

Controlware Security Day 2022



A woman with blonde hair in a ponytail, wearing a red long-sleeved shirt, is looking at a computer monitor in a dimly lit office. In the background, another person is visible at a desk with a desk lamp. The scene is overlaid with a semi-transparent dark grey banner containing text.

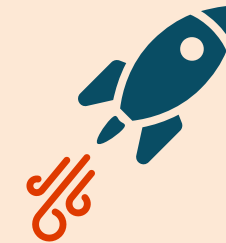
proofpoint®

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



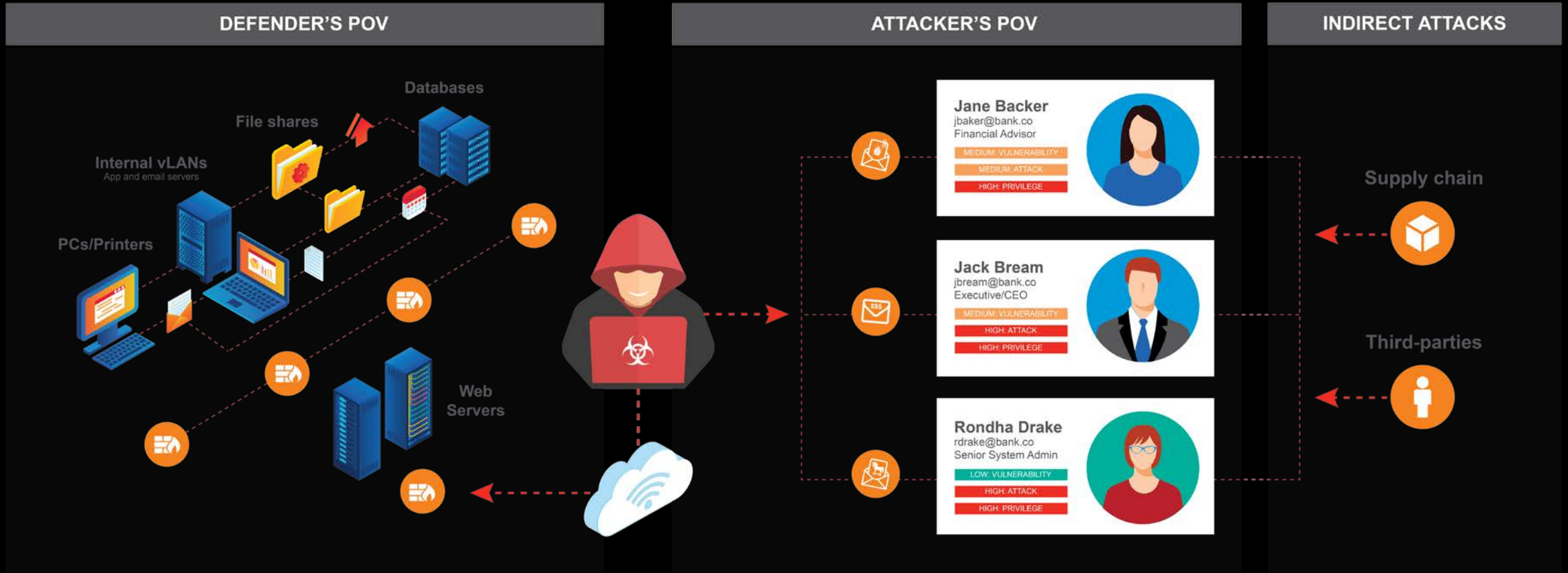
- Phishing
- Malware
- BEC



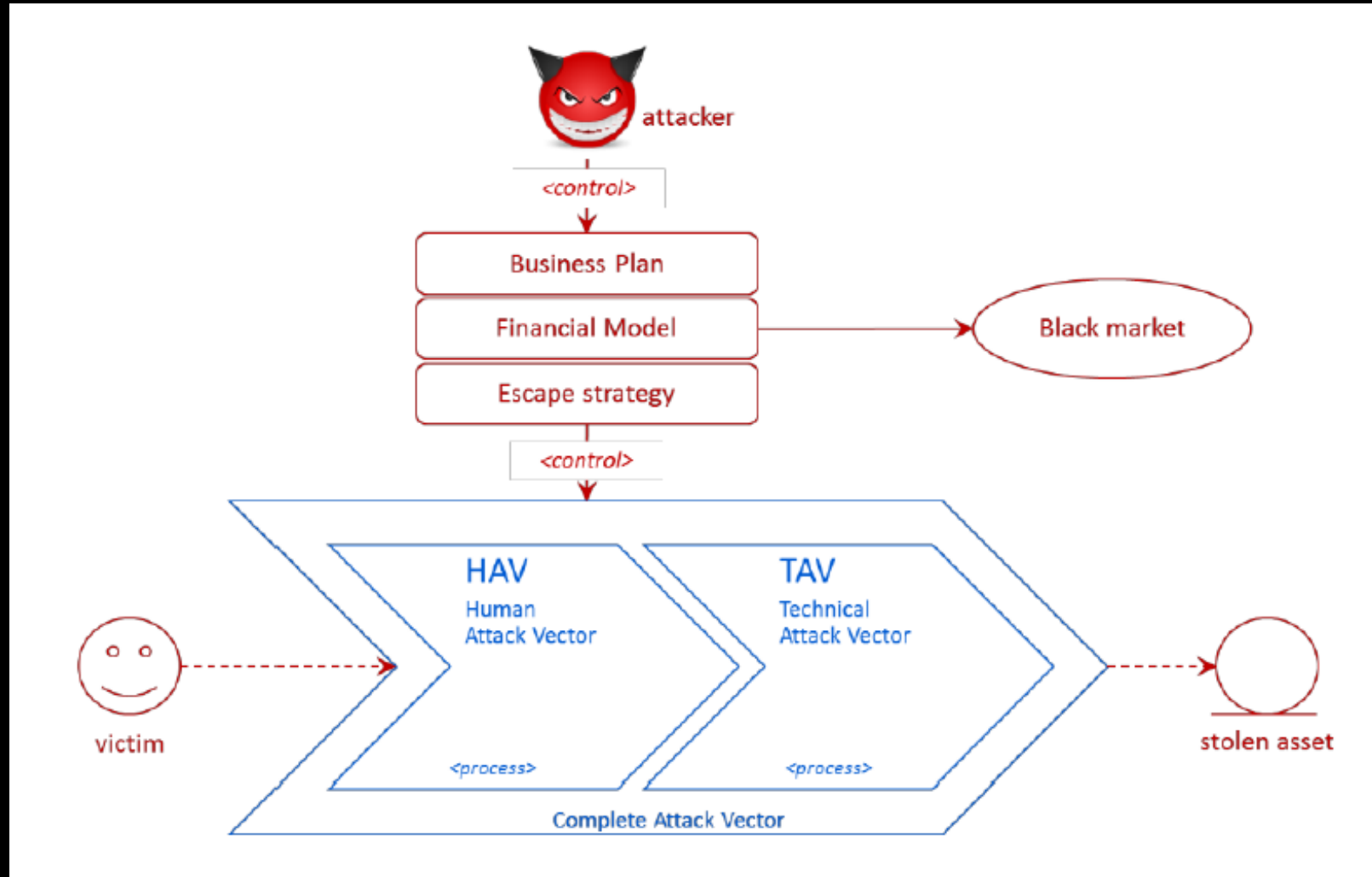
Microsoft 365

- Ransomware
- File Sharing Abuse
- Supply Chain Attacks

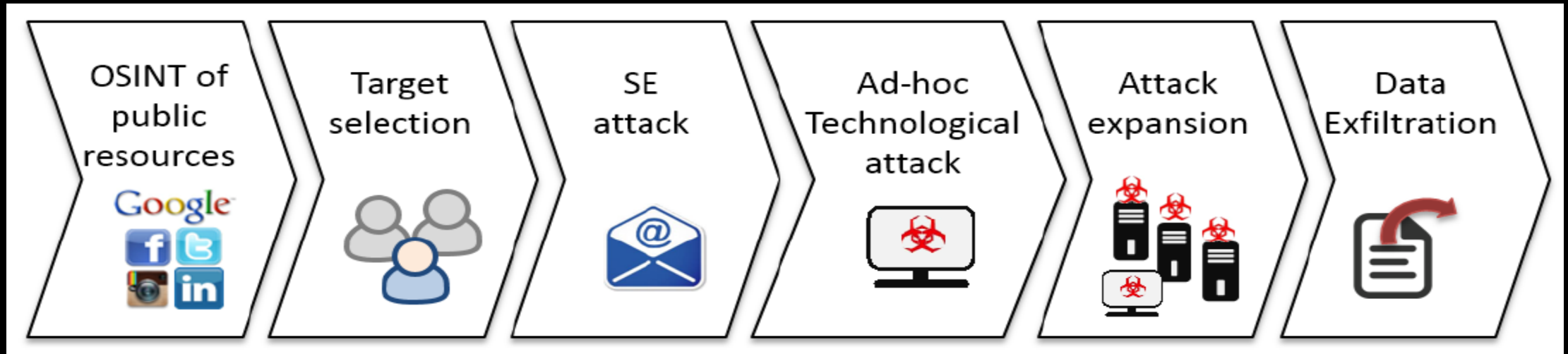
Angreifer fokussieren auf den Menschen als Sicherheitslücke



Moderne Angriffe: Human Attack Vector + Technical Attack Vector



Social Engineered Attack: “Kill-Chain”

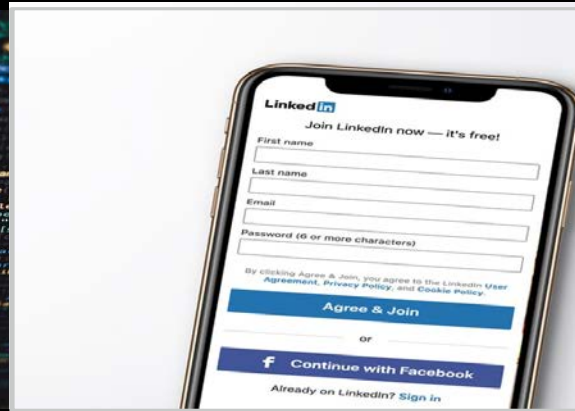


Quelle: <https://www.dogana-project.eu/>

Häufige Social Engineering Taktiken:



**RUNNING ATTACKER'S
CODE FOR THEM**



**HANDING OVER
CREDENTIALS TO THEM**



**TRANSFER FUNDS OR
DATA TO THEM**

Starten des Schadcodes

Message

Get early access Squid Game season 2.

FM


Early_Access.-57918...
309.4 KB

[Download All](#) • [Preview All](#)

Hi Customer,
Get early access to the new season Squid Game
New story line, new game, new challenges.
Please fill out a short document to gain access.

N SERIES

SQUID GAME




early_access--3708553699_20211027 [Read-Only] - Excel

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW

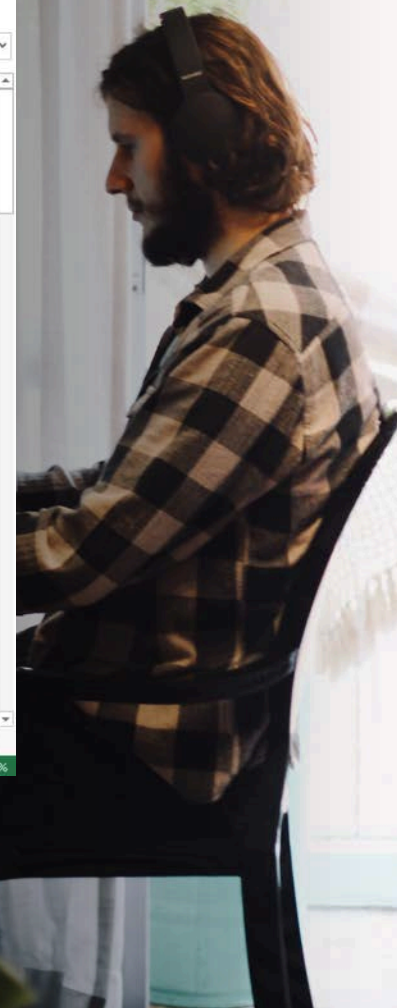
A1

VIEW OR PRINT ACCESS CODE



Sheet1 Sheet2 Sheet3



READY 100%




Weitergabe von Anmeldedaten

Message


John Wilcox shared "Employee Update - Covid" with you.



 John Wilcox
To: 




John Wilcox shared a file with you


We spoke about some changes and here they are...

 Employee Update - Covid

 This link will work for anyone in 

[Open](#)

 [Privacy Statement](#)

 Microsoft

Sign in
to continue to Outlook

Email address, phone number, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

[Next](#)

[Terms of use](#) [Privacy cookies](#)

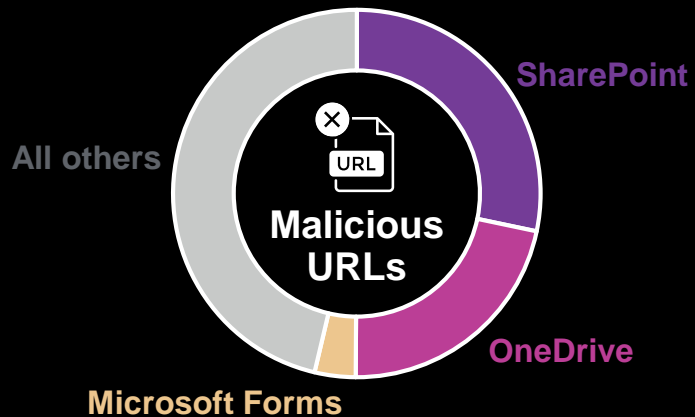
“Gut genug” ist nicht immer gut genug

Weaponizing the Cloud

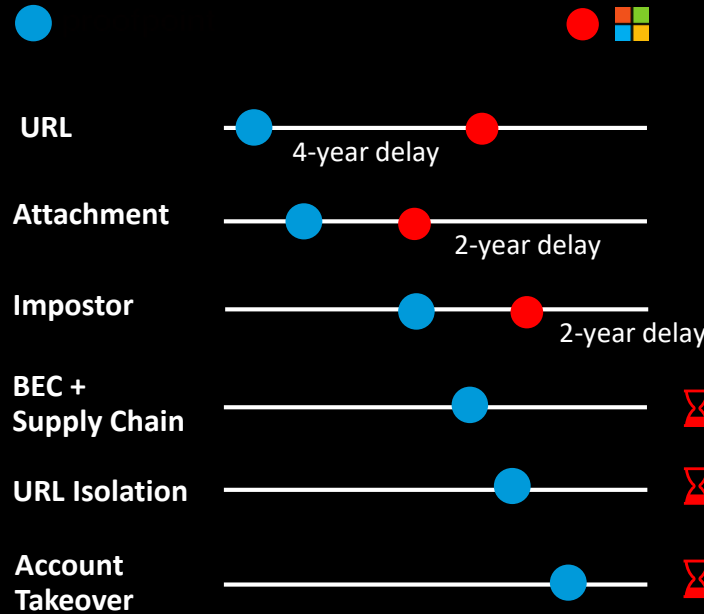


~110M

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



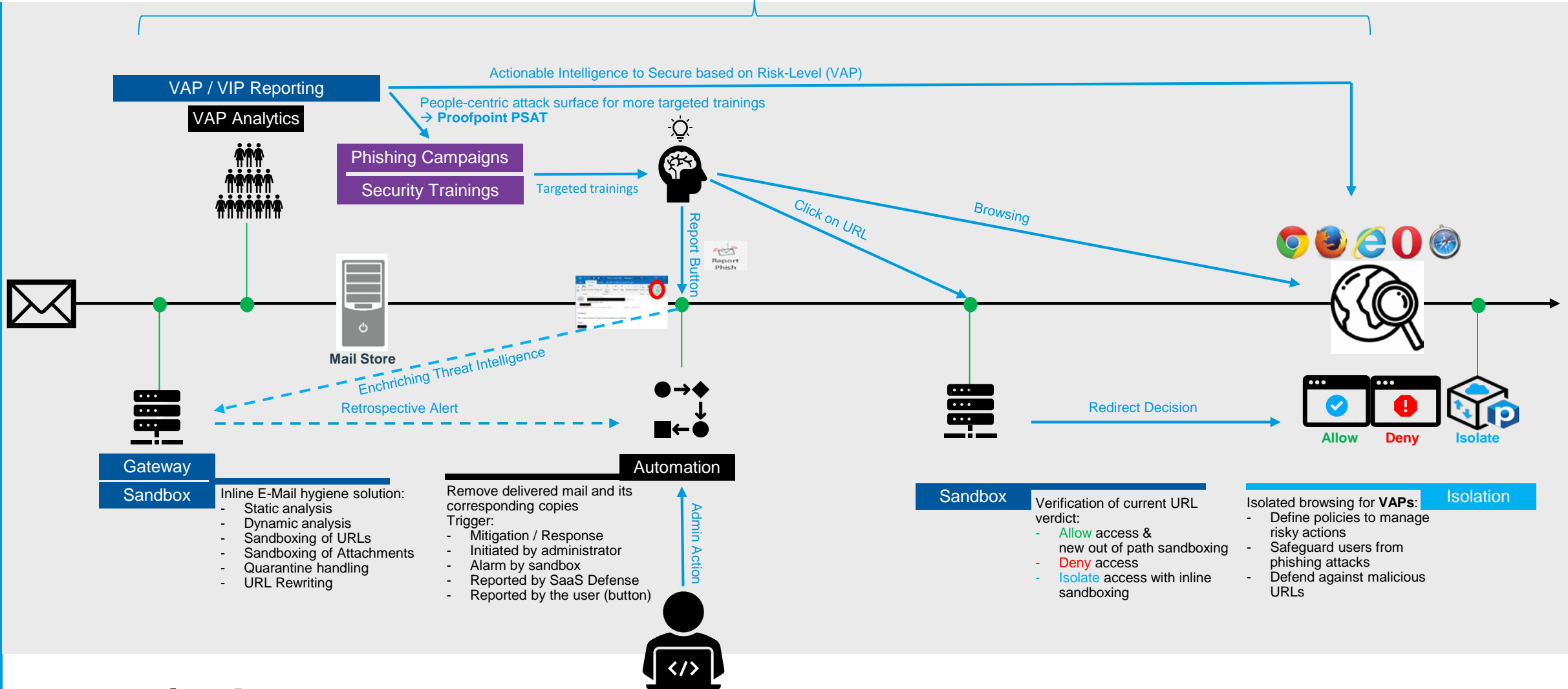
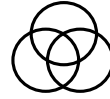
Reaktion



Proofpoint Threat Response Auto-Pull

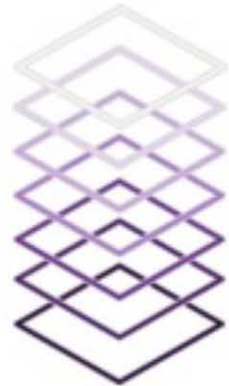
Proofpoint Advanced Email Security – High Level

Nexus People Risk Explorer



Proofpoint AI & ML Detection Engines vs Microsoft

Proofpoint URL Defense



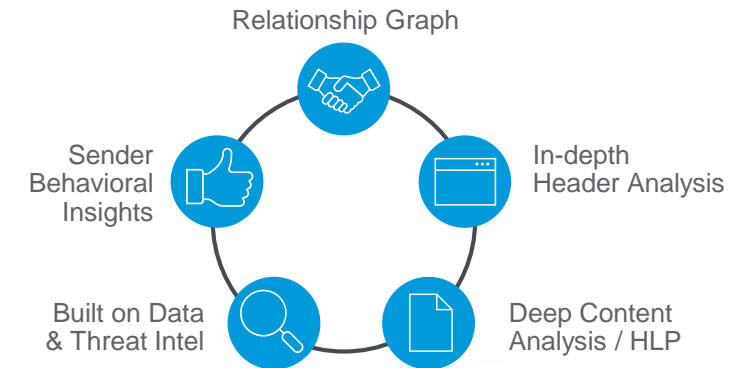
- Reputation Analysis
- Predictive Sandbox Engine
- Static Analysis
- Dynamic Analysis (URLs & files)
- ML Feedback Loop
- Automated Expert Systems
- Browser Isolation

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



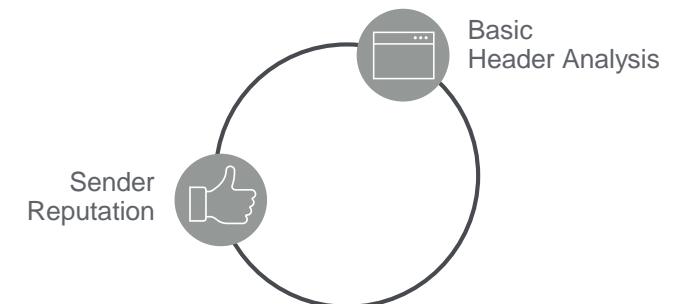
- Reputation Analysis
- Static File Analysis
- Dynamic File Analysis

Microsoft Safe Attachments



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

Microsoft Spoof Intelligence



KI / ML basierend auf einzigartiger Sichtbarkeit



#1 DEPLOYED SOLUTION OF THE F100, F1000, G2000

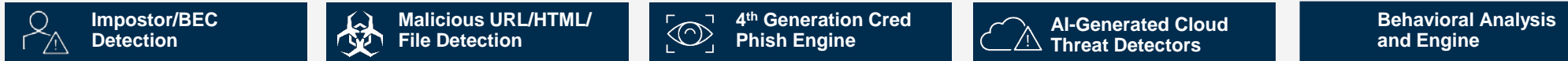
8,000+ ENTERPRISE CUSTOMERS

200,000+ SMB CUSTOMERS

150+ WORLD'S LARGEST ISPS

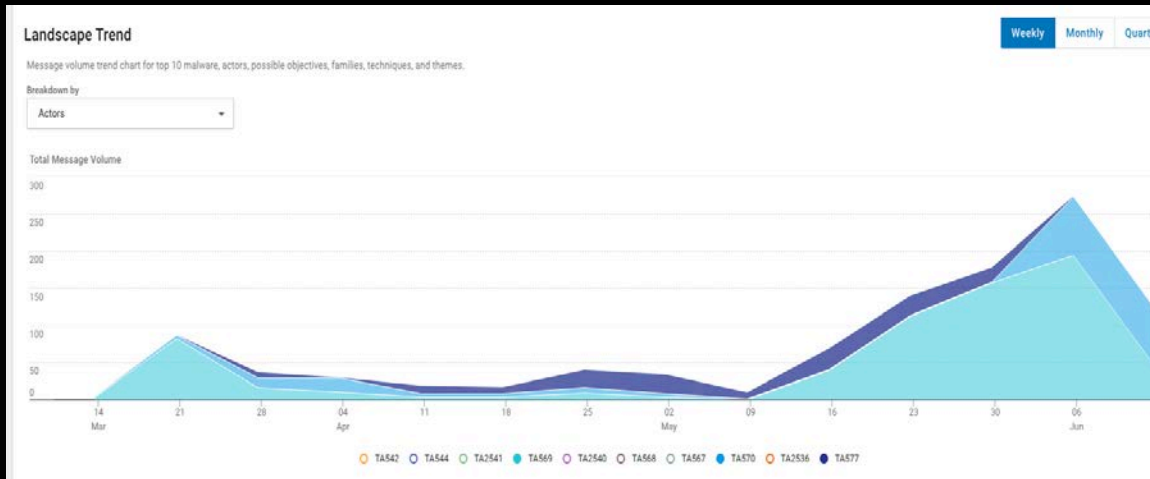
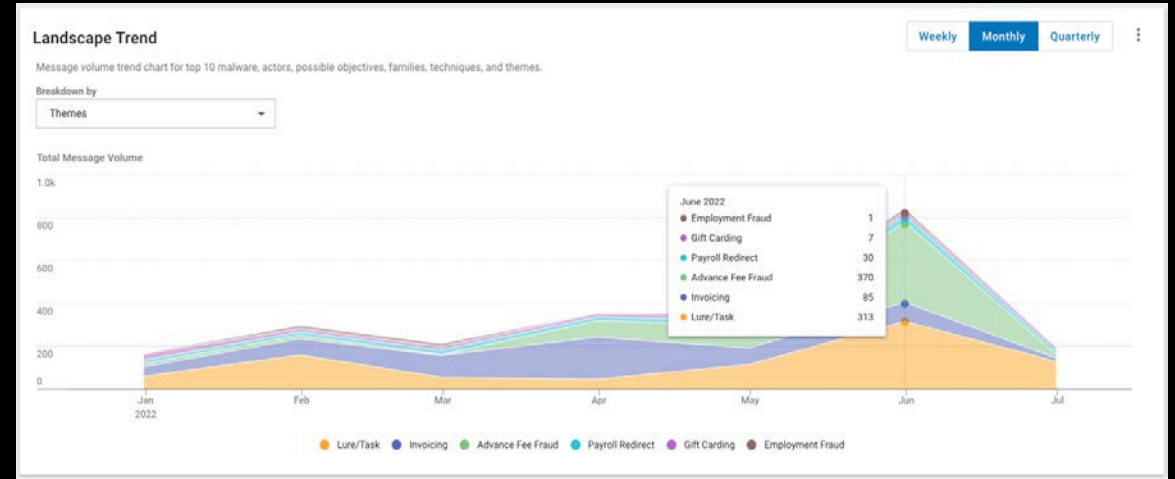
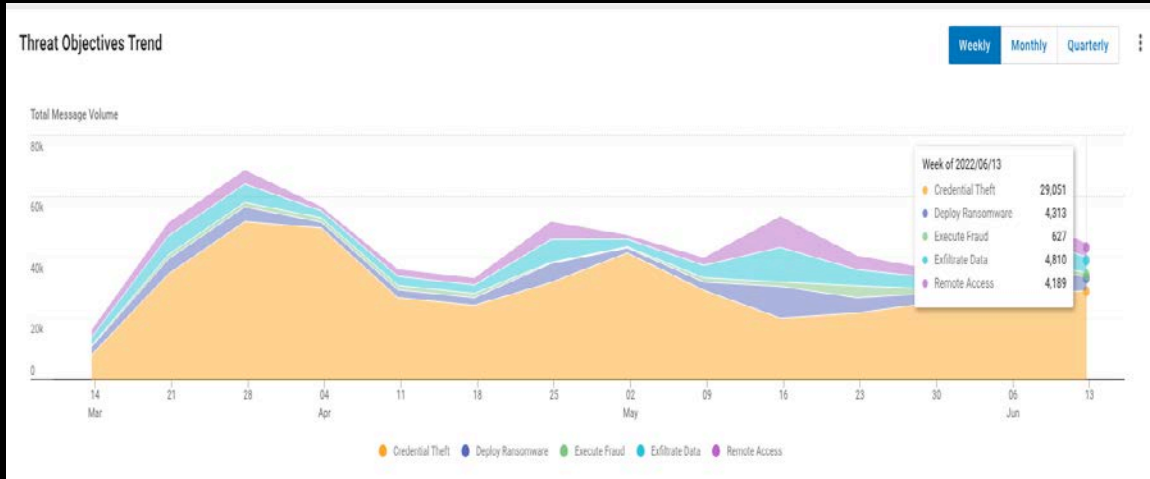


1 TRILLION+ NODE NEXUS THREAT GRAPH



NEXUSAI: PROOFPOINT'S 4th GENERATION MACHINE LEARNING

Zusätzliche Visibilität durch Proofpoint



5.5 Risk Level

↓ Risk Motion

⚡ Attacked

★ Privileged

🛡️ Vulnerable

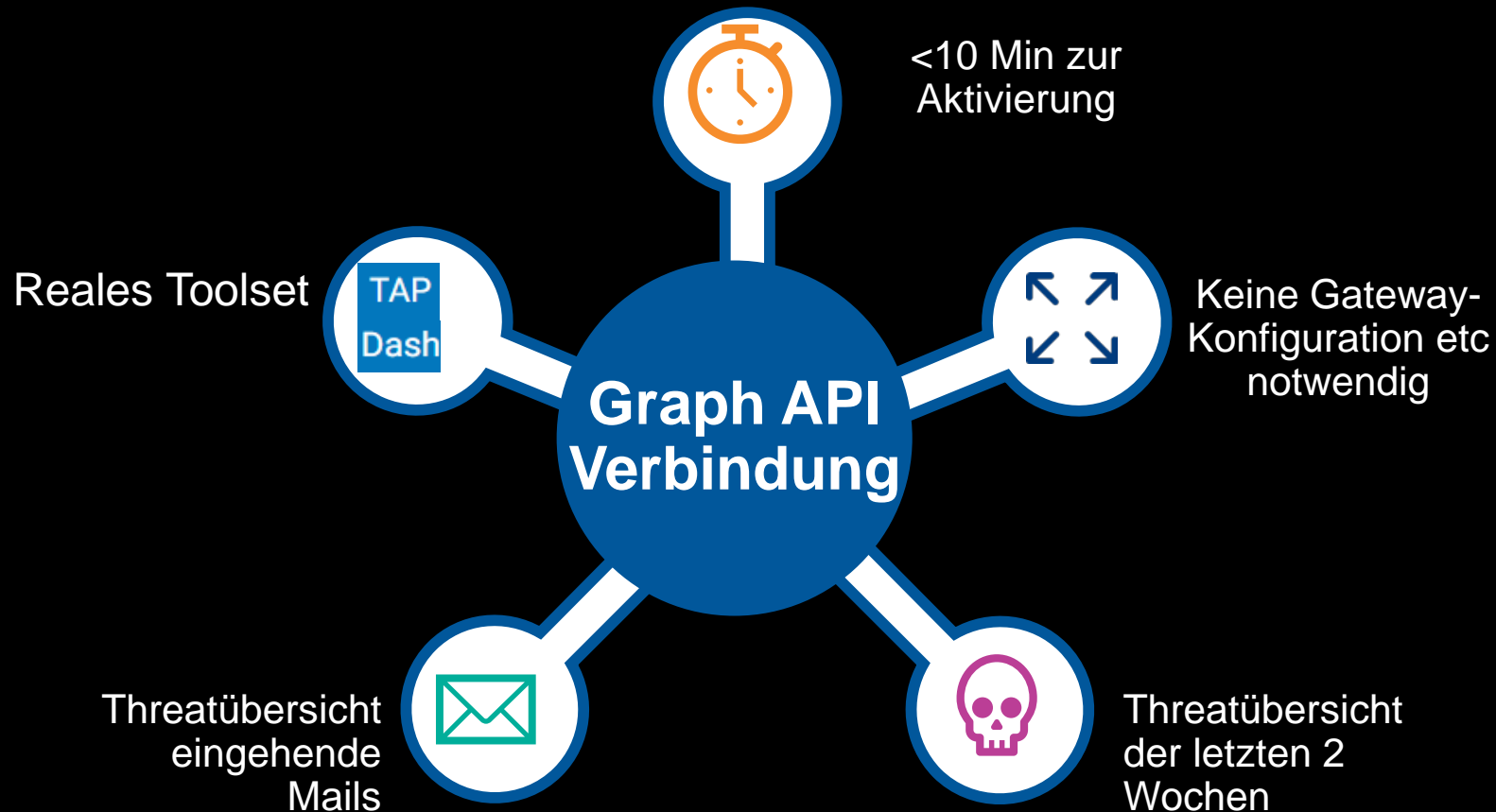
Targets

Name	VIP	Risk	⚡	★	🛡️
Arlene Pena Supervisor, Strategic Meeting Planning		9.1	10	10	8.5
Tillie Brewer Payroll Services HR Consultant		8.9	9.1	9.4	8.5
Carmine Bowman Payroll Services Senior HR Generalist		8.8	9	10	8.5
Ihor Ross Service Specialist - SMB Service		8.4	9.3	10	7.4
Bristol Albert President And CEO	★	7.9	6.3	10	8.3
Brayson Hicks Retirement Desk Relationship Consultant		7.5	5.9	10	8.5
Braeden Boone Virtual Sales Representative - SMB		7.4	6.7	6.9	8.5
Adriane Skinner Operating Risk Representative II		7.3	7.8	8.9	6.4

Vulnerabilities

Name	Risk	People
Clicker vulnerability Risk 7	██████████	27
3PAs Risk 7	██████████	14
Cloud Compromised Account Risk 7	██████████	7
Clicker vulnerability Risk 6	██████████	101
User's most common location is a risky country Risk 4	██████████	1
3PAs Risk 3	██████████	26
Distribution List Risk 3	██████████	16
3PAs Risk 2	██████████	192

Ihr Lagebild auf Basis von Realdaten? Rapid Risk Assessment



Option für EU oder US Rechenzentren

Einfache Aktivierung

- Aktivierung mit wenigen Klicks
- Keine MX-/Konfigurationsänderungen
- <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 Verfügungsbereich des Nutzers.



proofpoint®