert Systems
- Browser Isolation

Proofpoint Attachment Defense

- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection
- Evasion Detection
- URL Extraction
- Network & Protocol Analytics
- Ecosystem Partnerships
- ML Feedback Loop
- Automated Expert Systems

Proofpoint Supernova for BEC



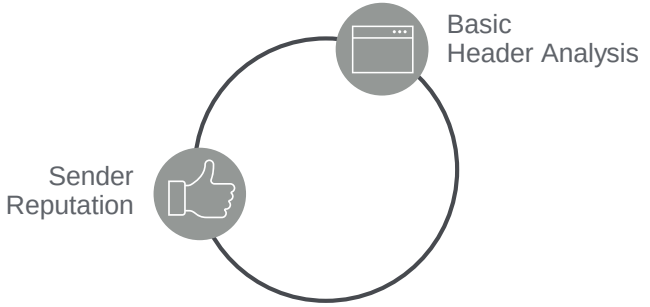
Microsoft Safe Links

- Reputation Analysis
- Static File Analysis
- Dynamic File Analysis

Microsoft Safe Attachments

- Reputation Analysis
- Password File Analysis
- Download / Redirect Following
- Macro & Script Detection

Microsoft Spoof Intelligence



proofpoint.

KI / ML basierend auf einzigartiger Sichtbarkeit

#1 DEPLOYED SOLUTION OF THE **F100, F1000, G2000**

8,000+ ENTERPRISE CUSTOMERS | **200,000+** SMB CUSTOMERS | **150+** WORLD'S LARGEST ISPS

- **2.6B+** daily emails
- **28M+** cloud accounts
- Global **threat research** and **data science** teams
- **13K+** IDS sensors
- **430M+** domains monitored
- **49B+** URLs
- **46k+** apps in catalog
- **26+** detection engines (static, ML, behavior, etc.)
- Deployed at key **internet backbones**
- **143k+** social media accounts
- **1.9B+** attachments
- **2.9K+** cloud tenants
- Tracking **100+** threat actors
- **600K+** weekly unique malware samples

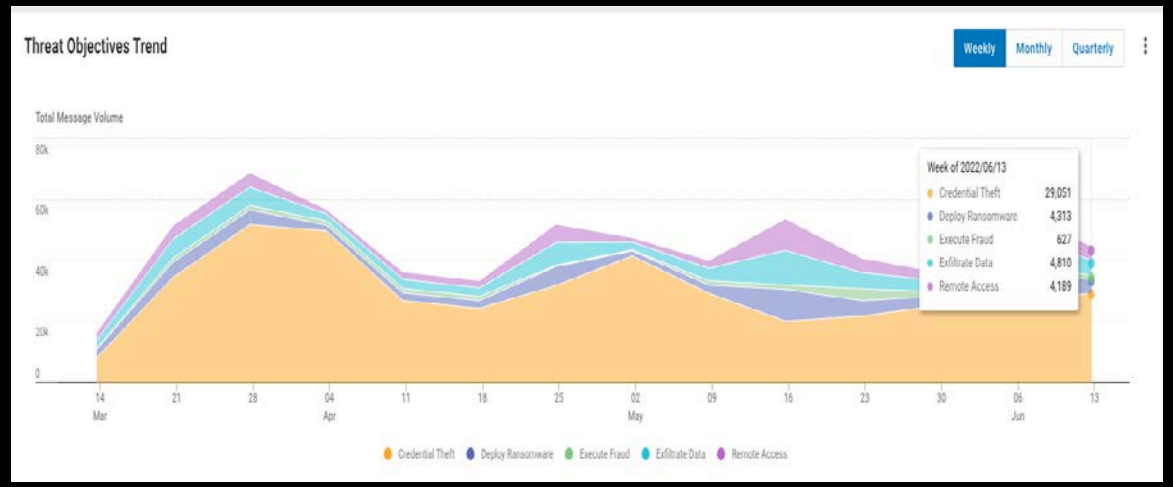
1 TRILLION+ NODE NEXUS THREAT GRAPH

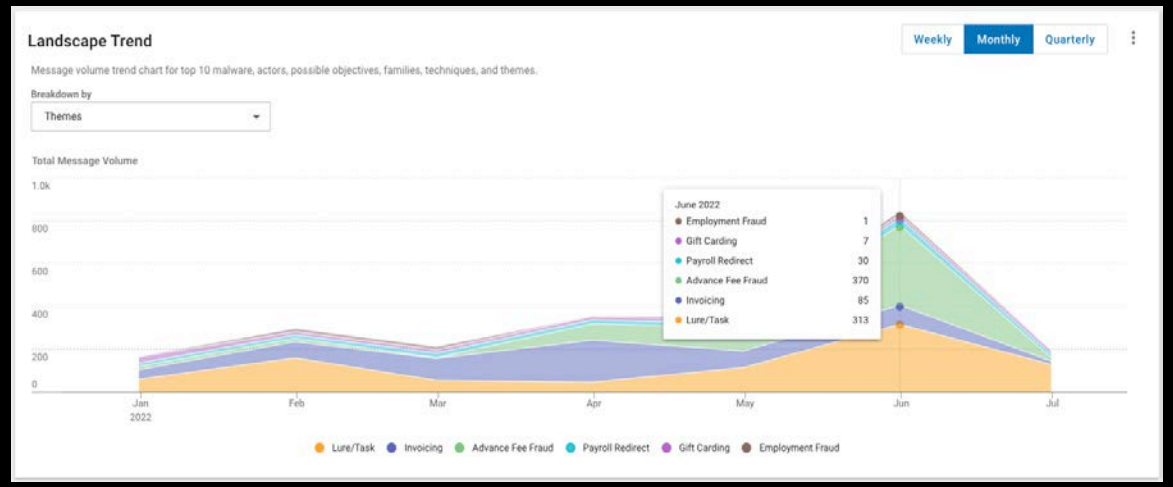
- **Impostor/BEC Detection**
- **Malicious URL/HTML/ File Detection**
- **4th Generation Cred Phish Engine**
- **AI-Generated Cloud Threat Detectors**
- **Behavioral Analysis and Engine**

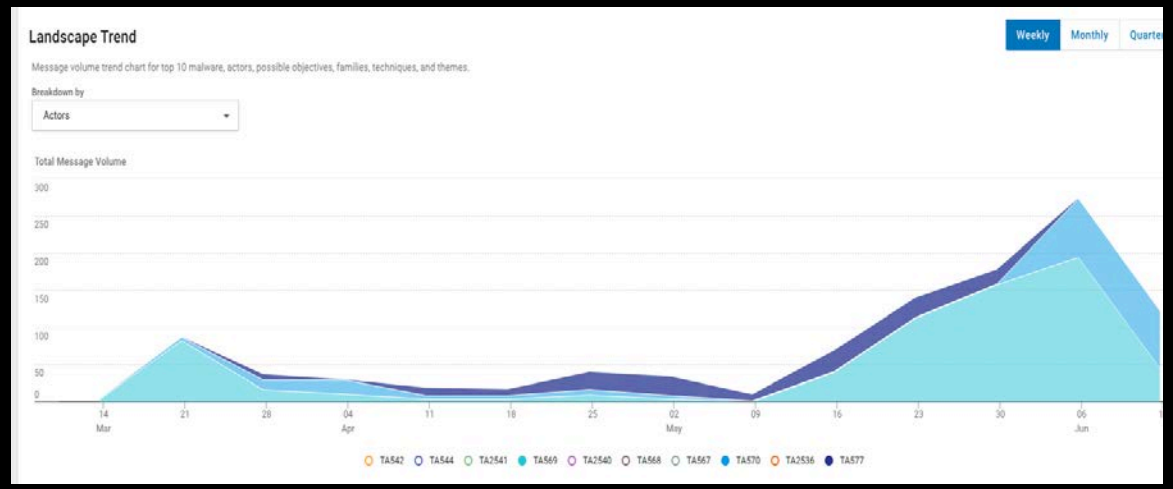
NEXUSAI: PROOFPOINT'S 4th GENERATION MACHINE LEARNING

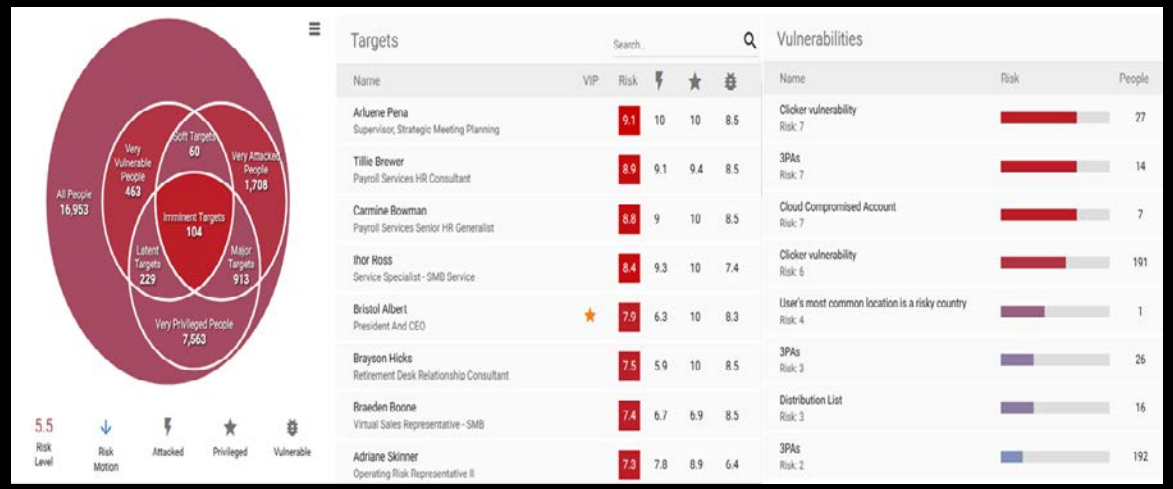
proofpoint.

Zusätzliche Visibilität durch Proofpoint

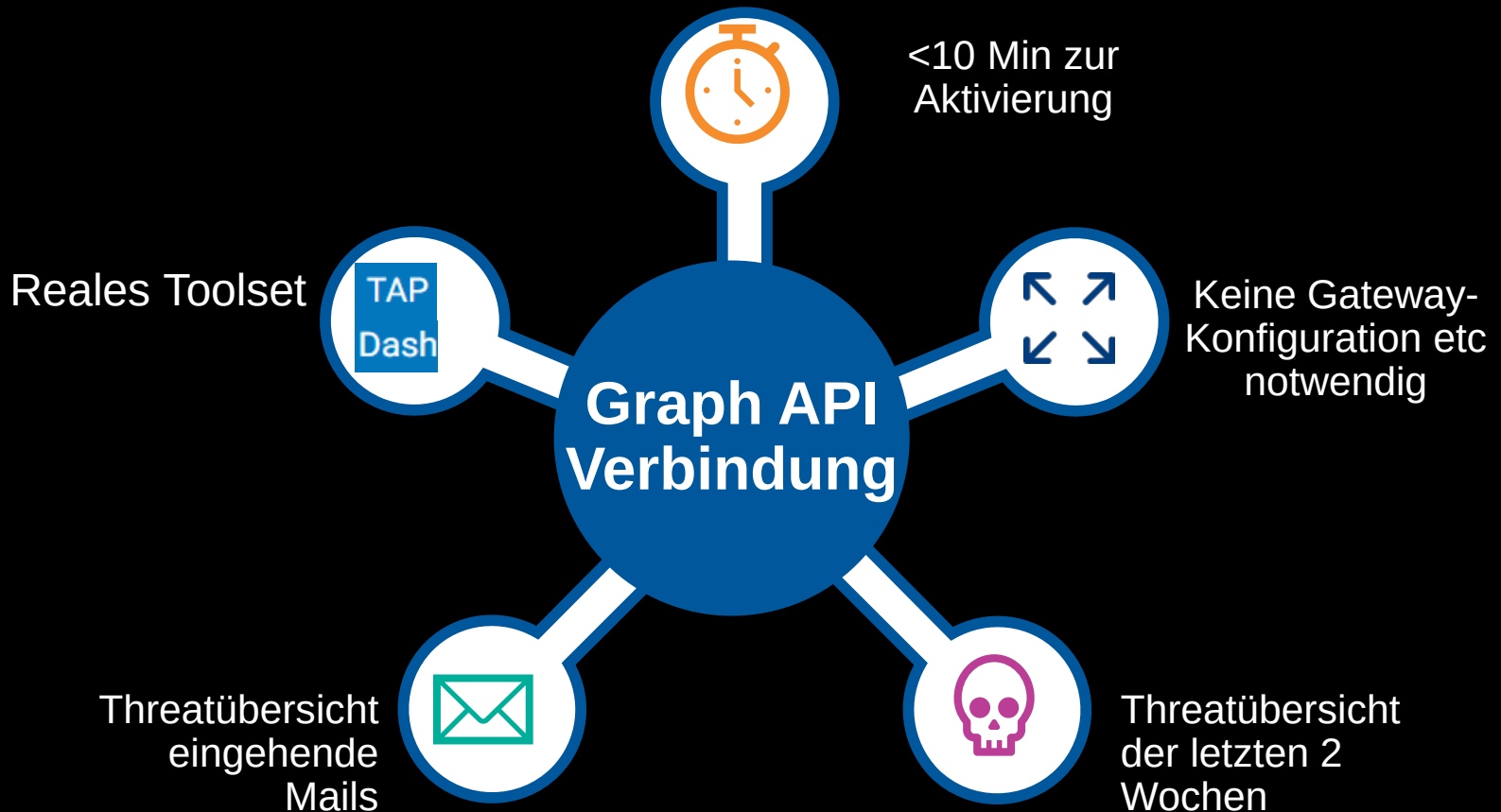








Ihr Lagebild auf Basis von Realdaten? Rapid Risk Assessment



Option für EU oder US Rechenzentren

Einfache Aktivierung

- Aktivierung mit wenigen Klicks
- Keine MX-/Konfiguraitionsänderungen
- <10 Minuten zur Aktivierung

Sicherheitsüberblick in kurzer Zeit

- 14-Tage Übersicht in die “Vergangenheit”
- < 48 Std für belastbare Daten

Zeigt Erkennungslücken von MS

- Scannen der Nachrichten in den Inboxen der Nutzer (ohne Junk Folder)
- Nachrichten im Verfügungsbereicht des Nutzers.