


# SZA
# System zur Angriffserkennung

Olaf Müller-Haberland
Lead Auditor


©TEHTRIS

FACE THE UNPREDICTABLE

# Agenda

Ausgangslage 01

02 Bausteine des SZAs

Aufgepasst! 03


©TEHTRIS




# 01

# Ausgangslage


©TEHTRIS

# Bedrohungslage

International Politics

German Politics

ISO27001/TISAX

BSI

KRITIS, BAIT, ….

Datenschutz




KRIM-Invasion

Turkey

China, Taiwan

Critical Infrastructure

100 Milliarden Paket

kaspersky

Automatische Angrifferkennung

IT-Sicherheitsgesetz

B3S-Papers

KWG §25 | MaRisk | KRITIS 1.0 | BAIT | VAIT | KAIT | BAIT 2.0 | KRITIS 2.0 = SZA | NIS2

BDSG

DSGVO 24/25/28 (BDSG §76)

Bußgeldkatalog

GeschGehG

Fachkräftemangel bei Unternehmen, Behörden, Partner, MSSPs, …

2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | … 2024

EPP (Antivirus) & Firewall

SIEM

EDR / NDR (NTA)

XDR

MDR/SOC Services

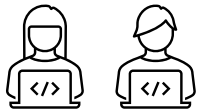
**TEHTRIS XDR Platform**



©TEHTRIS

# Ausgangslage

## Betreiber einer kritischen Infrastruktur (Energie)



Kleine bis mittlere IT-Abteilung (wenig Ressourcen)



ISO 27001 zertifiziert



KRITIS => BSI SZA (System zur Angriffserkennung)


©TEHTRIS

# Ausgangslage

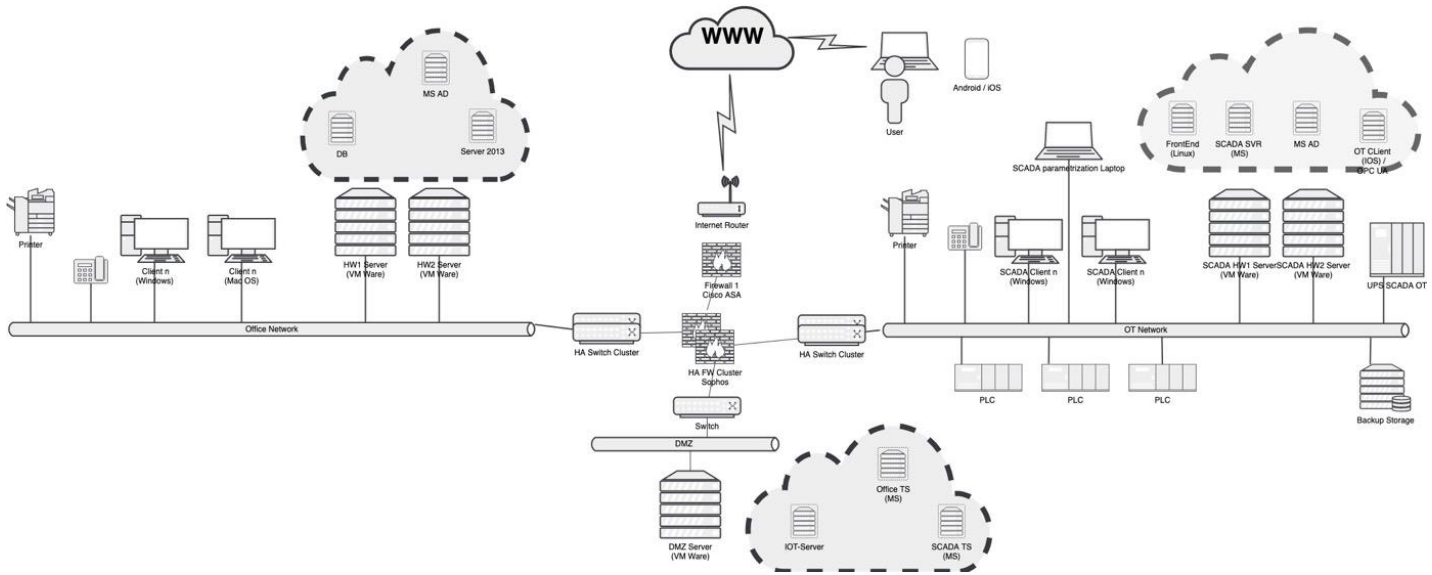
## Betreiber einer kritischen Infrastruktur (Energie)

**Bestand:**

- Endpoint-Security Lösung implementiert (bedingt gepflegt)
- New Generation Firewall (in der Teststellung)

**Offen:**

- SIEM (Log-Überwachung)
- EDR? NDR? MDR?





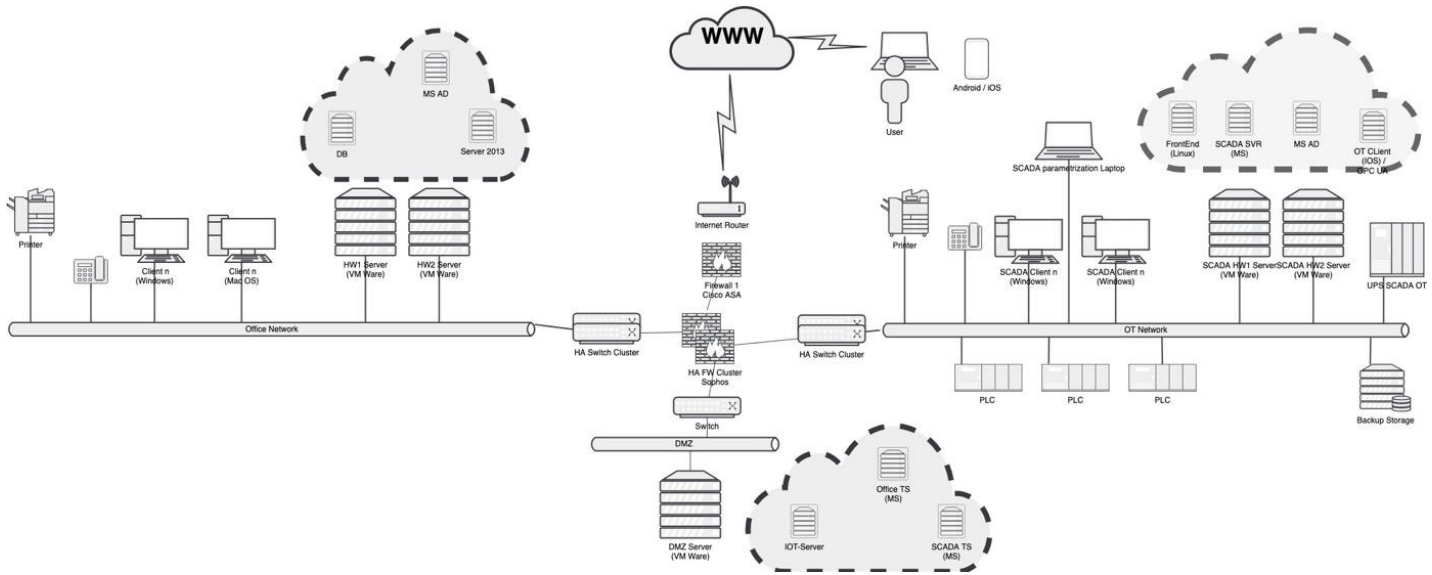
©TEHTRIS

# Ausgangslage

## Betreiber einer kritischen Infrastruktur (Energie)

**Herausforderungen des Kunden:**

- Pflege und Bedienung von min. 5-10 Security Tools
- Bei gleicher Personalstärke





©TEHTRIS



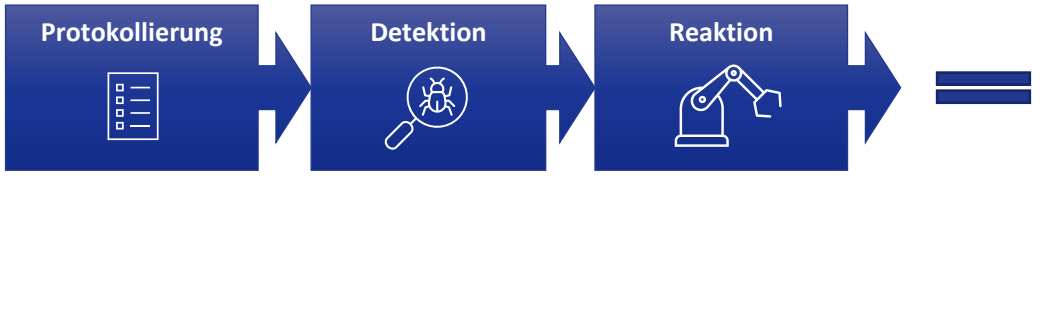

# 02

# SZA (System zur Angriffserkennung)


©TEHTRIS

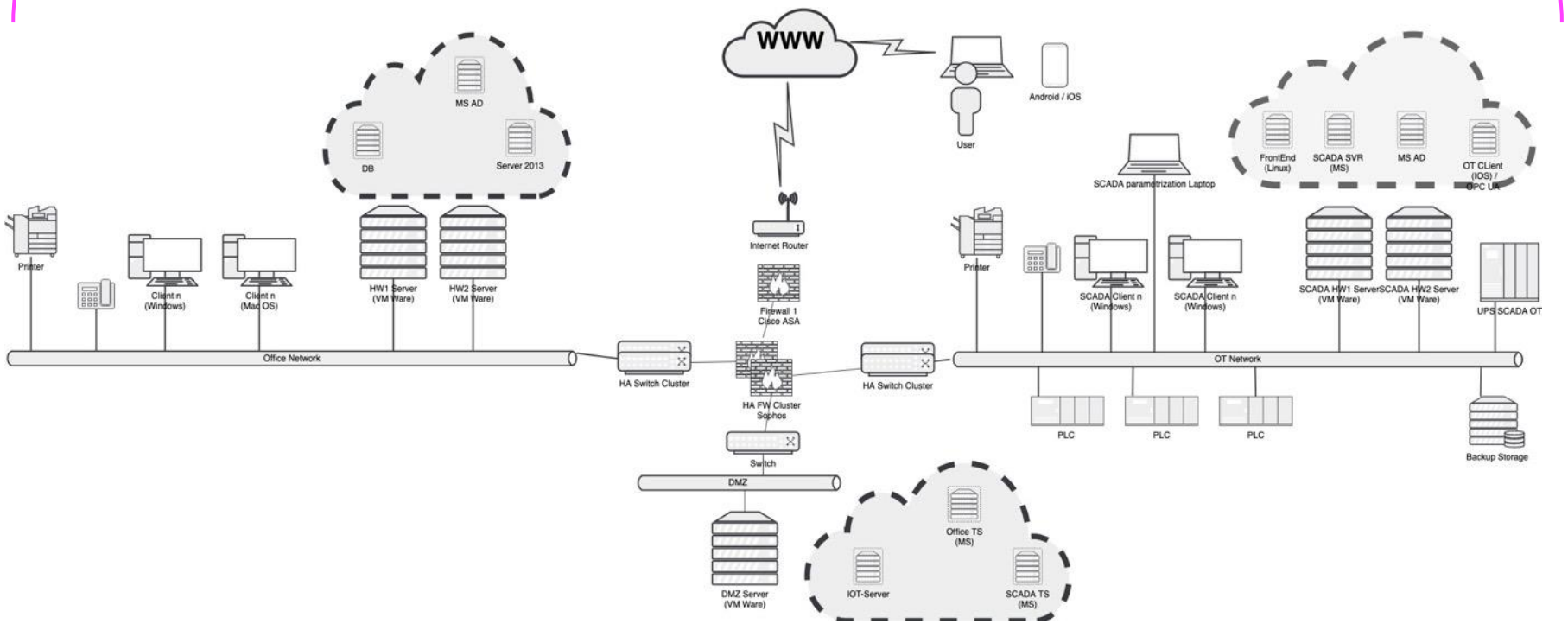
# System zur Angriffserkennung

## Ausgangslage











©TEHTRIS

# System zur Angriffserkennung

## MITRE ATT&CK





©TEHTRIS

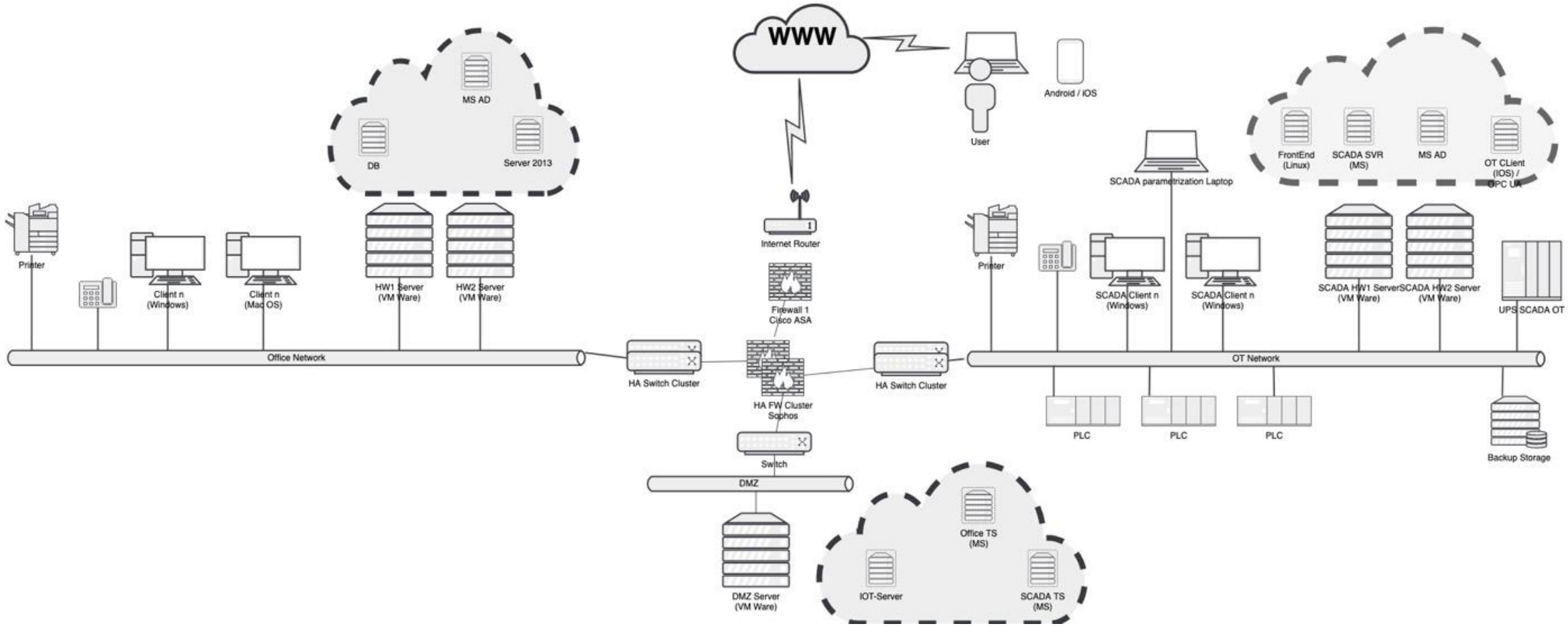
# Zentrale holistische Lösung zur IT-/OT-Security

## IT/OT Infrastruktur

Dateien

Anwendungen / Prozesse

Logdateien





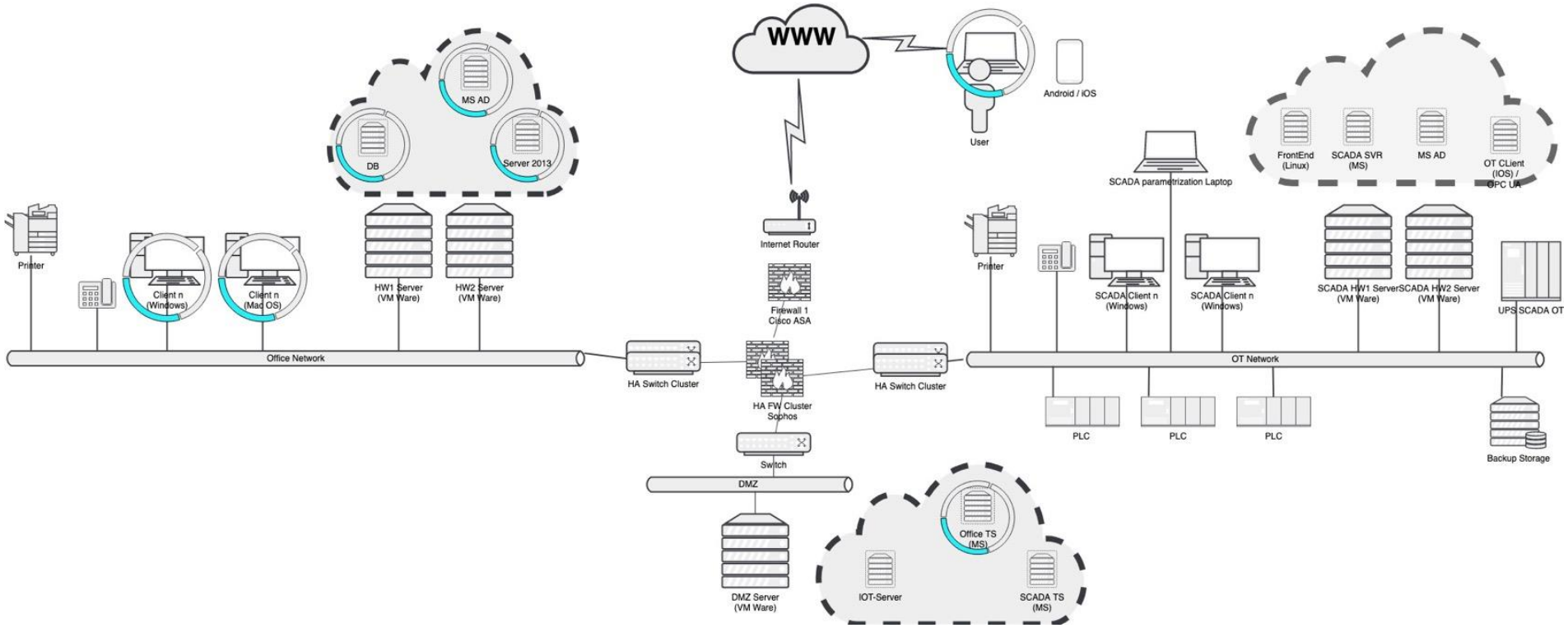
©TEHTRIS

# Zentrale holistische Lösung zur IT-/OT-Security

## EPP (Endpoint Protection Platform)

EPP

Datei





©TEHTRIS

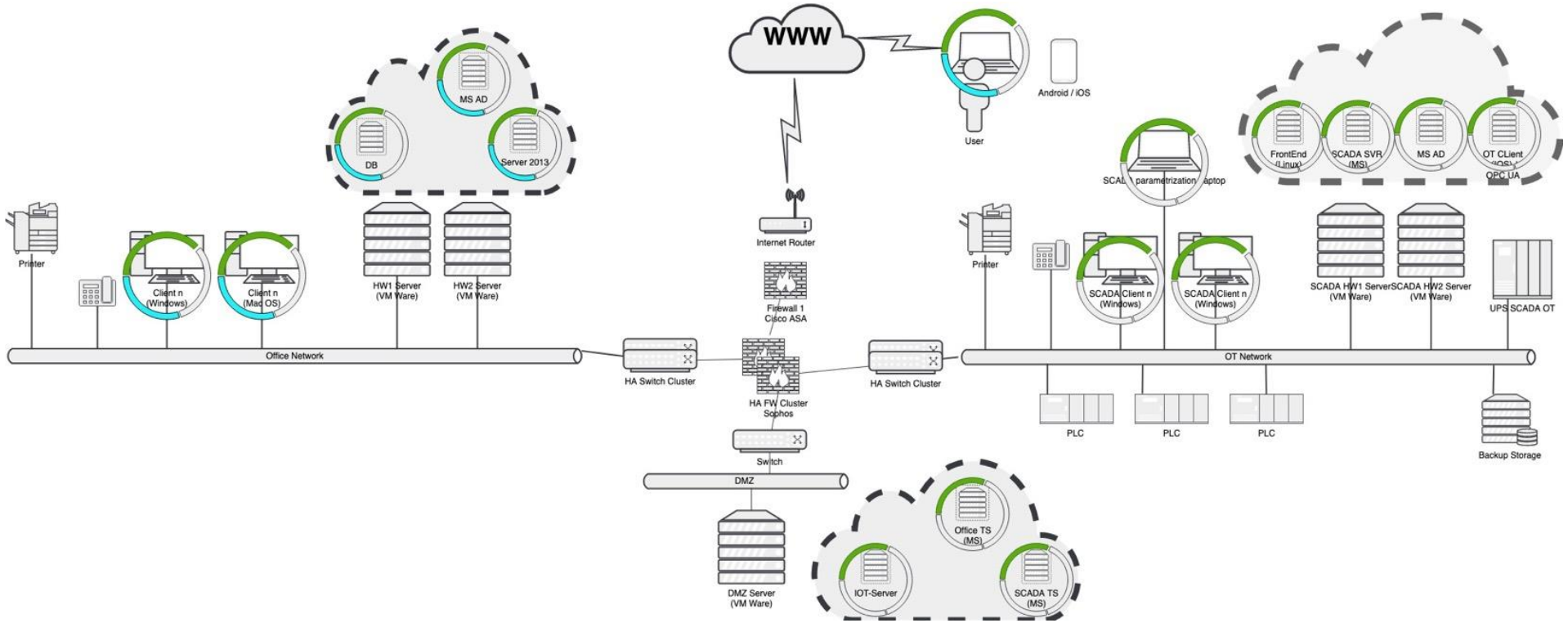
# Zentrale holistische Lösung zur IT-/OT-Security

## EDR (Endpoint Detection Responce)

EDR

Dateien

Anwendungen / Prozesse





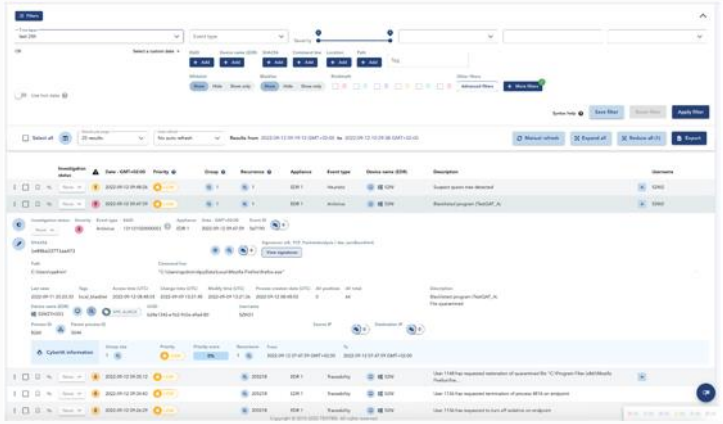
©TEHTRIS

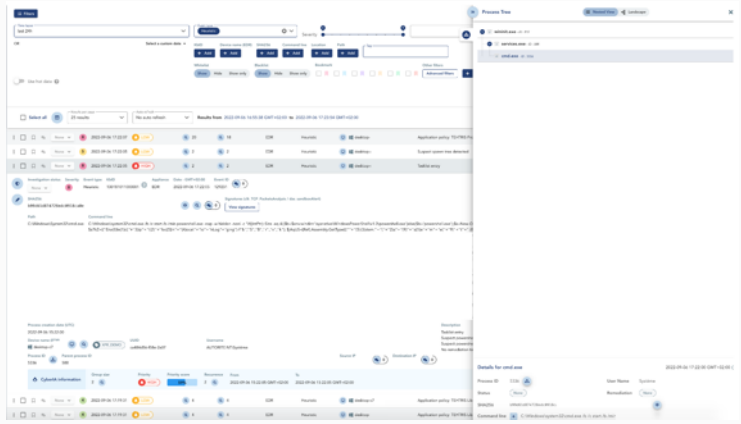
# System zur Angriffserkennung

## EDR (Endpoint Detection Responce)

### DETEKTION VON BEDROHUNGEN

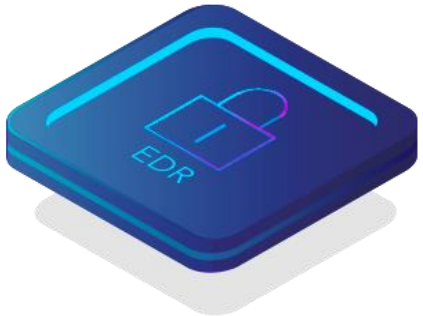
- Echtzeit Überwachung und Monitoring aller Arbeitsplätze und Server
- Scannen der Festplatte und die Verarbeitung der gewonnenen Informationen durch unsere KI CYBERIA und unsere CTI-Bedrohungsdatenbank
- Investigation & IOC Hunting
- Blacklisting & whitelisting Funktionen
- Endpoint vulnerability und Compliance Audits
- Shadow IT: Aufspüren ungeschützter Rechner
- SOC in the Box: Intelligente und automatisierte Alarmverarbeitung
- Powershell attacks detection und Überwachung der Windows-Registrierung





### ANGRIFFE NEUTRALISIEREN

- Automatische und detaillierte Analyse von bekannten und unbekannten Bedrohungen
- Sofortige Blockierung von Bedrohungen und Neutralisierung
- Malware-Quarantäne
- Dashboard und Berichtswesen





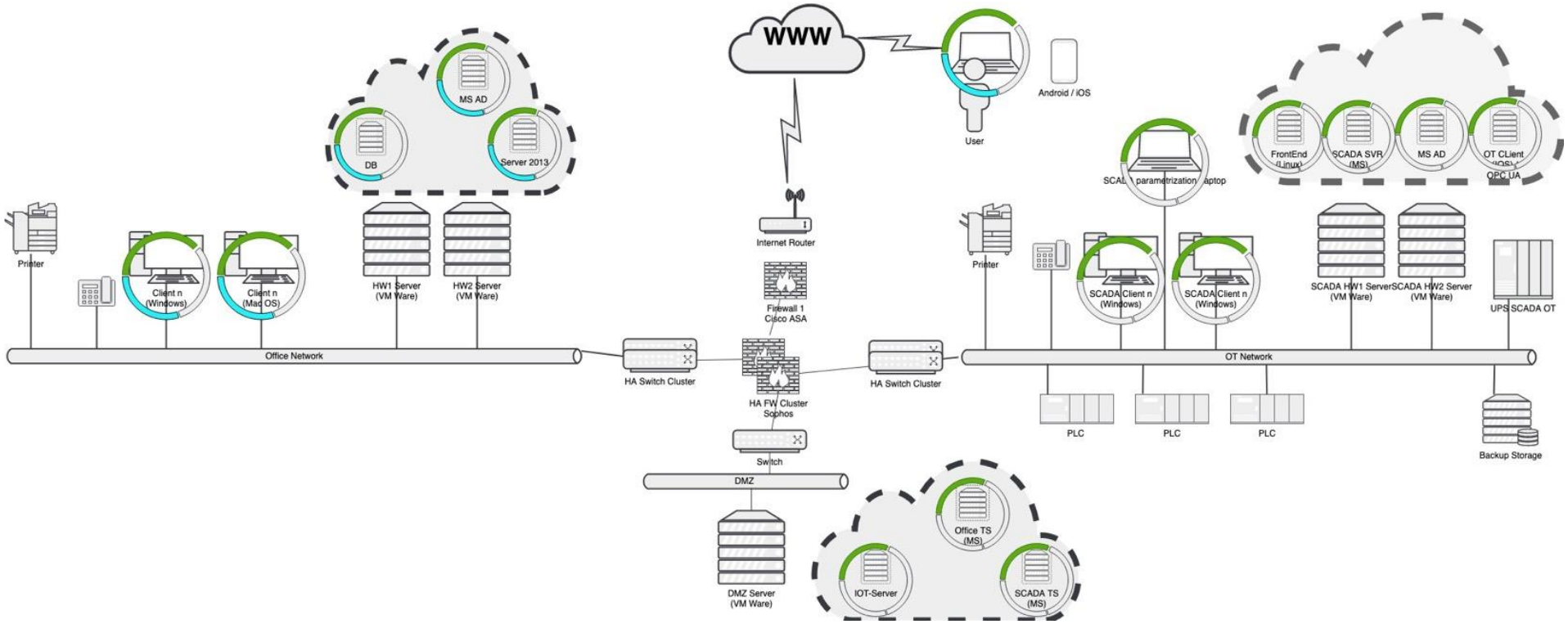
©TEHTRIS

# Zentrale holistische Lösung zur IT-/OT-Security

Dateien

Anwendungen / Prozesse

Logdateien





©TEHTRIS

# System zur Angriffserkennung

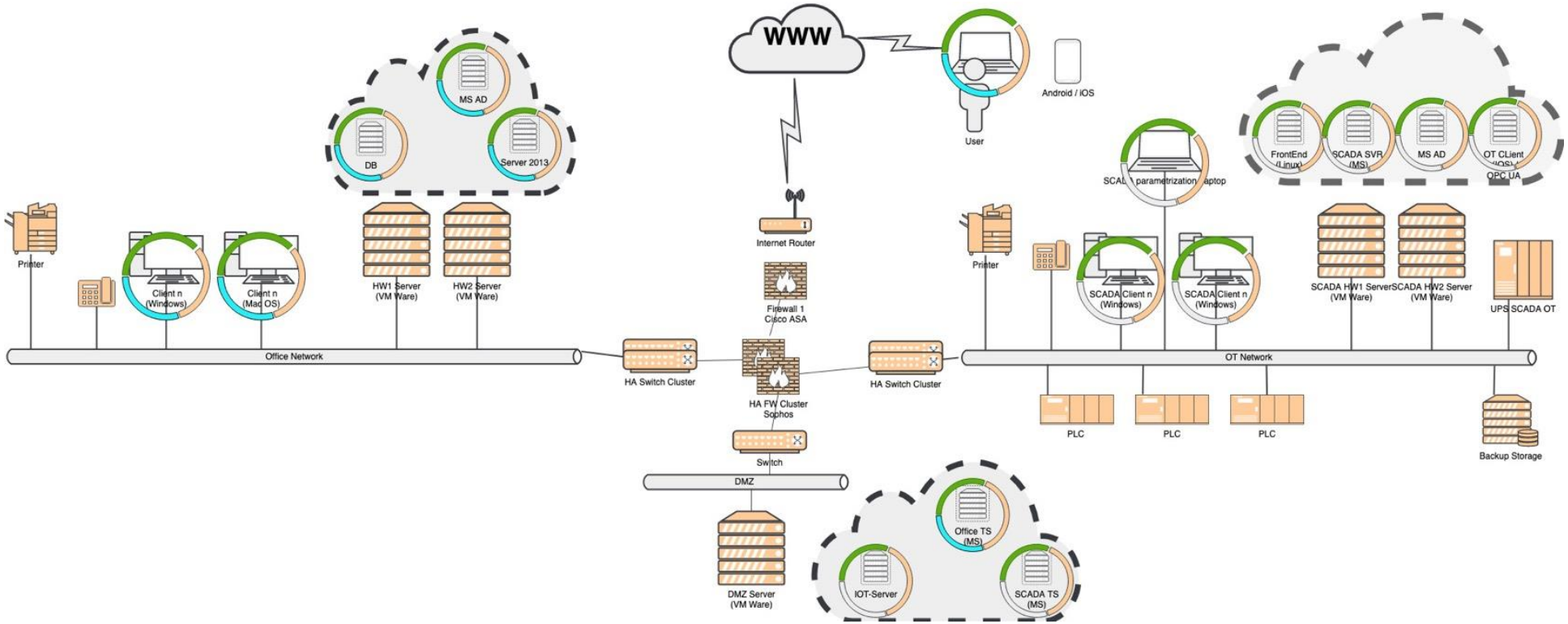
## SIEM (Security Information Event Management)

SIEM

Dateien

Anwendungen / Prozesse

Logdateien

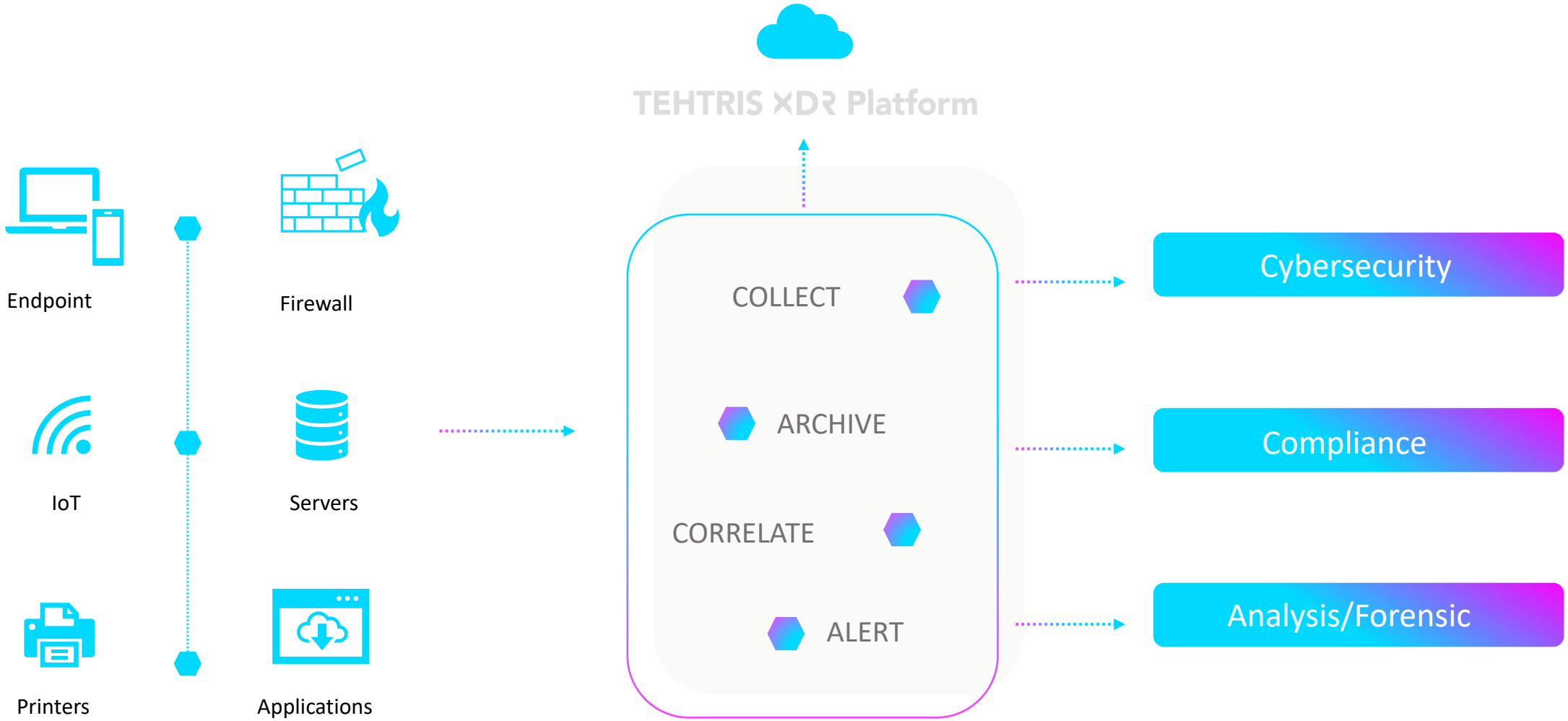




©TEHTRIS

# System zur Angriffserkennung

## SIEM (Security Information Event Management)





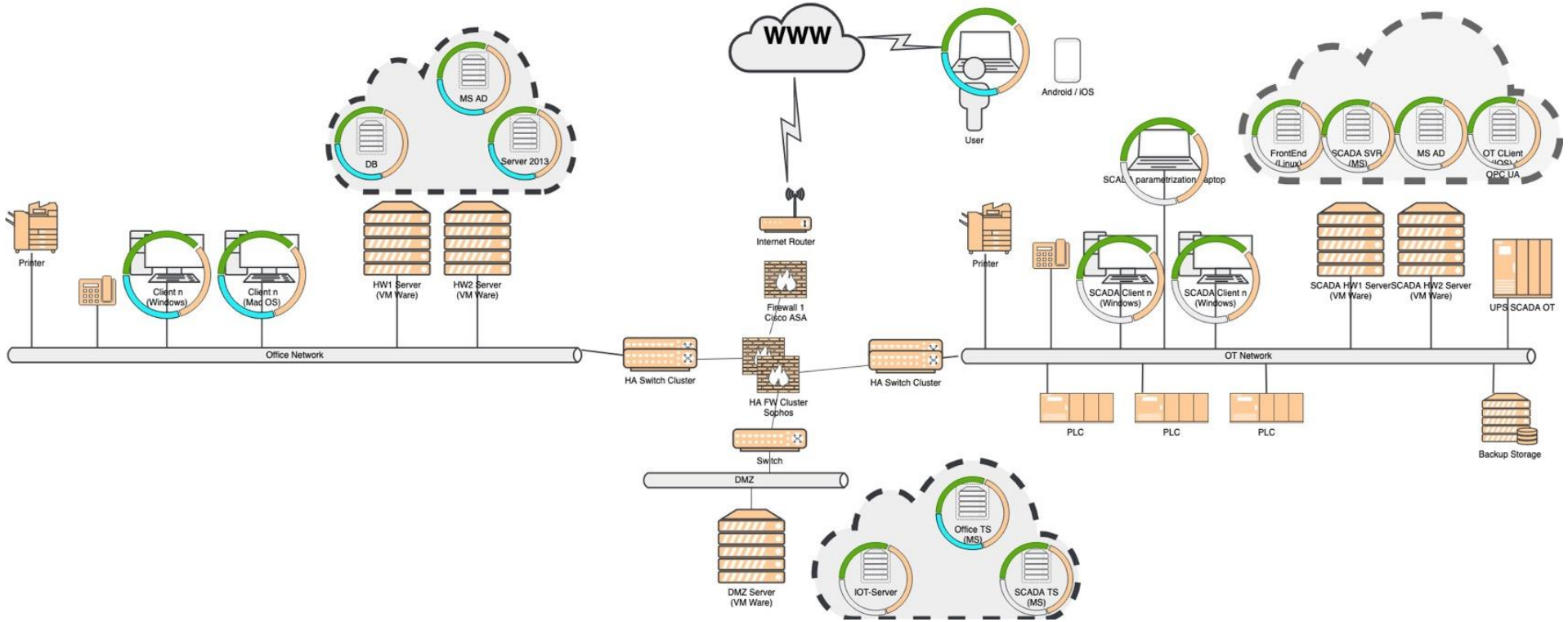
©TEHTRIS

# System zur Angriffserkennung

Dateien

Anwendungen / Prozesse

Logdateien





©TEHTRIS

# System zur Angriffserkennung

## NTA (Network Traffic Analysis)

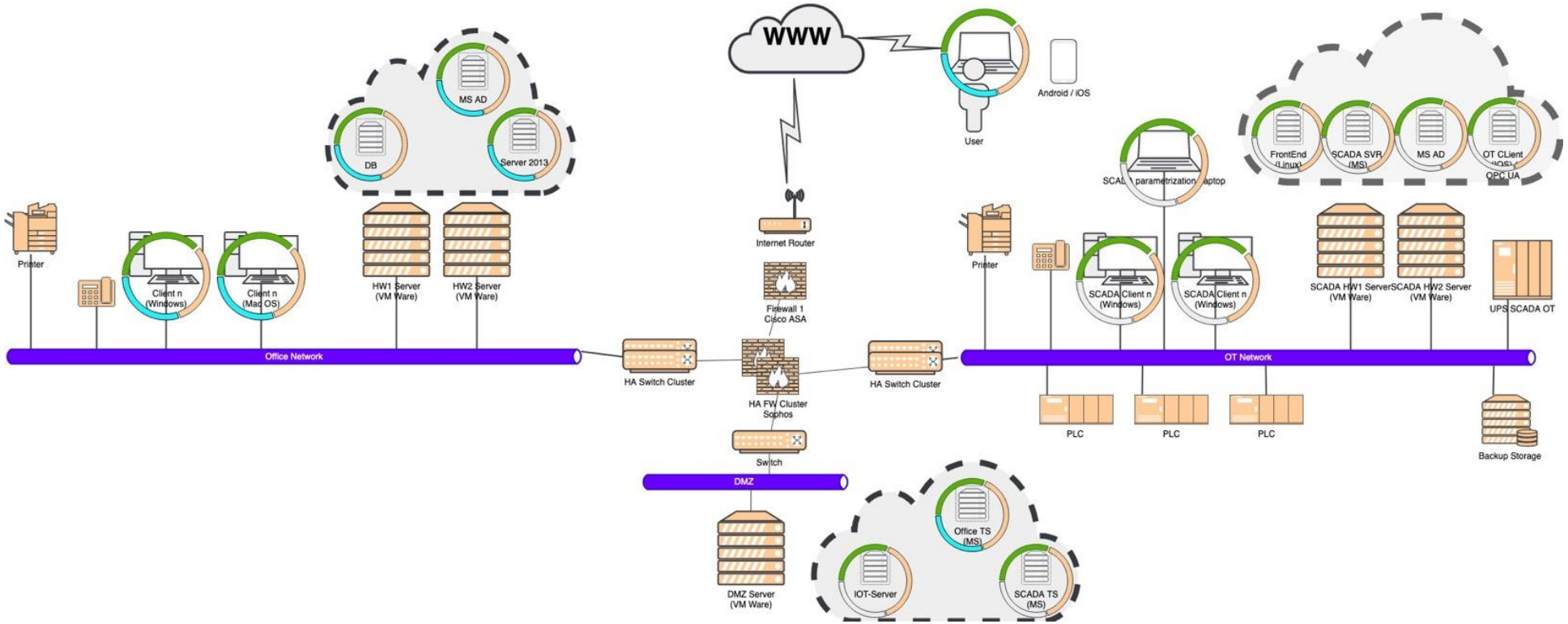
NTA

Dateien

Anwendungen / Prozesse

Logdateien

Netzwerk





©TEHTRIS

# System zur Angriffserkennung

## NTA (Network Traffic Analysis)




- Netzwerküberwachung
- Erkennung abnormaler Aktivitäten
- Zugang zur TEHTRIS XDR-Plattform und ihrer erweiterten Technologie (SOAR, CTI, CYBERIA)
- Vollständige Abdeckung von IT- und OT-Netzwerken
- Einfache Bereitstellung und Integration
- Überwachung des Netzwerkverkehrs: jeder angeschlossene Rechner, sowohl intern als auch extern (Dienstanbieter, Besucher...)
- + 60.000 MITRE-konforme Regeln, die ständig aktualisiert werden
- + 40 Arten von Warnungen
- Forensische Analyse auf Basis von Rohdaten


©TEHTRIS

# System zur Angriffserkennung

## MTD (Mobile Threat Detection)

MTD

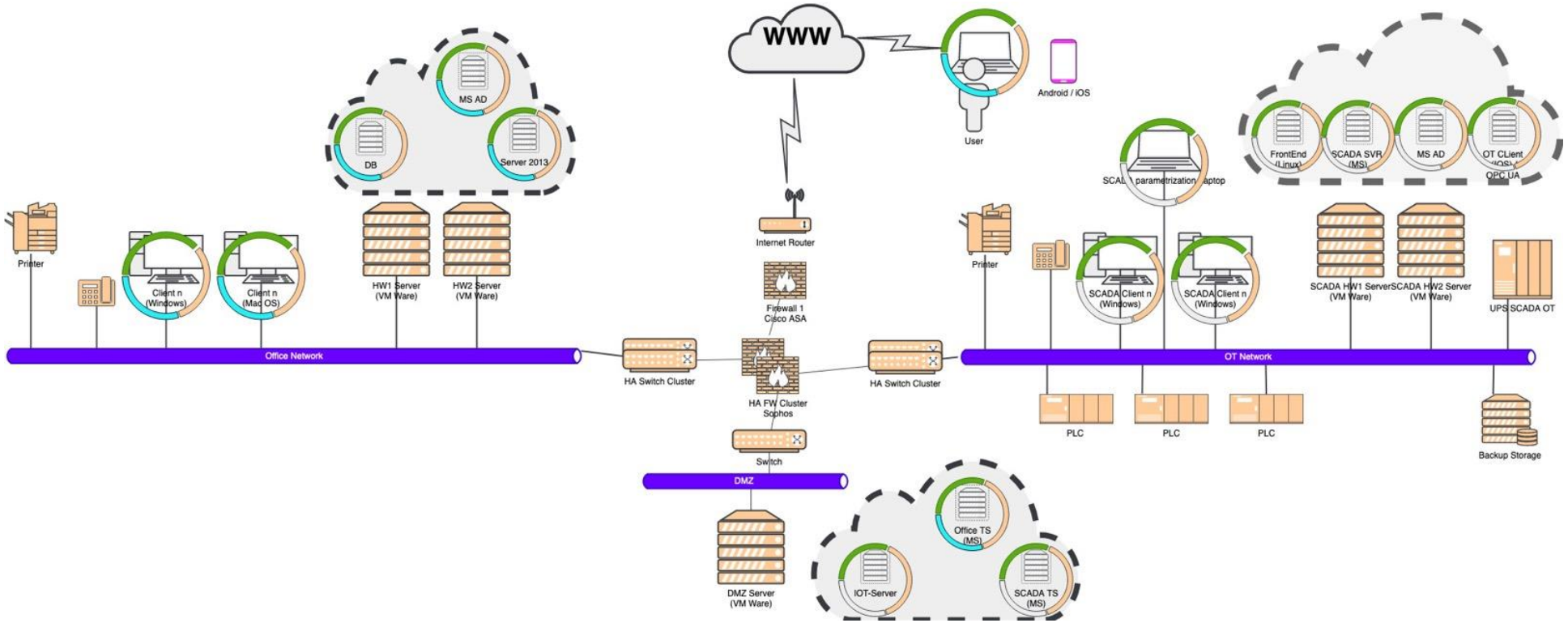
Dateien

Anwendungen / Prozesse

Logdateien

Network

Mobile





©TEHTRIS

# System zur Angriffserkennung

## DR (Deceptive Response)

Dateien

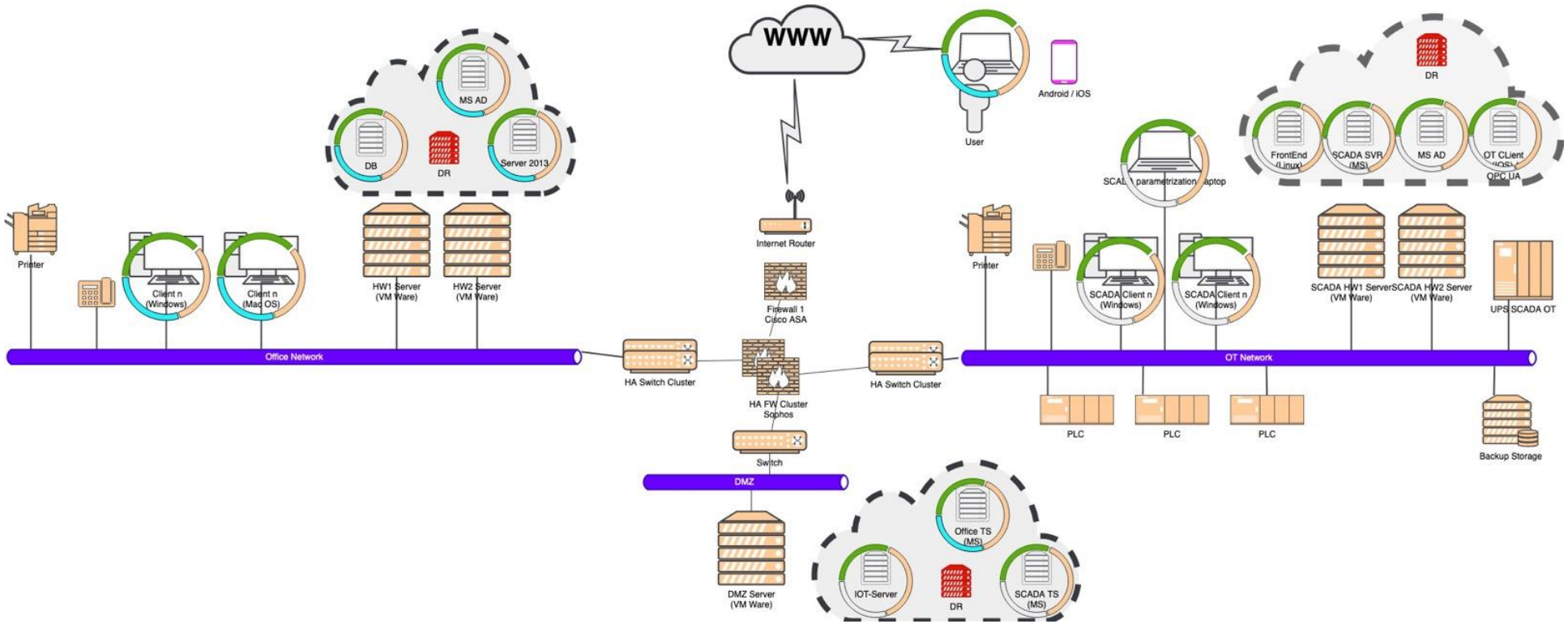
Anwendungen / Prozesse

Logdateien

Network

Mobile

Honeypot

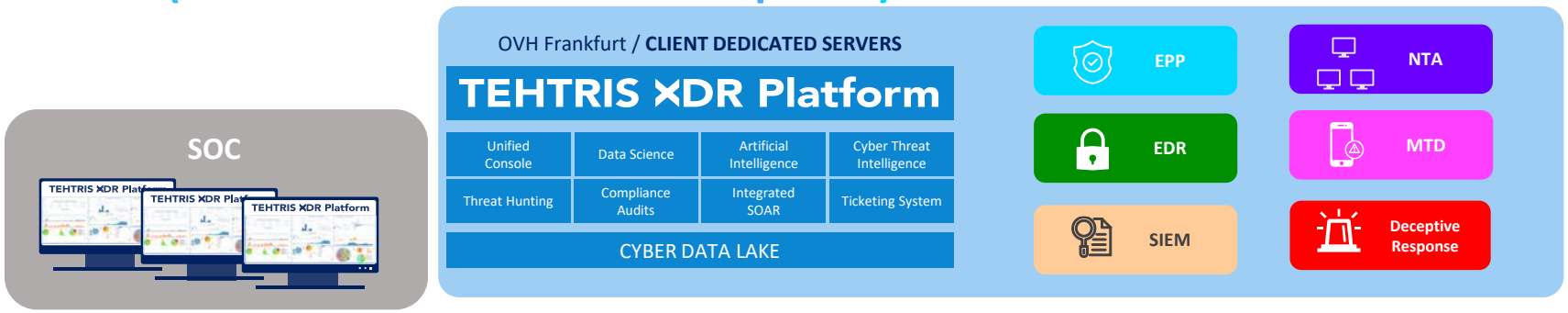




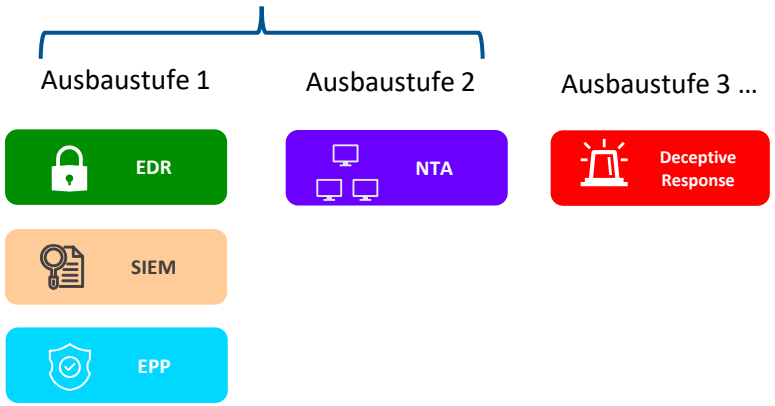
©TEHTRIS

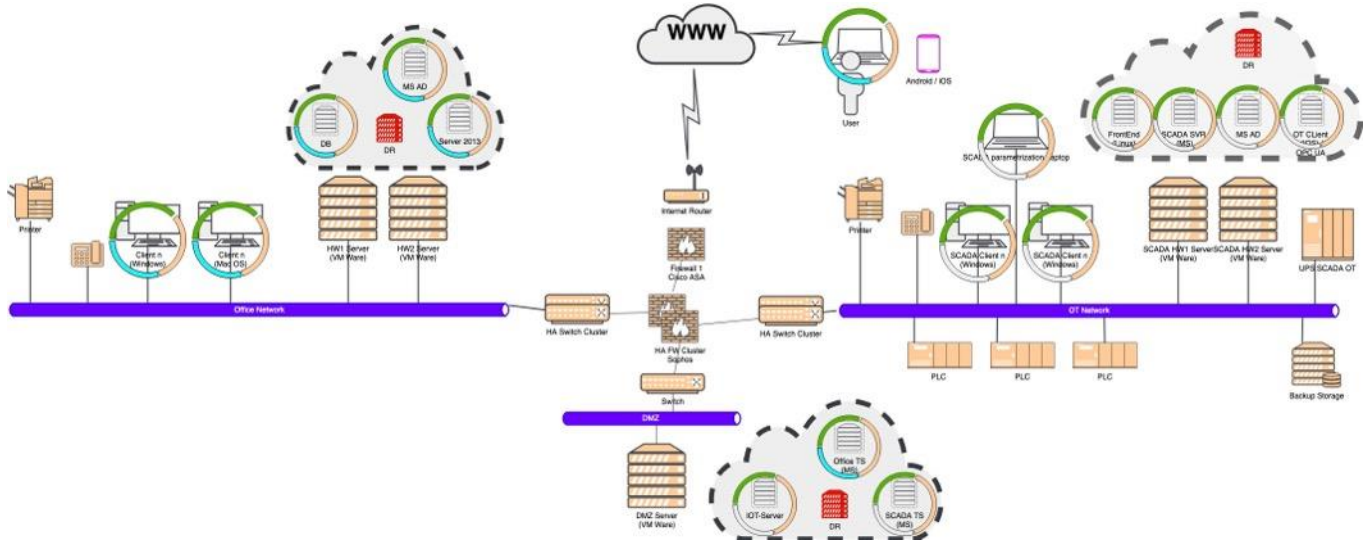
# System zur Angriffserkennung

## XDR (eXtended Detection and Response)




Empfehlung: Mindestmaßnahmen



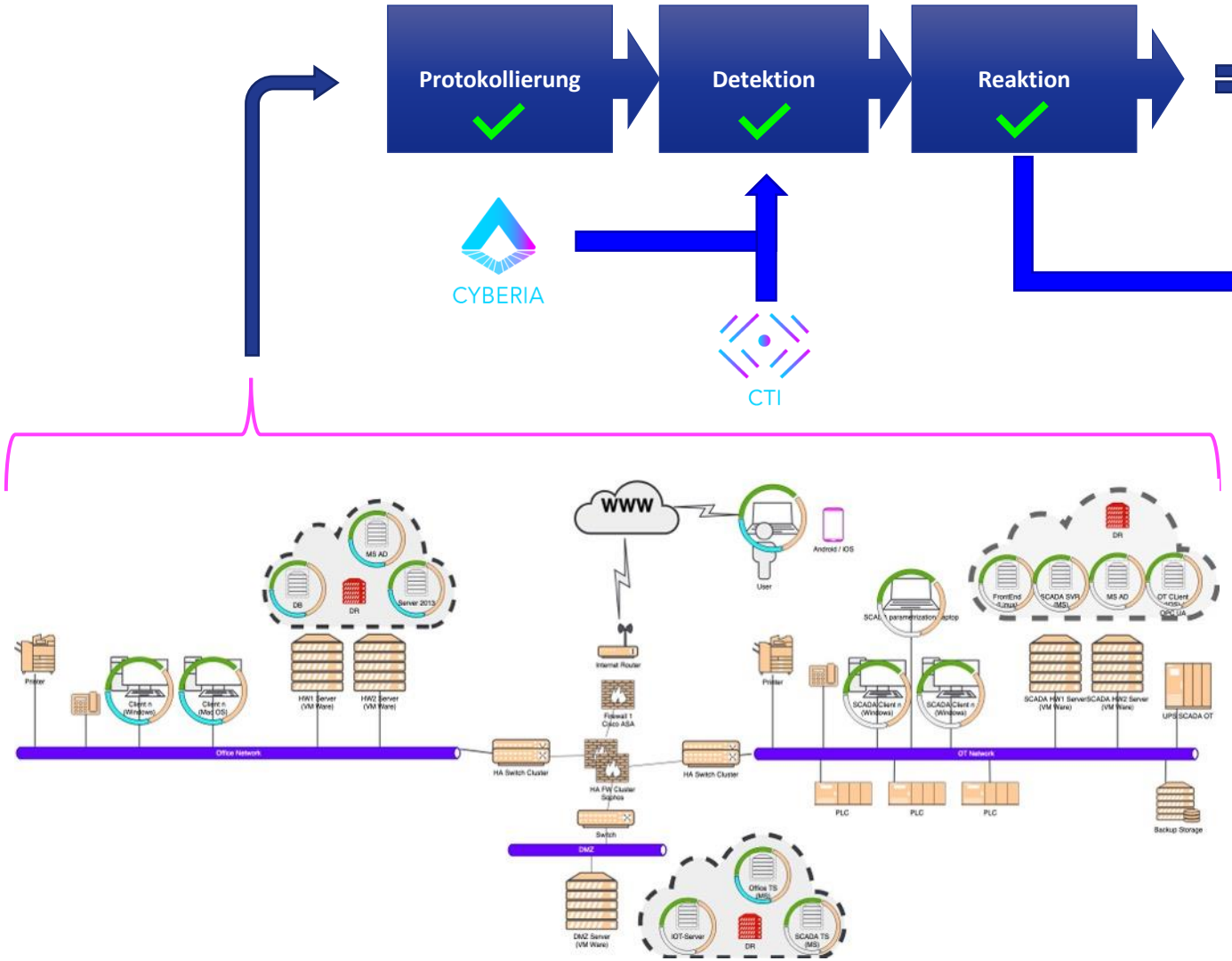

**Vorteile einer XDR Plattform:**

- **Modular /Flexibel**
- **Skalierbar / Cloud / on Prem**
- **Intern verschlüsselt und gehärtet**
- **Schützen ihre Investitionen**
- **Erfahren in OT Umgebungen**


©TEHTRIS

# System zur Angriffserkennung

## mit TEHTRIS





©TEHTRIS




# 03

# Aufgepasst!


©TEHTRIS

# Künstliche Intelligenz „der 5te Mann im SOC“




DNSF

NTA

SIEM

EDR

CTI

MTD

EDR

EDR

Raw logs

Alerts

Files

Alerts

## Weak signal detection

- Behavioral analysis - UEBA
- Anomaly detection

## Malicious file detection

- Next generation antivirus
  - Windows
  - Linus
  - Android *

## SOC pre-analysis

- Priorisation
- Grouping

Alerts
Reports

Alerts

Priorisation
Groups

XDR

# System zur Angriffserkennung

## EDR

## Abwärts – Kompatibilität

### macOS

| Operating System | arm64 | 64bits |
|---|---|---|
| macOS Monterey | ✓ | ✓ |
| macOS Big Sur | ✓ | ✓ |
| macOS Catalina | | ✓ |
| macOS Mojave | | ✓ |
| macOS High Sierra | | ✓ |
| macOS Sierra | | ✓ |

### Windows

| Operating System | 32bits | 64bits |
|---|---|---|
| Windows 11 | - | ✓ |
| Windows 10 IoT | ✓ | ✓ |
| Windows 10 | ✓ | ✓ |
| Windows 8.1 | ✓ | ✓ |
| Windows 8 | ✓ | ✓ |
| Windows 7 Embedded | ✓ | ✓ |
| Windows 7 | ✓ | ✓ |
| Windows Vista | ✓ | ✓ |
| Windows XP | ✓ | ✓ |
| Windows Server 2022 | - | ✓ |
| Windows Server 2019 | - | ✓ |
| Windows Server 2016 | - | ✓ |
| Windows Server 2012 R2 | - | ✓ |
| Windows Server 2012 | - | ✓ |
| Windows Server 2008 R2 | ✓ | ✓ |
| Windows Server 2008 | ✓ | ✓ |
| Windows Server 2003 | ✓ | ✓ |

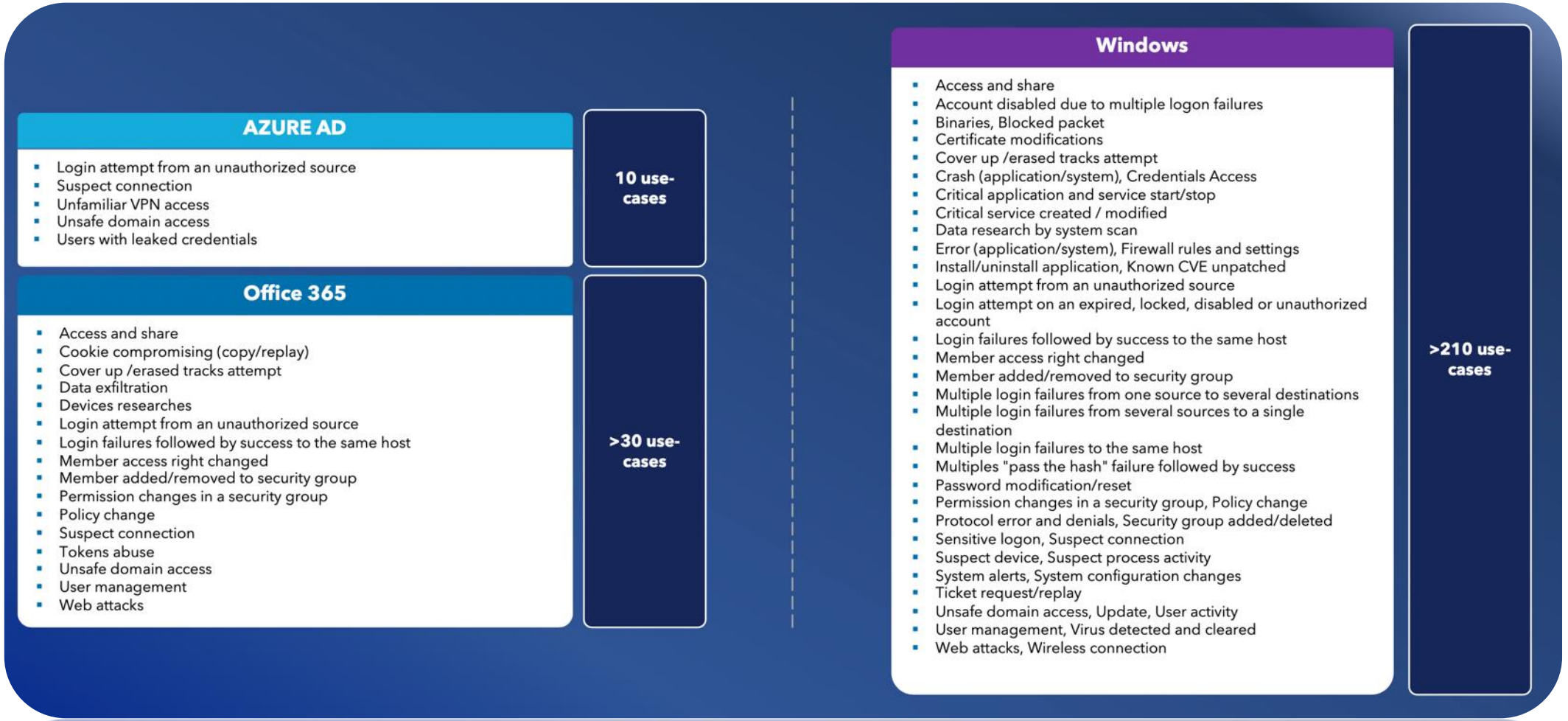
### Linux

| Operating System | 32bits | 64bits |
|---|---|---|
| CentOS 5+ | ✓ | ✓ |
| Ubuntu 8+ | ✓ | ✓ |
| RedHat 5+ | ✓ | ✓ |
| Debian 5+ | ✓ | ✓ |
| SUSE Entreprise Server 11 | ✓ | ✓ |
| SUSE Entreprise Server 12 | ✓ | ✓ |
| Oracle Linux 6.8 | ✓ | ✓ |
| Oracle Linux 6.10 | ✓ | ✓ |


©TEHTRIS

# System zur Angriffserkennung

## SIEM Use-Cases





©TEHTRIS

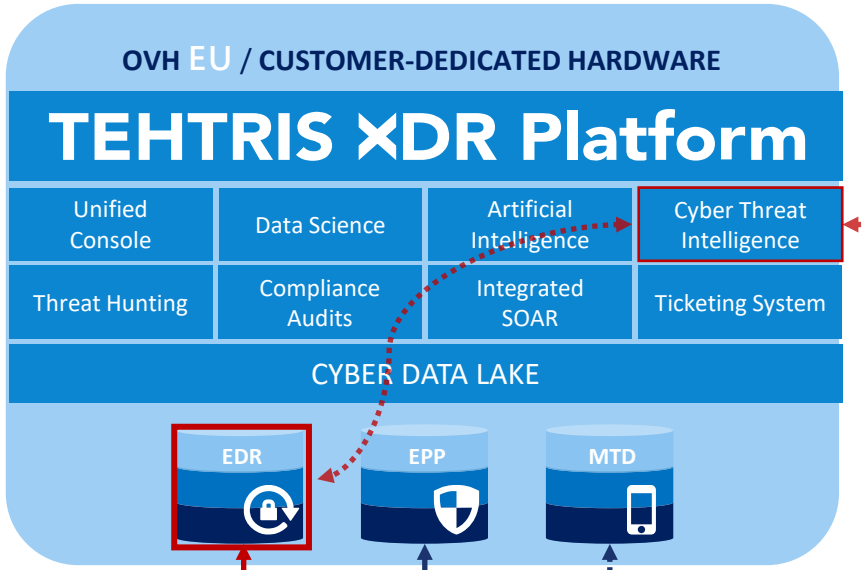
# DATA FLOW

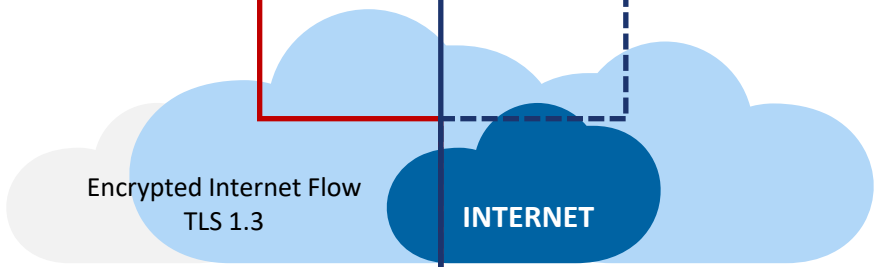
Binaries hashes flow analysis
(detailed on the next slide)

VPN

## Customer environment

SIEM is not represented in this picture



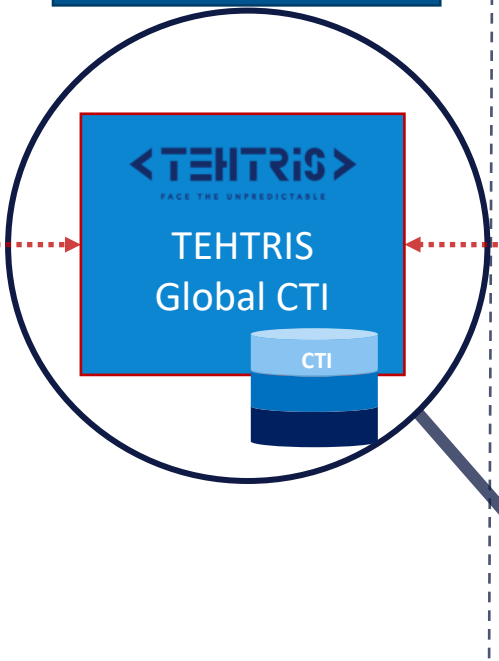




**Endpoints at Customer sites**
**+ endpoints in mobility**



EDR, EPP (& MTD) agents managed by dedicated appliances

## Zoom on TEHTRIS CTI




## External sources

If hashs are unkown from TEHTRIS CTI, a private request is done to external database

External CTI feeds

**TEHTRIS never sends binary files belonging to the customer out of the TEHTRIS XDR platform**

**TEHTRIS products do not allow the opening or access to ANY customer file, unlike other competitors.**




**100% EU native technology with EU hosting.**






**Only EU jurisdiction will apply**





©TEHTRIS

# System zur Angriffserkennung

## Abschließende Tips:

Achten Sie auch bei der Auswahl Ihrer Produkte und Dienstleister auf Sicherheit (taktisch).

MDR und SOC sind schöne Marketingbegriffe. Achten Sie auf die Inhalte und SLAs.

Setzen Sie Security-Lösungen ein, um Ihre Infrastruktur zu schützen und nicht nur um Vorschriften zu erfüllen.

Handhabbare Maßnahmen und hybride Technologien.


©TEHTRIS

# MERCI !

# THANK YOU !

Contact us!

**Olaf.Mueller-Haberland@tehtris.eu**

+49 151 1949 8606

TEHTRIS

FACE THE UNPREDICTABLE

# Proactive Cybersecurity

## How defenders can get an advantage



# Agenda

- Proactive cybersecurity vs reactive cybersecurity
- Does proactive cybersecurity work?
- Defenders have an advantage.
- Case study: US National Security Agency, Center for Internet Security
- Example controls in action.

# Reactive cybersecurity

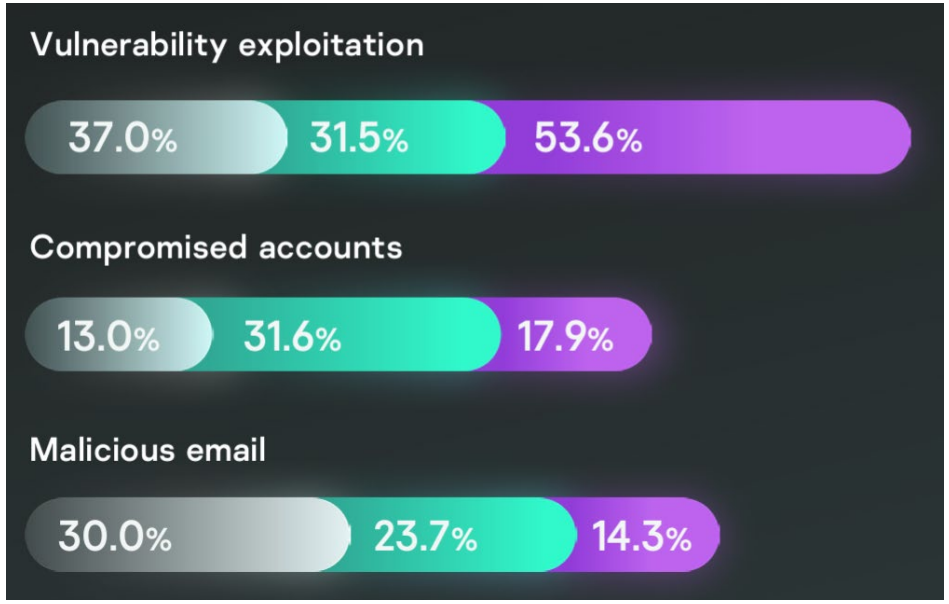
- Identifying breach after the fact.
  - Intrusion Detection Systems (IDS).
  - Log monitoring systems
- Procedures to deal with the consequences of the breach
  - Paying ransomware
  - Alerting authorities
  - Rebuilding systems
- Reactive cybersecurity is often the main focus.
  - Stopping attackers in their tracks is exciting.

# Proactive cybersecurity

- Security controls that prevent attacks from becoming breaches.
- Examples
  - NIST 800-53
    - Technical controls
  - Center for Internet Security (CIS).
    - Top 7 Controls
- Proactive cybersecurity is often neglected.
  - Not exciting.
  - No AI ☺).

# Defenders have an advantage - if we implement proactive controls

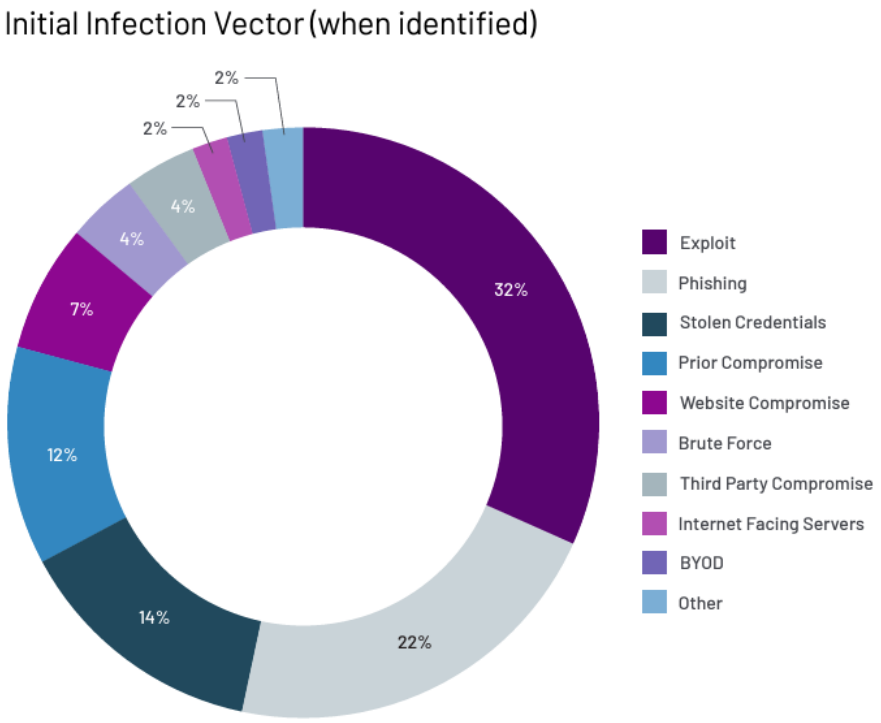
- Kaspersky “The nature of cyber incidents 2022”



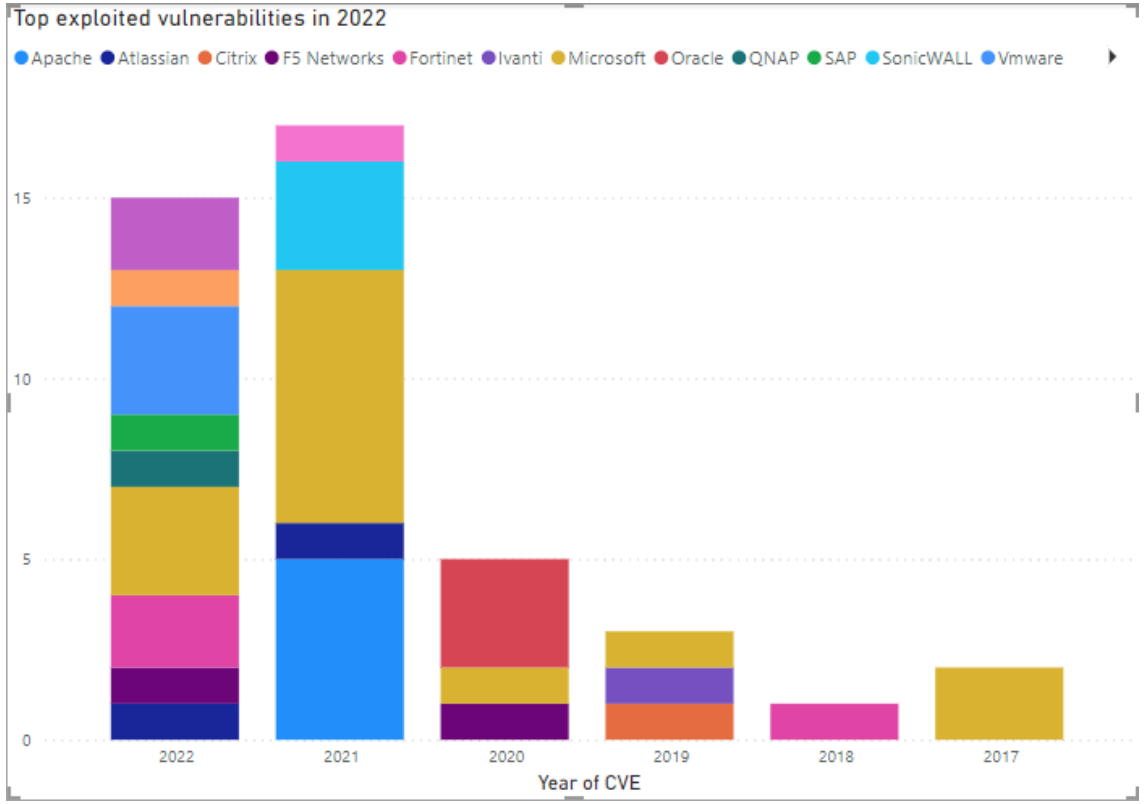



# Defenders have an advantage

- Mandiant M-Trends 2023

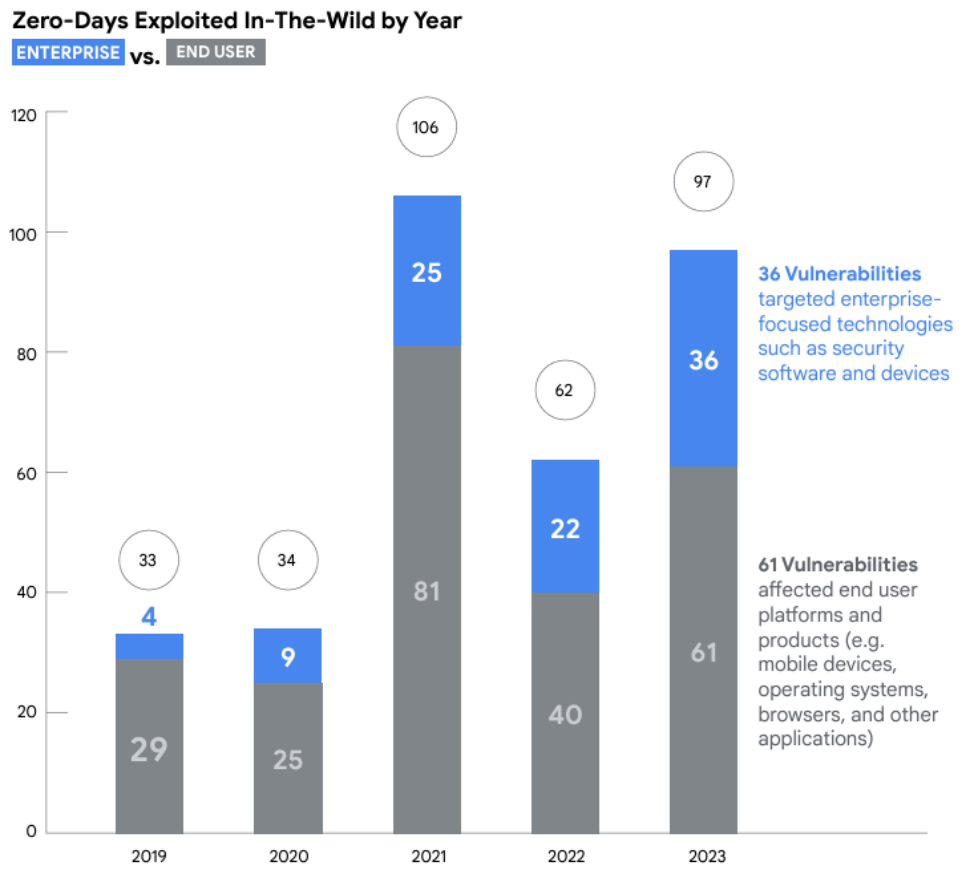


# Top exploited vulnerabilities in 2022

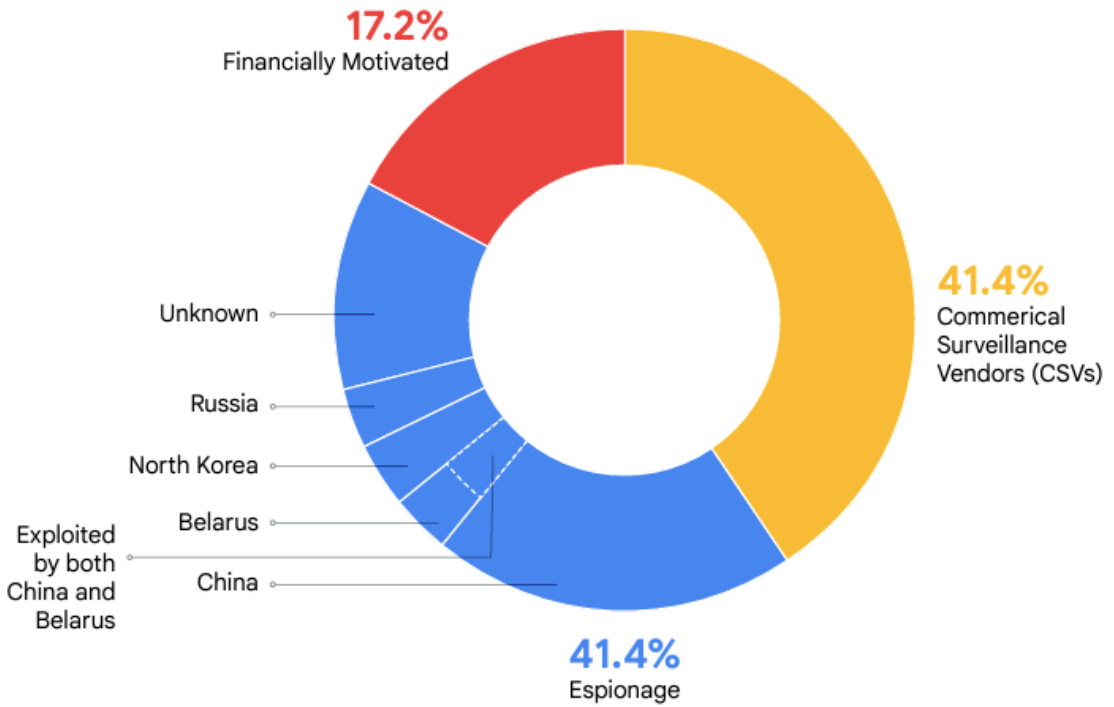



| Year | Total CVEs | Percent |
|---|---|---|
| 2022 | 15 | 34.88 |
| 2021 | 17 | 39.53 |
| 2020 | 5 | 11.63 |
| 2019 | 3 | 6.98 |
| 2018 | 1 | 2.33 |
| 2017 | 2 | 4.65 |
| **Total** | **43** | **100.00** |

# What about zero days?



# Especially if you have IP or are government



# Does proactive cybersecurity work?

- NSA IAD under Tony Sager and Curt Dukes.
  - Responsible to defend US DoD from cyber attacks.
  - Red Team and Blue Team lessons learned.
    - Same attack vectors successful time after time.
  - Result: Defined cyber security controls within DoD
  - DoD and its contractors have gotten much better
    - Since the SecDef's Exchange Server breach and F-35 design data loss.

# Does proactive cybersecurity work?

- Center for Internet Security
  - Initially funded by NSA to impart lessons learned to industry.
  - Originally Top 20 Security Controls
    - Original Top 5 will reduce risk of breach by 85%, all 20 by 94%

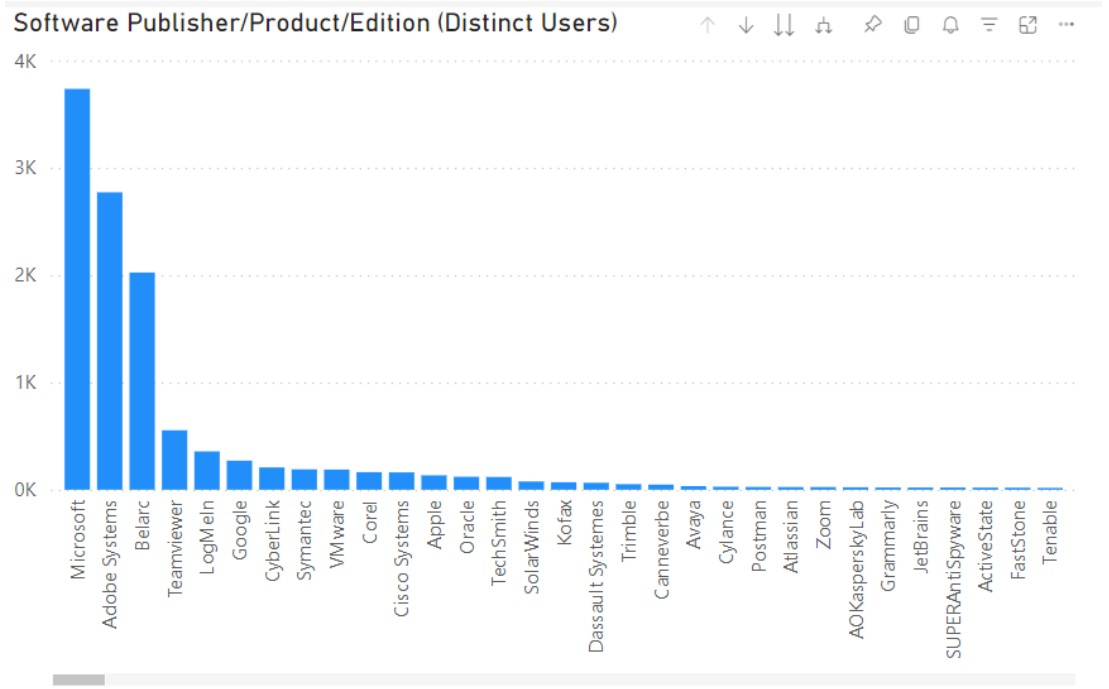
# CIS Critical Security Controls

- Version 8 – May 2021 (Top 7)
  - 1-Inventory and Control of Enterprise Assets (hardware & devices)
  - 2-Inventory and Control of Software Assets
  - 3-Data Protection
  - 4-Secure Configurations of Enterprise Assets and Software
  - 5-Account Management (manage credentials)
  - 6-Access Control Management (MFA and user privileges)
  - 7-Continuous Vulnerability Management

# Government or valuable IP

- These are in a different league
  - Not just Ransomware or theft of PII
- Vendor systems breached
  - Use of Microsoft signing key to access Exchange Online mailboxes.
  - SolarWinds
- Open source libraries
  - Log4j – logging utility
  - xz Utils for Linux
- Solutions will involve government & industry
  - Support for open source volunteers.
  - Critical vendors need to be held to high standards.

# Approved software




Software not used for X days

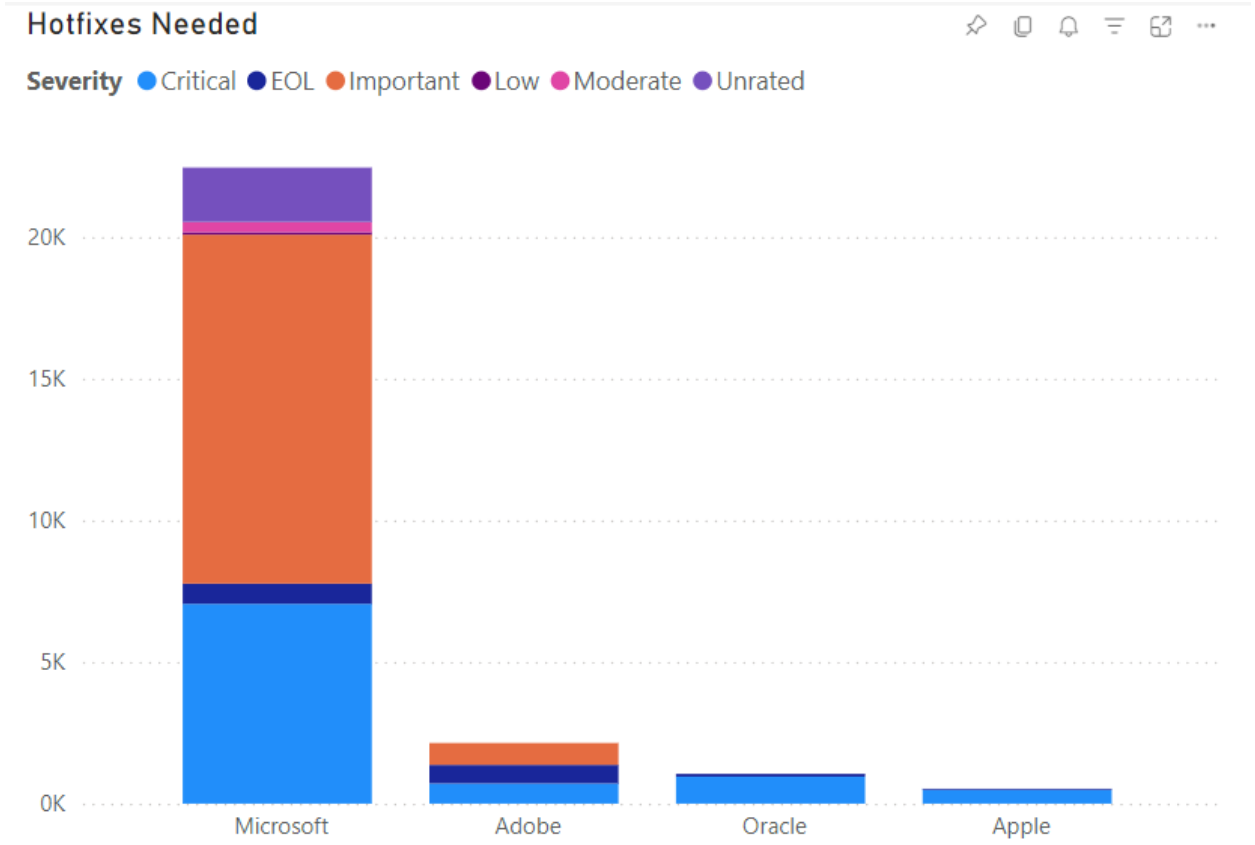
-1 6916

License Required?

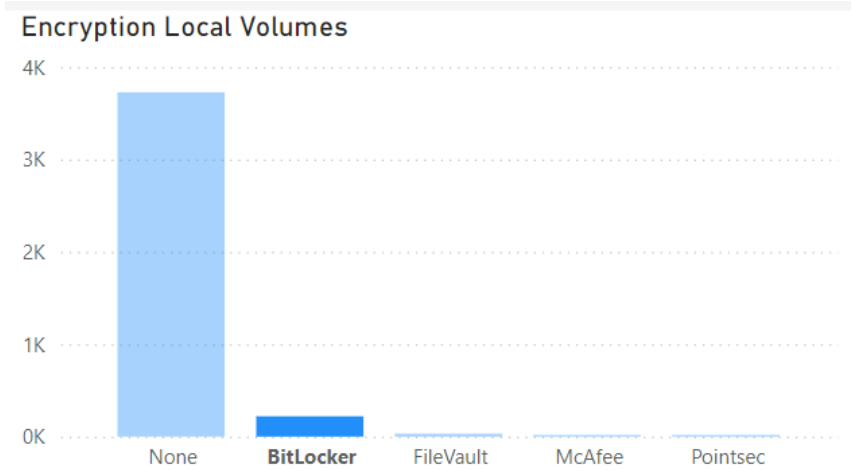
no

yes

# Vulnerabilities – hotfixes needed



# Vulnerabilities – drive encryption




Encryption Local Volumes

| Computer | User | Encryption |
|---|---|---|
| nb_692 | 1002 | BitLocker |
| nb_1390 | 1007 | BitLocker |
| nb_468 | 102 | BitLocker |
| nb_1786 | 1021 | BitLocker |
| nb_2067 | 1022 | BitLocker |
| nb_56 | 1023 | BitLocker |
| desk_1664 | 1037 | BitLocker |
| nb_1385 | 1045 | BitLocker |
| nb_1203 | 1054 | BitLocker |
| desk_1393 | 1060 | BitLocker |

**Total**

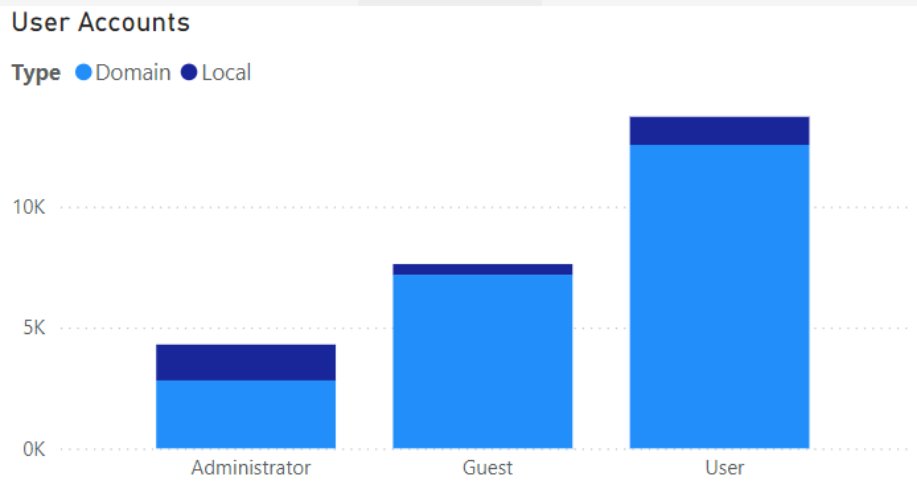
Encryption Suspended

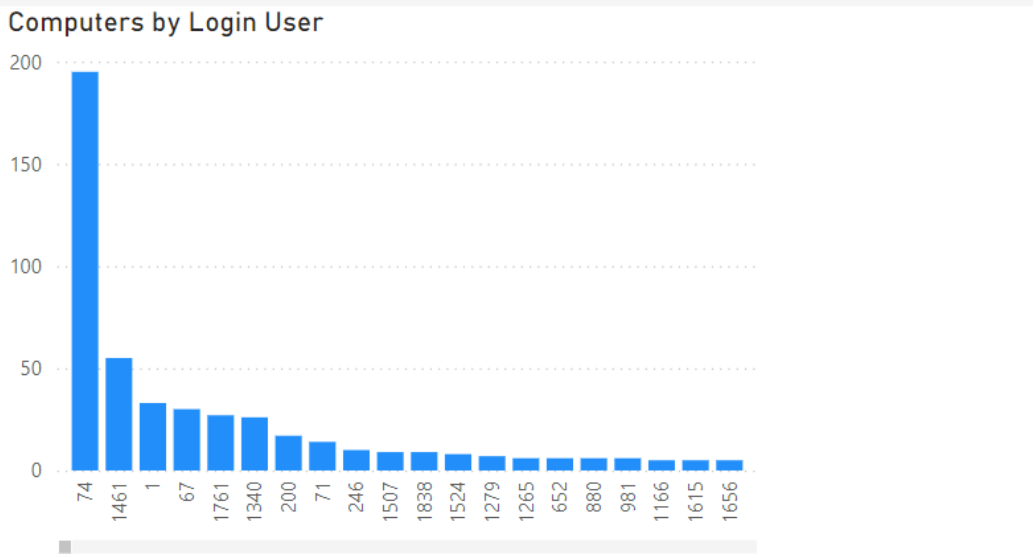
- ☐ (Blank)
- ☐ no
- ☐ yes

Local Volumes

220

# User accounts



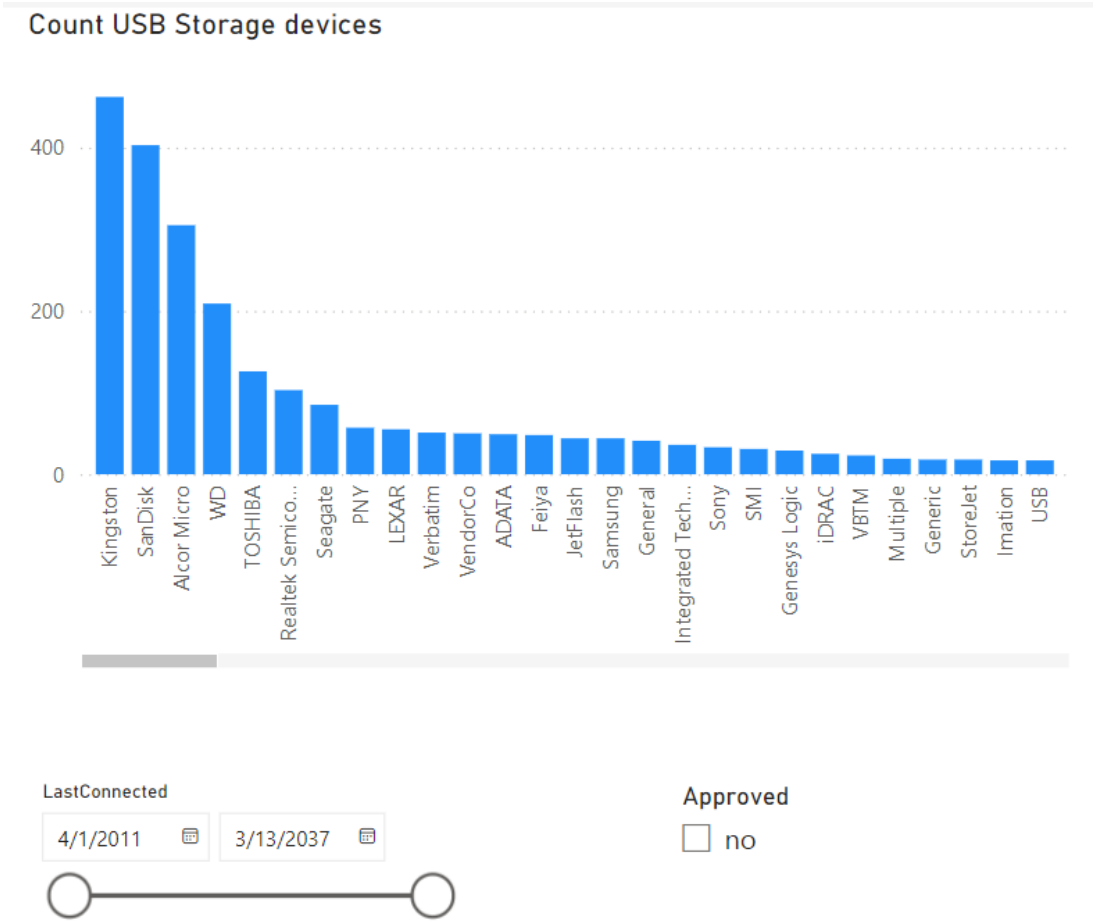

Jser Accounts

| Type | Administrator | Guest | User | **Total** |
|---|---|---|---|---|
| Domain | 2810 | 7181 | 12551 | **21387** |
| Local | 1485 | 442 | 1164 | **2940** |
| **Total** | **4114** | **7608** | **13510** | **23786** |

Password Age more than X days

0 11790

# USB storage device usage



# Secure configurations

**Score:** **1.00** of 10

**Risk Category:** **High**

**Benchmark:** **DISA - Windows 10, version 2.3**

**Benchmark Results by Section and Setting (• = Pass, X= Fail ):**

X **Operating System Settings**

- • 1. Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.
- • 2. Windows 10 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.
- X 3. Windows 10 systems must be maintained at a supported servicing level.
- • 4. Local volumes must be formatted using NTFS.
- X 5. Accounts must be configured to require password expiration.
- • 6. Internet Information System (IIS) or its subcomponents must not be installed on a workstation.
- • 7. Simple Network Management Protocol (SNMP) must not be installed on the system.
- • 8. Simple TCP/IP Services must not be installed on the system.
- • 9. The Telnet Client must not be installed on the system.
- • 10. The TFTP Client must not be installed on the system.
- X 11. The Windows PowerShell 2.0 feature must be disabled on the system.
- • 12. The Server Message Block (SMB) v1 protocol must be disabled on the system.
- • 13. The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.
- • 14. The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.
- X 15. The Secondary Logon service must be disabled on Windows 10.
- • 16. Data Execution Prevention (DEP) must be configured to at least OptOut.

X **Account Lockout and Password Policy Settings**

- • 1. Windows 10 account lockout duration must be configured to 15 minutes or greater.
- • 2. The number of allowed bad logon attempts must be configured to 3 or less.
- • 3. The period of time before the bad logon counter is reset must be configured to 15 minutes.
- X 4. The password history must be configured to 24 passwords remembered.
- • 5. The maximum password age must be configured to 60 days or less.
- X 6. The minimum password age must be configured to at least 1 day

# Belarc company

- Over 1,800 customers worldwide
  - Commercial
    - Autodesk, Novelis (Canada, Korea), Shell Canada, Travelers Insurance (India)
  - US Federal Government
    - Environmental Protection Agency, Federal Aviation Administration, NASA, Patent & Trademark Office, Department of State (DS), US Air Force (844$^{th}$ CG)
  - Many long term >10 years
  - Located in 50 countries
- Eight US and Worldwide Patents

# Questions?

Sumin Tchen

(e) stchen@belarc.com

www.belarc.com

xorlab

Bosch CyberCompare 2024 | Protect – Detect – Respond

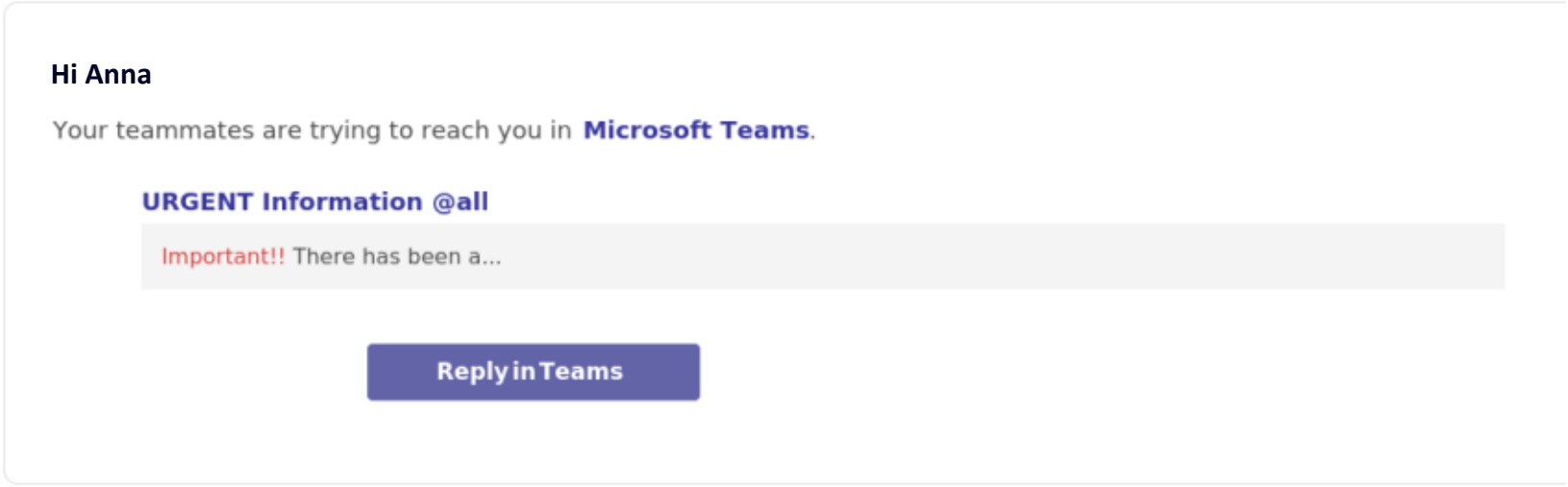
# Protect: E-Mail Security neu gedacht

Benjamin Hindelang | 4. Juni 2024

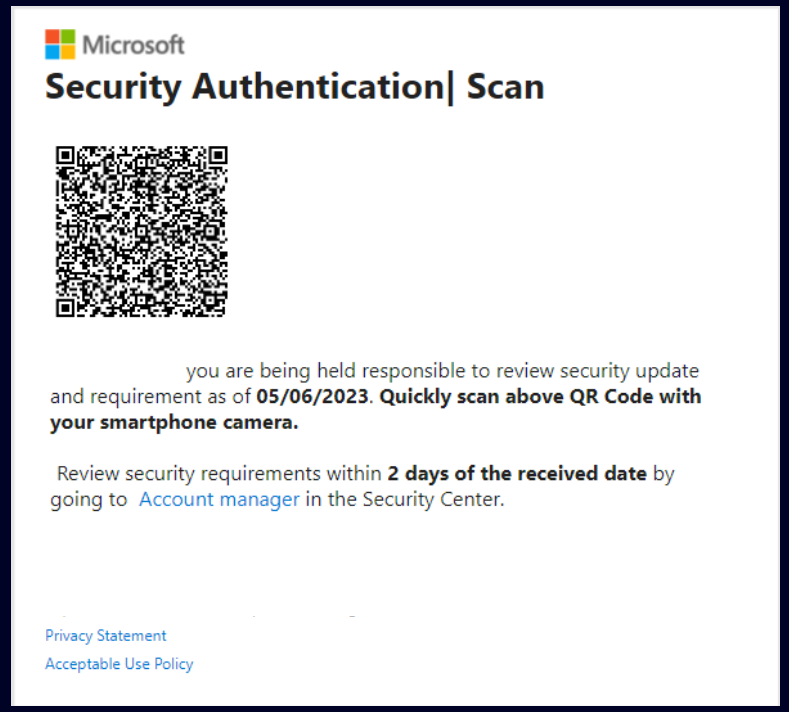

I
LO VE
HA TE
Y O U


FOKUS

# Praxis-beispiel | 1

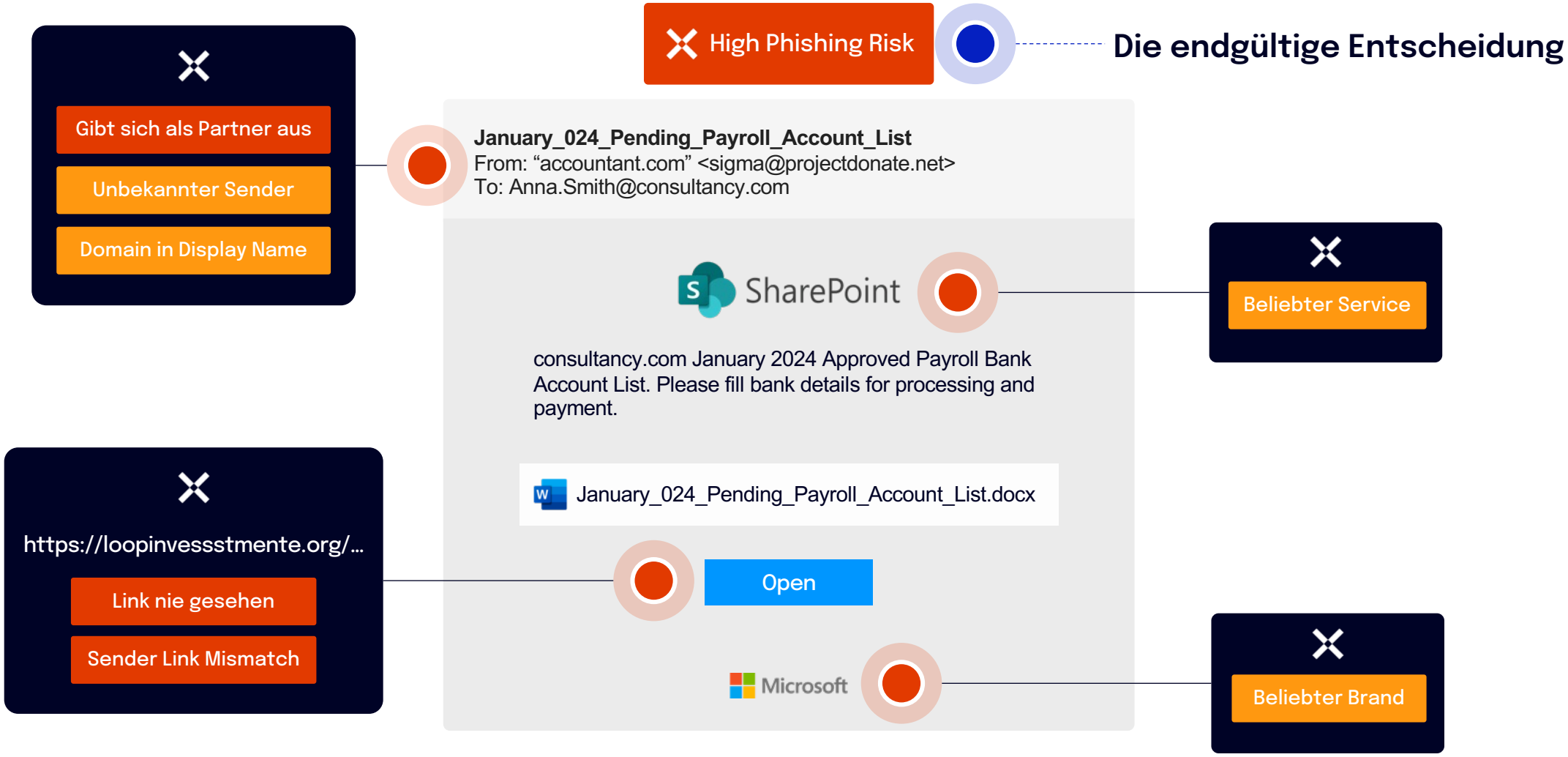


# Praxisbeispiel | 2






# Praxisbeispiel | 3



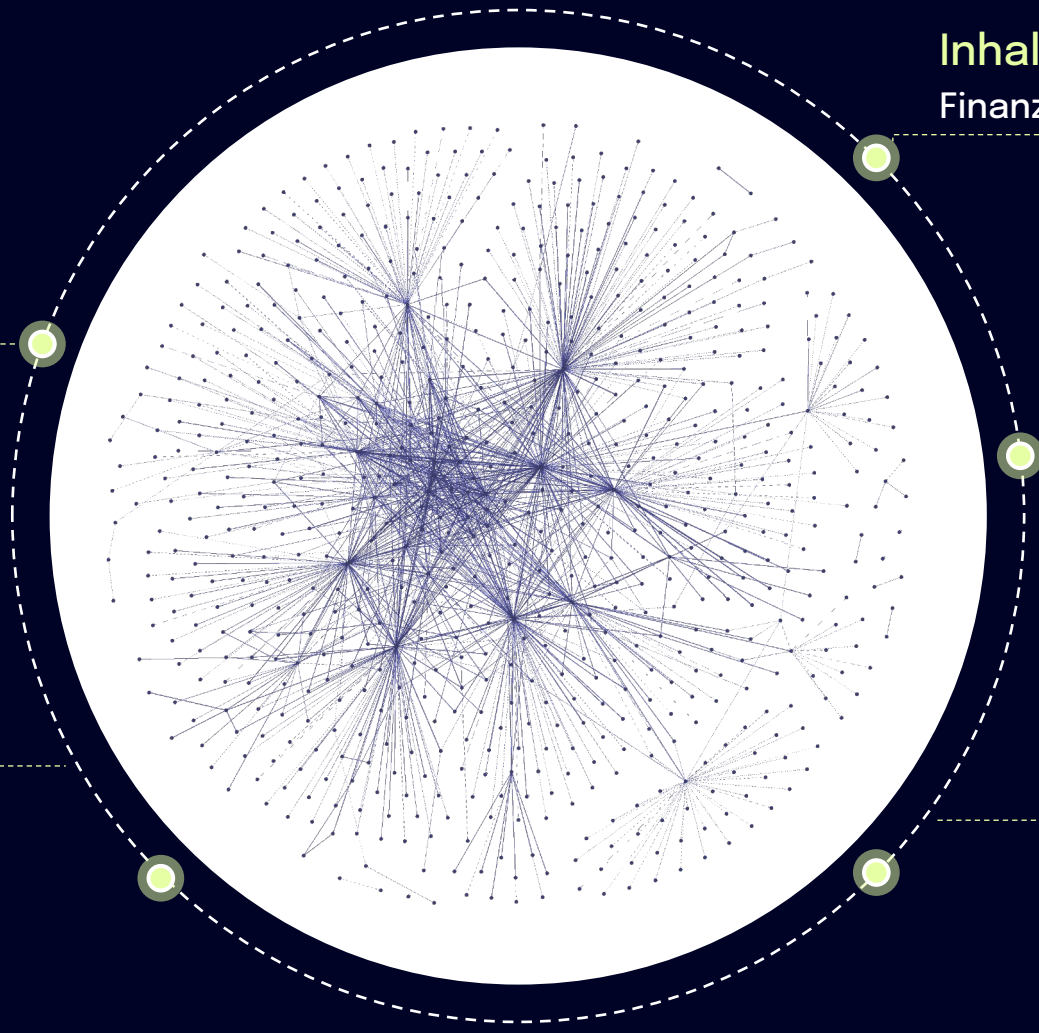
# Zero-Hour



# KI-gestützte Kontext-Intelligenz

**Inhaltliche Themen**
Finanzielle Transaktionen| Passwort Reset | usw.

**Beziehungen**
Lieferanten | Kunden | usw.



**Tonalität**
Dringlichkeit | Autorität | usw.

**Dateien & Attribute**
Makros & aktive Inhalte |
Encrypted Archives | usw.

**Links & Domänen**
Cloud Services | Schatten-IT | usw.

Plot: Visualisierung der Beziehungen aus der E-Mail-Kommunikation von 3 Monaten xorlab

# KI-gestützte Kontext-Intelligenz

## Erwartbar

Relationship

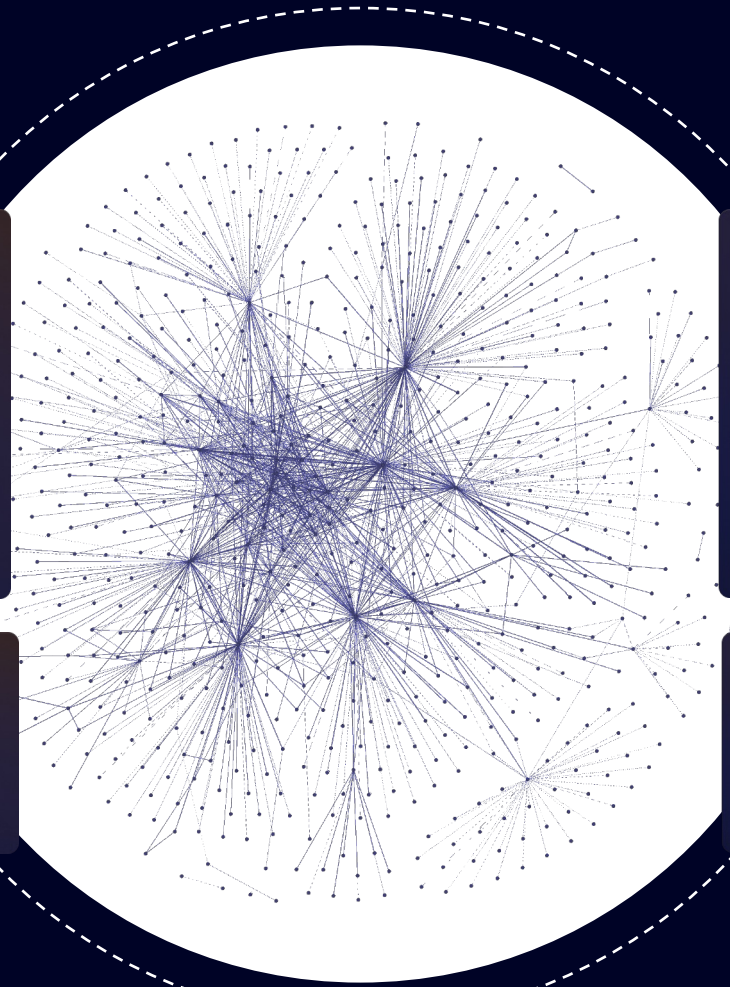
Sender **anthony@jj-tech.io** — 84 — Recipient **luca@xorlab.com**

jj-tech.io — 95 — xorlab.com

24

anthony@jj-tech.io — 65 — luca@xorlab.com

| URL | RELEVANCE | TYPE |
|---|---|---|
| jj-agency.com | 87 | Hyperlink |



## Potenziell gefährlich

Relationship

Sender **jantina@icloud.com** — 0 — Recipient **antonio@xorlab.com**

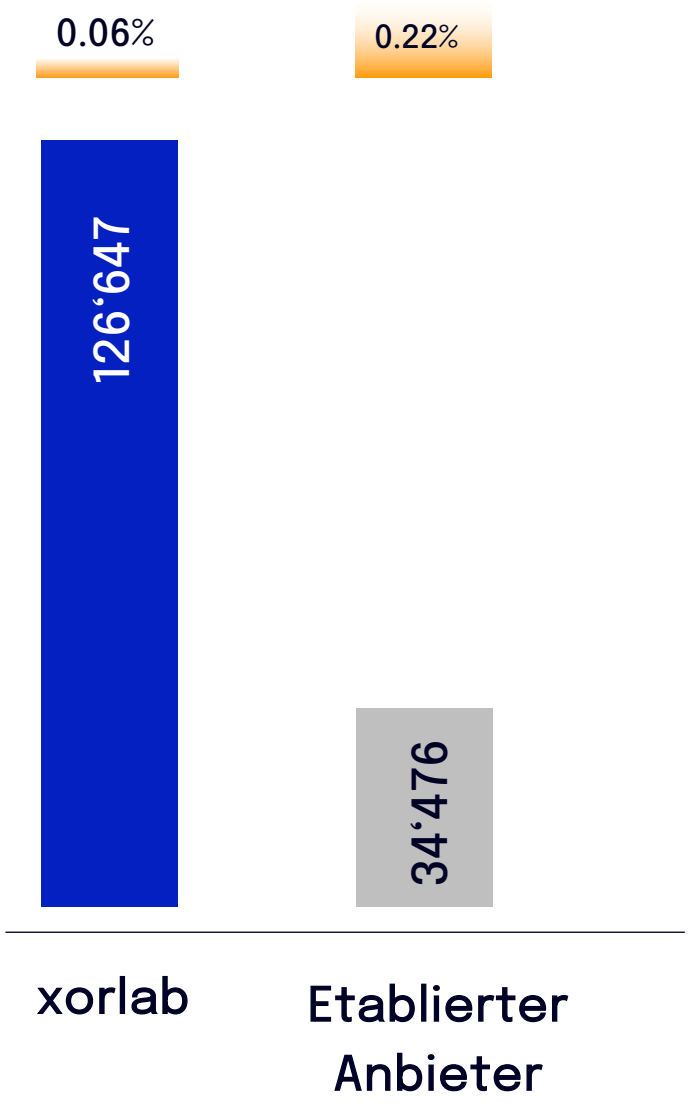
icloud.com — 0 — xorlab.com

0

jantina@icloud.com — 0 — antonio@xorlab.com

| URL | RELEVANCE | TYPE |
|---|---|---|
| track.shop….com | 0 | QR Code |

Plot: Visualisierung der Beziehungen aus der E-Mail-Kommunikation von 3 Monaten xorlab


0.06%
0.22%
False-
Positives
126‘647
34‘476
xorlab
Etablierter
Anbieter


CERN

“Ich interessiere mich weniger für blockierte, sondern mehr für erfolgreiche Angriffe.

Mit xorlab ist diese Zahl sehr niedrig.”

Dr. Stefan Lüders

Chief Security Officer, CERN



# Höhere Erkennung und geringerer Aufwand

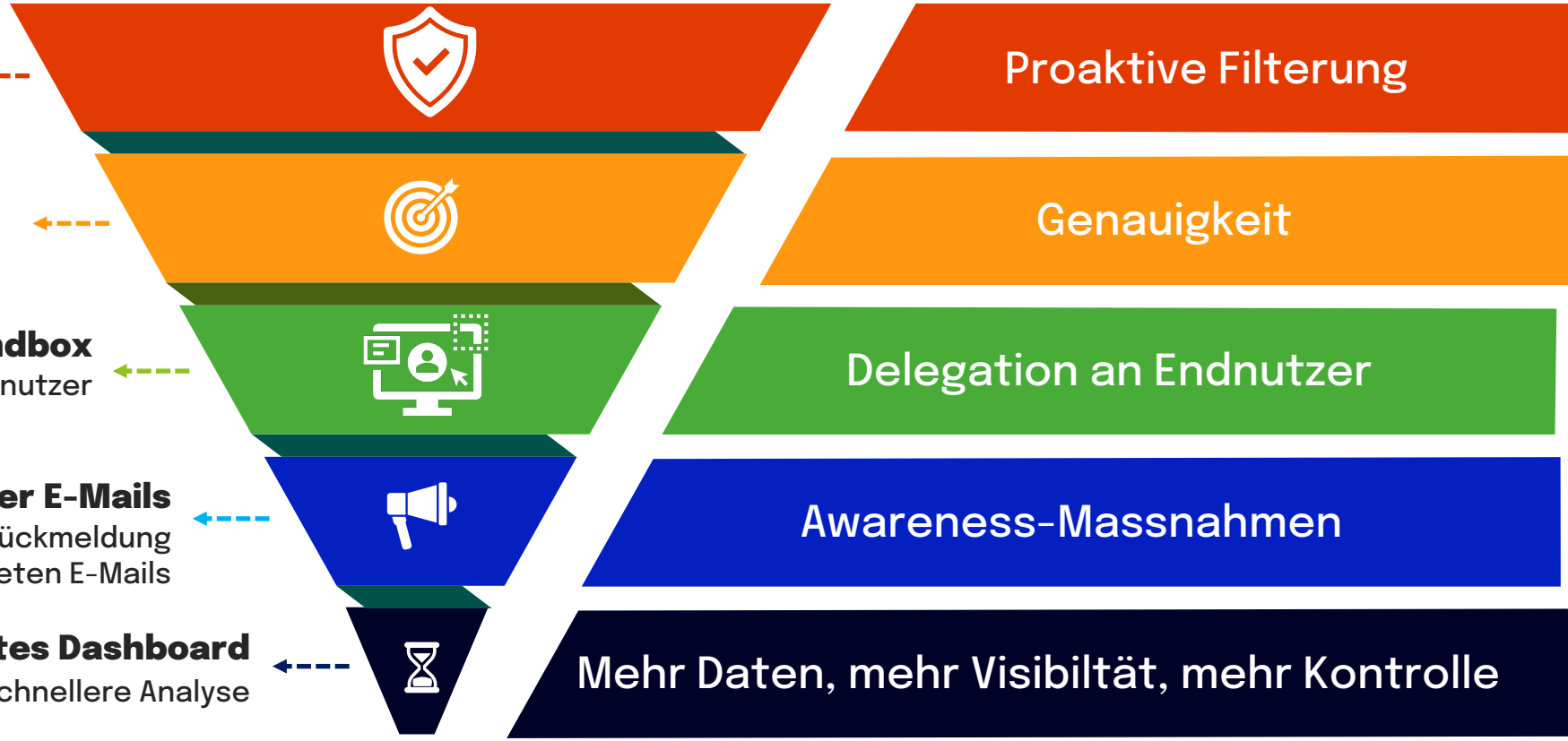
**Kontext-Intelligenz**
Mind. 4x mehr Phishing geblockt

**Qualität der Erkennung**
Ca. 70% weniger Fehlalarme (Falsch-Positive)

**Quarantäne & Sandbox**
Schutz & Sichtbarkeit aller Endnutzer

**Melden verdächtiger E-Mails**
Bis zu 90% automatisierte Rückmeldung von gemeldeten E-Mails

**Transparentes Dashboard**
Bis zu 95% schnellere Analyse



# Benefits

## 4x mehr Bedrohungen blockiert

im Vergleich zu gängigen professionell betriebenen Umgebungen

## 1.500 Stunden Zeitersparnis

pro Jahr bei der Bearbeitung gemeldeter E-Mails durch das Sicherheitsteam

## Hunderte von Signalen pro E-Mail

werden mit den erwarteten Kommunikationsmustern abgeglichen, um Bedrohungen zu erkennen

Quelle: Basierend auf xorlab-Daten für Kunden mit durchschnittlich 5'000 E-Mail-Postfächern.



“xorlab ist eine der wenigen Cybersicherheitslösungen, die zusätzliche Sicherheit bieten und Kosten sparen helfen.”

Michael Meli

CISO

Julius Bär



“Durch die Aktivierung der xorlab Security Platform,sind unsere Phishing-Meldungen über Nacht um 60% zurückgegangen.”

Dominic Alber

Head of Cyber Defense

Vontobel



“Die beziehungsbasierte Bedrohungserkennung von xorlab stoppt gezielte Angriffe und produziert nur sehr wenige Falsch-Positive.”

Alexander Bösch

CISO

Implenia®

# E-Mail Security neu gedacht

## Bereiche

1. Kontext-sensitive Banner für bessere Endnutzer Experience
2. Third Party Risk Intelligence Dashboard
3. Schwarmintelligenz durch Adaptive Policy Sharing

**Invoice from new external organization**

#newsender #neworg #invoice #careful

If you have not expected this message please ignore or report it.

**New external sender**

The external sender is not known to us, but the organization is. If you have not expected this message, please ignore or report it.

**Increased communication activity with external sender**

Be cautious with new relationships in new communication channels. When in doubt, please report the message.

# E-Mail Security neu gedacht

## Bereiche

1 Kontext-sensitive Banner für bessere Endnutzer Experience

**2 Third Party Risk Intelligence Dashboard**

3 Schwarmintelligenz durch Adaptive Policy Sharing



# E-Mail Security neu gedacht

## Bereiche

1 Kontext-sensitive Banner für bessere Endnutzer Experience

2 Third Party Risk Intelligence Dashboard

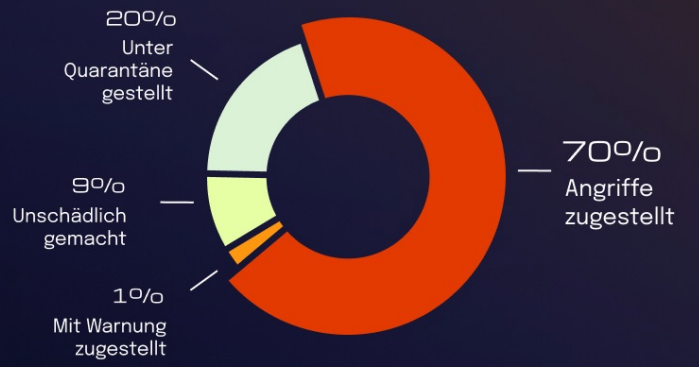
**3 Schwarmintelligenz durch Adaptive Policy Sharing**



# E-Mail Attack Simulation




## xorlab Bericht Angriffssimulation




| | Gesendet | Gestoppt | Zugestellt |
|---|---|---|---|
| Phishing mit Link | 130 | 11 | 119 |
| Phishing mit Anhang | 25 | 0 | 25 |
| Malware | 57 | 41 | 16 |
| Business Email Compromise | 4 | 0 | 4 |

xorlab



# Boost your e-mail!

**Benjamin Hindelang | Account Executive**

benjamin.hindelang@xorlab.com

Diese Organisationen vertrauen auch auf xorlab:

Julius Bär · Vontobel · Zürcher Kantonalbank · coop · USZ Universitäts Spital Zürich · HAUFE

KIRCHHOFF AUTOMOTIVE · DIE POST · swisscom · Implenia · CERN · VISANA

# 100.000 Schwachstellen – was nun?

Strategien zur effektiven Schwachstellenbehebung

Aleksander Groshev – CEO

Autobahn security

# Autobahn Security ist Spezialist im Bereich **Schwachstellen Priorisierung** und hilft Kunden bei der Stärkung ihrer Hacking Resilienz

## The pain we solve

*"Companies gain little insights from their cyber data – until Autobahn Security prioritizes and translates data into actions."*

## Our history

- Initial entwickelt vom Cyber Think Tank Security Research Labs
- Kunden in mehr >20 Ländern und verschiedenen Branchen
- Büros in Berlin, Jakarta und Singapur

## Founded by



**Dr. Karsten Nohl – Chief Scientist**

- Hacking Koryphäe und Sicherheitsforscher
- Mehrfacher CISO
- Keynote Speaker



**Aleksander Groshev – CEO**

- SaaS B2B Product Leader
- IT-Security Experte
- Startup Experte

## Trusted by

SAP Customer Experience · Allianz · Taboola · Rakuten Symphony · SWISS POST Yellow in motion. · KNIPEX · MISTER SPEX · LOGWIN · *...and more*

# Jeder der mit IT-Schwachstellen zu tun hat, kennt mindestens eines dieser Probleme



*AI generiert

1. **Fragmentierte Tools**
   Jonglieren mehrerer Scanner für unterschiedliche Zwecke (Web, Netzwerk, Code, etc.)

2. **Priorisierungs-Puzzle**
   Mit begrenzten Ressourcen entscheiden, welche Schwachstellen priorisiert werden sollen

3. **Überlastete Teams**
   Sicherheits- und IT-Teams ertrinken in Listen an Schwachstellen und Behebungstickets

# 1 Fragmentierte Tools




* echt

> **Inkonsistente Daten**
> Verschiedene Scanner verwenden unterschiedliche Methoden und Bewertungssysteme, was zu inkonsistenten Daten und Vergleichsschwierigkeiten führt

> **Tool-Überlastung**
> Die Verwaltung mehrerer Dashboards, Schnittstellen und Berichtssysteme erhöht den Arbeitsaufwand und das Fehlerrisiko

> **Begrenzte Sichtbarkeit**
> Silo-Daten von einzelnen Scannern verhindern einen ganzheitlichen Überblick über die gesamte Hacking Resilienz

# 2 Priorisierungs-Puzzle im Security Team



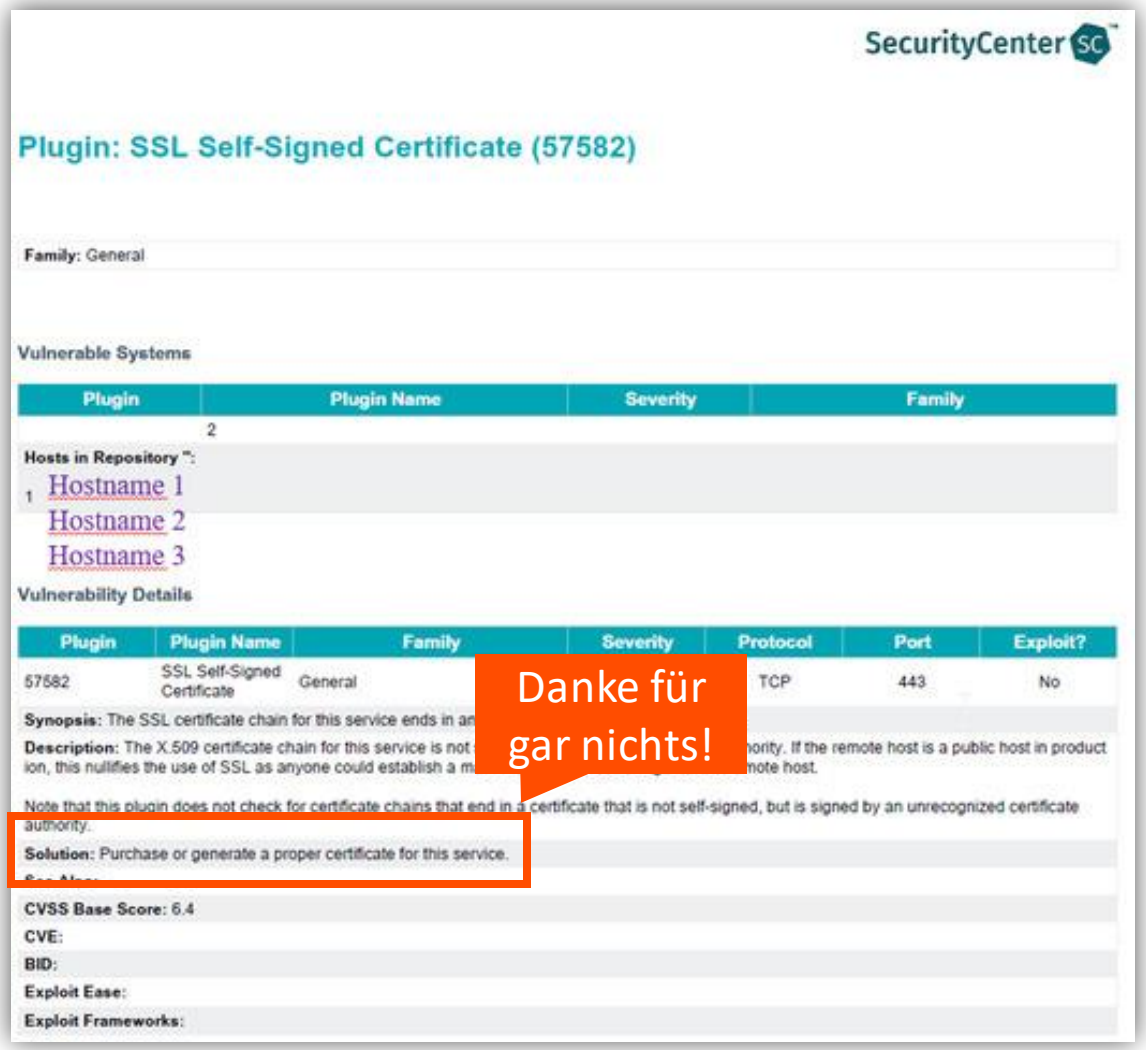
*AI generiert

> **Überwältigende Menge**
> Schiere Anzahl von Schwachstellen erschwert eine effektive Priorisierung, was verschwendeten Ressourcen und Demotivation führt

> **Kontextuelle Faktoren ignoriert**
> Kontextuelle Faktoren wie Kritikalität der betroffenen Assets oder die Ausnutzbarkeit der Schwachstelle selbst werden oft nicht berücksichtigt

> **Überlastung durch manuelle Bewertungen**
> Security Teams verbringen zu viel Zeit mit der **manuellen** Bewertung und Priorisierung von Schwachstellen, wodurch Ressourcen von anderen wichtigen Aufgaben abgezogen werden

# 3 Überlastete IT- und DevOps Teams




* echt

> **Schwachstellenlawinen**
> Der ständige Zustrom von Schwachstellen Reports führt zu einem Rückstand an unbearbeiteten Tickets, was zu Burnout und Demotivation führt

> **Überlastung der Behebung**
> Manuelle Behebungsprozesse sind zeitaufwändig und fehleranfällig, was die IT-Teams zusätzlich belastet

> **Begrenzte Sichtbarkeit**
> Der Mangel an zentraler Sichtbarkeit in den Behebungsfortschritten behindert die effektive Ressourcenallokation.

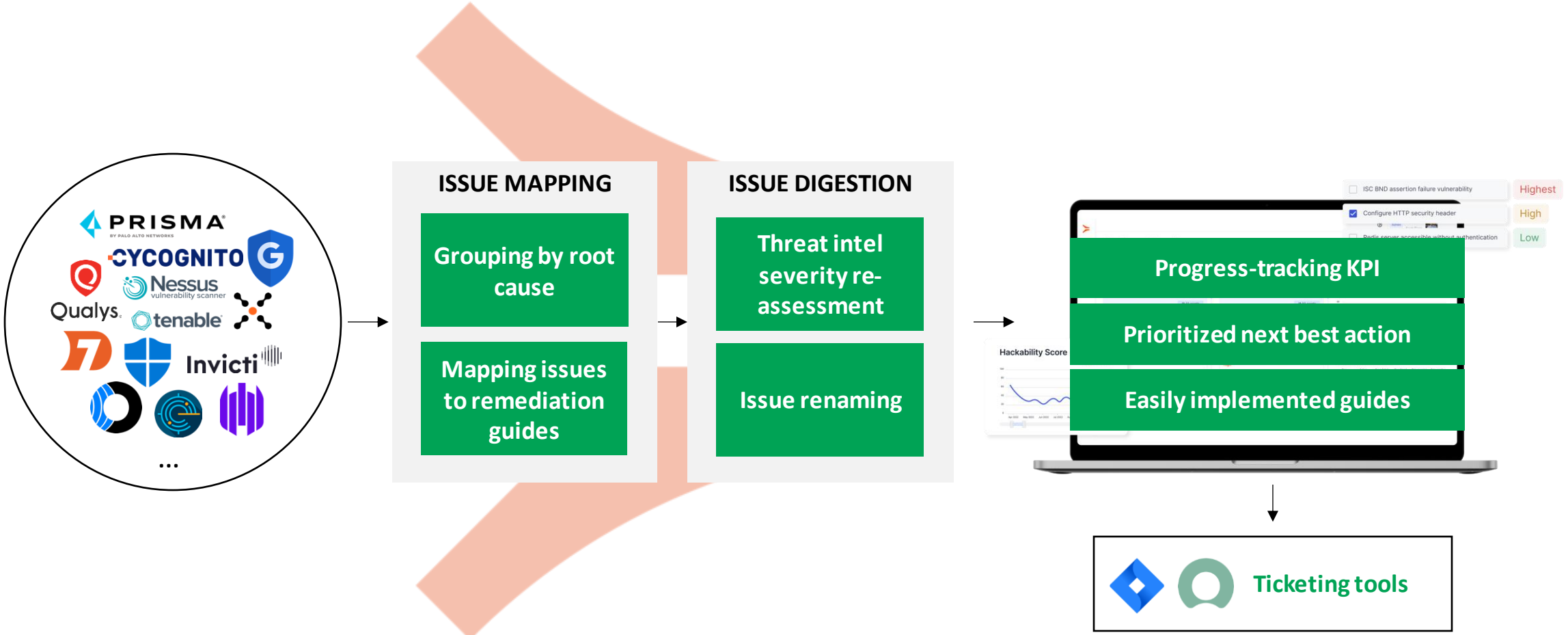
# Wie kann ich mein Unternehmen und meine Teams befähigen?

| Scan | Aggregate | Prioritize | Remediate | Report |
|---|---|---|---|---|
| ▪ Prüfen, welche Scanner **wirklich** relevant sind | ▪ Daten in **einer Plattform** zusammenführen | ▪ Echte “Severity“ der Schwachstelle und **Kritikalität** des Assets prüfen | ▪ Schwachstellen nach Root Cause gruppieren | ▪ Möglichst eine zentrale KPI reporten |
| ✓ Best-of-breed Scanner | ✓ Excel, Grafana und co.<br>✓ Aggregation Tools | ✓ Excel, Grafana und co.<br>✓ Prioritization Tools | ✓ Excel, Grafana und co.<br>✓ Auto Patch Tools | ✓ Excel, Grafana und co.<br>✓ Reporting Tools |

Selbst entwickeln oder outsourcen -> teuer, große Freiheit und Flexibilität

Automation Tooling einkaufen -> preiswert, ggf. eingeschränkte Flexibilität

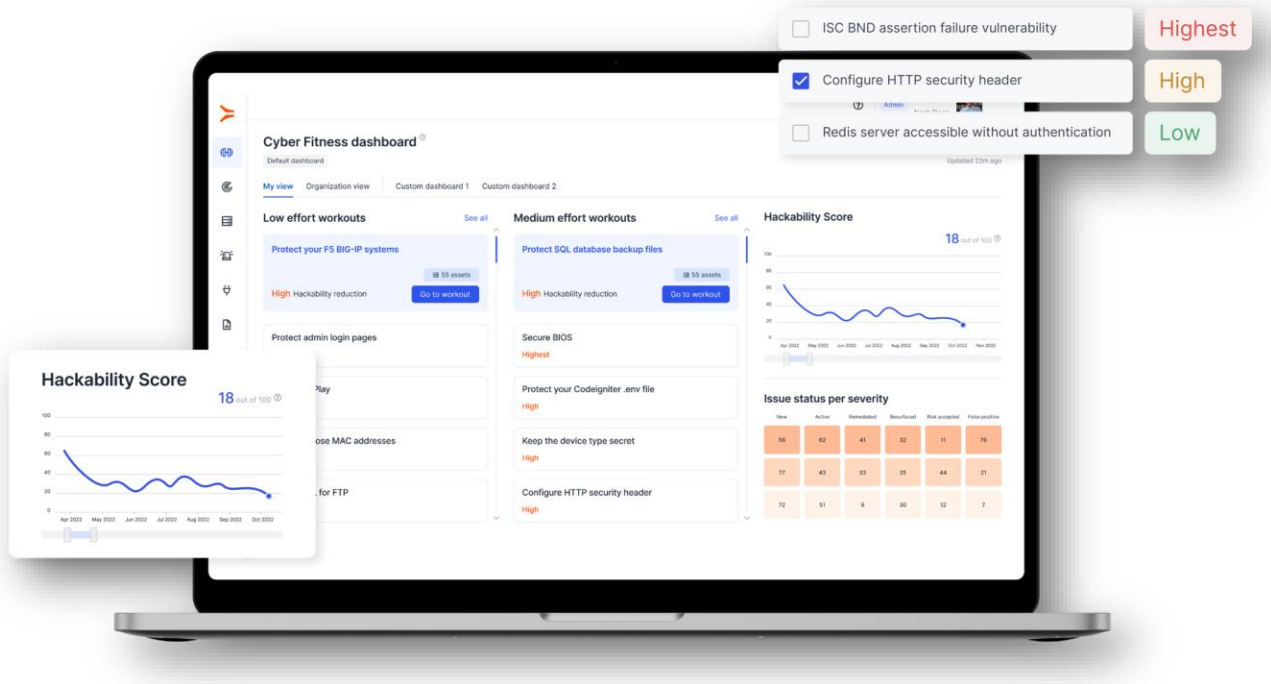
# Durch Automatisierung von Arbeitsabläufen können Schwachstellen bis zu 90 % schneller behoben werden



# Anstatt lange Listen von Schwachstellen durchzugehen, konzentrieren sich User auf die Root Causes der Schwachstellen und deren Auswirkung auf die Hacking-Resilienz

**Summary of Top 20 Critical Severity Vulnerabilities to be Remediated**

| Plugin Name | Severity | Total |
|---|---|---|
| Unsupported Unix Operating System | Critical | 20 |
| MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check) | Critical | 12 |
| MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check) | Critical | 11 |
| MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) | Critical | 9 |
| MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732) | Critical | 9 |
| MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check) | Critical | 9 |
| MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check) | Critical | 9 |
| MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) | Critical | 8 |
| MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470) | Critical | 8 |
| MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414) | Critical | 7 |
| MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058) | Critical | 7 |
| MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check) | Critical | 5 |
| MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369) | Critical | 5 |
| MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594) | Critical | 5 |
| Adobe Flash Player Unsupported Version Detection | Critical | 5 |
| MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) | Critical | 5 |
| MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) | Critical | 5 |
| Microsoft Windows XP Unsupported Installation Detection | Critical | 4 |



# Durch die Bereitstellung von detaillierten Behebungs-Guides kann IT / DevOps Schwachstellen effizienter schließen

SecurityCenter

## Plugin: SSL Self-Signed Certificate (57582)

**Family:** General

**Vulnerable Systems**

| Plugin | Plugin Name | Severity | Family |
|---|---|---|---|
| | 2 | | |

**Hosts in Repository ":**

1 Hostname 1
Hostname 2
Hostname 3

**Vulnerability Details**

| Plugin | Plugin Name | Family | Severity | Protocol | Port | Exploit? |
|---|---|---|---|---|---|---|
| 57582 | SSL Self-Signed Certificate | General | | TCP | 443 | No |

**Synopsis:** The SSL certificate chain for this service ends in an

**Description:** The X.509 certificate chain for this service is not ... ority. If the remote host is a public host in product ion, this nullifies the use of SSL as anyone could establish a ... emote host.

... certificate that is not self-signed, but is signed by an unrecognized certificate authority.

**Solution:** Purchase or generate a proper certificate for this service.

**CVSS Base Score:** 6.4

**CVE:**

**BID:**

**Exploit Ease:**

**Exploit Frameworks:**

Danke für gar nichts!

### Renew the SSL certificates for your web servers

**Remediation option 1 - Linux**

- **1 - Connect to your web server via SSH**

Connect to your web server via SSH by running the following command in your Terminal:

```
ssh <user>@<web_server_ip>
```

- **2 - List your certificates**

```
sudo certbot certificates
```

A list with all the installed certificates and their details will be displayed.

- **3 - Renew certificates**

The following command will renew all the installed certificates that are near to expire:

```
sudo certbot renew
```

- **4 - Automate the certificate renewal**

You can use **crontab** to automate the renewal of the certificates. Edit the crontab entries by running:

```
sudo crontab -e
```

Add the following line at the end of the file

```
0 1 * * * certbot renew --non-interactive
```

**Note**

Automatic renewal is implemented and enabled by default in the latest **certbot**. You can find more about it here

# Zum kostenfreien Whitepaper:

Aleksander Groshev – CEO
agroshev@autobahn-security.com

Autobahn security

# Cybercrime-Trends, die Sie 2024 kennen sollten & Einblicke in Next-Generation Awareness Training



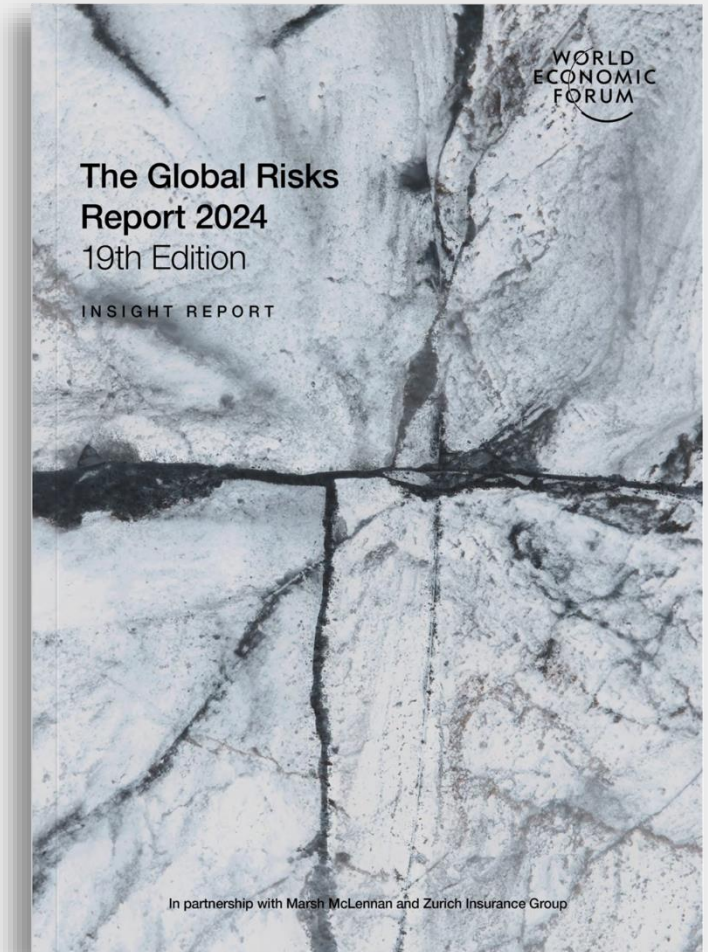
Die Macht des menschlichen Faktors in Zeiten von KI

sosafe

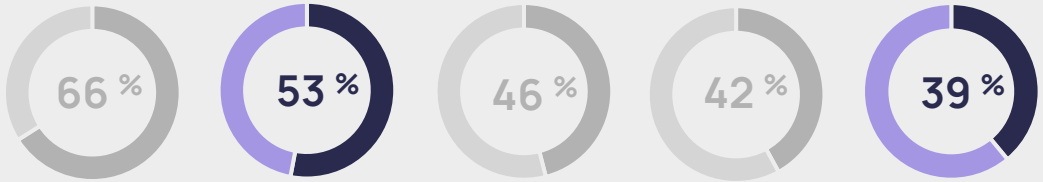
Juni 2024

EXPERTEN WELTWEIT SIND SICH EINIG

# Zu den größten gesellschaftlichen Risiken gehören 2024 KI-gesteuerte Desinformation und Cyberbedrohungen.




WORLD ECONOMIC FORUM




| 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|
| Extreme Wetter-ereignisse | KI-gesteuerte Fehl- und Desinformation | Gesellschaftliche bzw. politische Polarisierung | Krise bei Lebenshaltungs-kosten | Cyber-bedrohungen |

Quelle: World Economic Forum, 2024.

ÜBER SOSAFE

# Europäischer Marktführer im Human Risk Management

GERRY WEBER · SOS CHILDREN'S VILLAGES · CLARK · WWF · DeepL · ALDI MARKT · DAIMLER TRUCK · TUI · ADAC

BAUERFEIND · SCHÜCO · Handelsblatt · VORWERK · DACHSER Intelligent Logistics · CANYON · WAGO

## Warum unsere Kunden uns vertrauen

**Verhaltenspsychologisch fundiert**

**Benutzerfreundlich, anpassbar und skalierbar**

**100 % Compliance mit DSGVO und ISO 27001**

**450+**
Mitarbeitende vielfältiger Hintergründe

**4.500+**
Kunden aus verschiedensten Branchen

**3.000.000+**
Nutzende weltweit





DIESES JAHR KOMMT ES ZUM SHOWDOWN

# Die Angriffstrends, die Sie 2024 kennen müssen

## 1 Künstliche Intelligenz



## 2 Quantum Hacking



## 3 Professionalisierung der Cyberkriminalität



## 4 Globale Spannungen und Hacktivismus



## 5 Disinformation-as-a-Service



## 6 Öffentlicher Sektor und kritische Infrastrukturen



## 7 Pretexting und Multichannel-Strategien

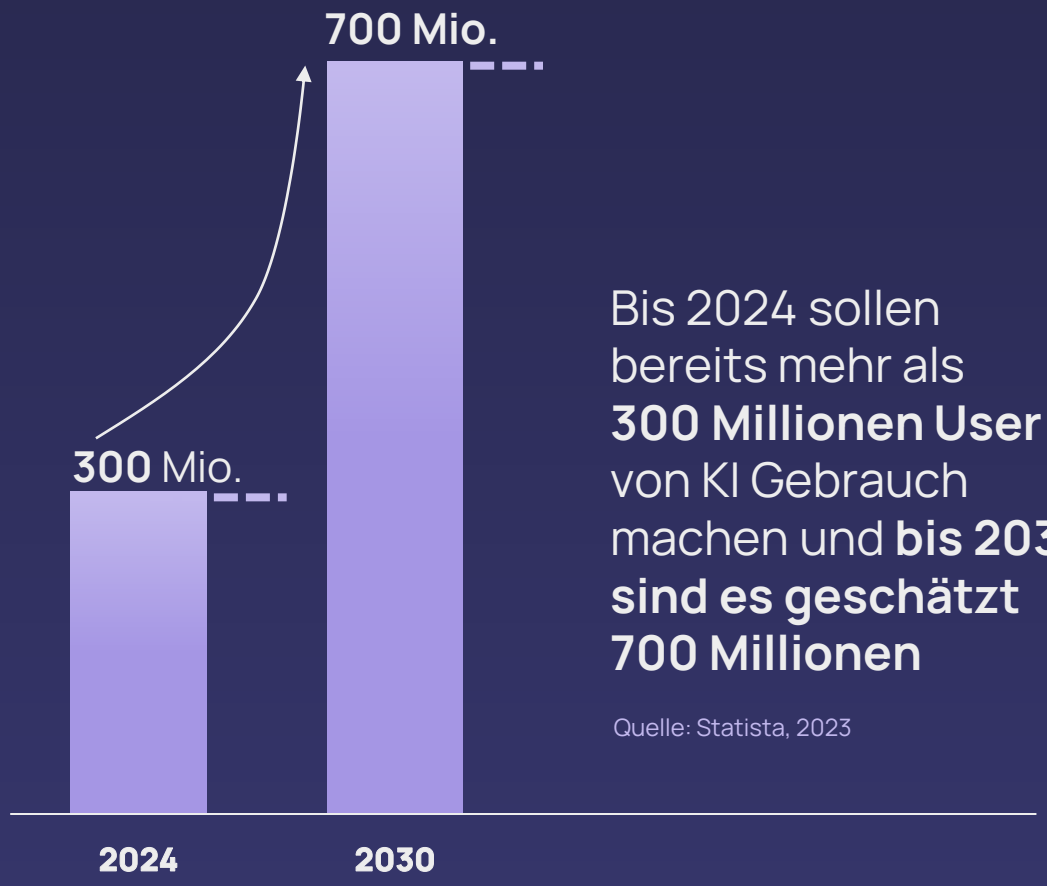


## 8 Steigende Burnout-Zahlen



KI VERÄNDERTE IM VERGANGENEN JAHR DIE WELT

# Trotzdem haben wir das volle Potenzial generativer KI in der Cybersicherheit noch nicht gesehen




Bis 2024 sollen bereits mehr als **300 Millionen User** von KI Gebrauch machen und **bis 2030 sind es geschätzt 700 Millionen**

Quelle: Statista, 2023

the decoder

**NCSC warnt: KI wird Ransomware-Bedrohung in den nächsten zwei Jahren verstärken**

CSO

GOOGLE-PROGNOSE 2024

**GenAI verstärkt Phishing-Kampagnen**

KI ENTWICKELT SICH IN RASANTEM TEMPO

# KI-generierte Deepfakes sind überzeugend realistisch – und oft erfolgreich

CSO

DEEPFAKE-BETRUG

**Betrüger ergattern 23 Millionen Euro mit Fake-Videokonferenz**

Jeder **4.**



wurde bereits Opfer von **Voice-Cloning** oder kennt jemanden, der es schon mal erlebt hat.

Quelle: McAfee

> Die technischen Möglichkeiten im Bereich **künstlicher Intelligenz und Deep Fakes** sind im letzten Jahr enorm gewachsen.



**Michael Brandes**
Head of Cyber Strategy, Governance, Assurance & Risk Management Merck KGaA

LARGE-LANGUAGE-MODELLE SCHREITEN EBENSO SCHNELL VORAN

# Die neue Möglichkeit, mit OpenAI personalisierte GPTs zu erstellen, schafft vielfältige Angriffsvektoren für Cyberkriminelle

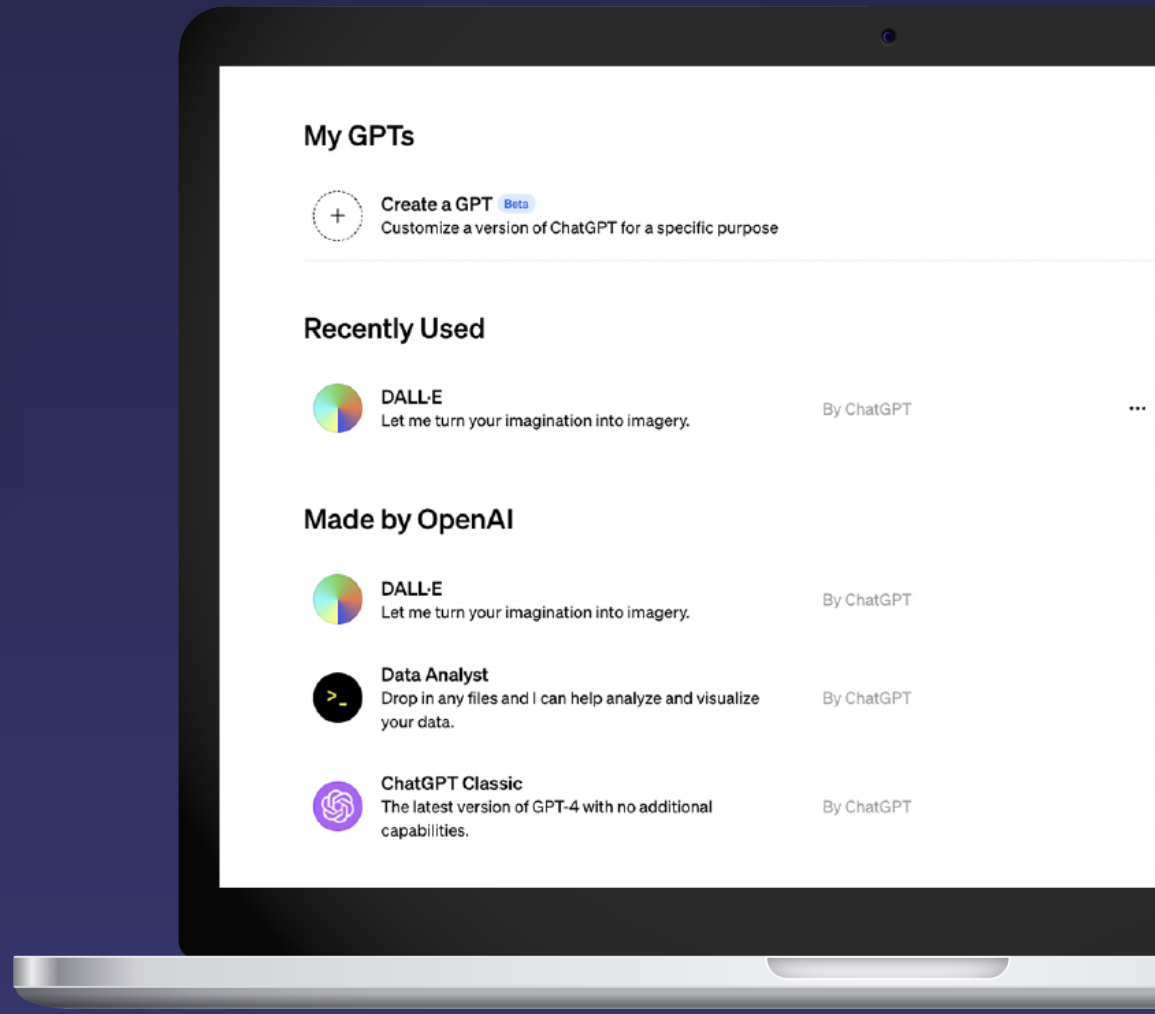
DARKREADING

CYBER RISK | DATA PRIVACY

**OpenAI's New GPT Store May Carry Data Security Risks**

The Washington Post
*Democracy Dies in Darkness*

**Chatbots are so gullible, they'll take directions from hackers**



UND CHATGPT IST NICHT DAS EINZIGE LLM

# Es sind zahlreiche schädliche Sprachmodelle im Umlauf

CHIP

**WormGPT ist das ChatGPT für Kriminelle: So gefährlich ist die neue KI**

Handelsblatt

WormGPT und FraudGPT

**KI macht auch „weniger Talentierte“ zu Trickbetrügern**

netzwoche

Generative AI ohne Moral

**WormGPT – der Chatbot, dem Cybergauner vertrauen**



FOLGEN VON RANSOMWARE-AS-A-SERVICE

# Die Professionalisierung der Cyberkriminalität erreicht 2024 ein neues Level der Profitabilität




**31%**

der Organisationen, die in den letzten drei Jahren Opfer eines Cyberangriffs wurden, hatten es mit **Ransomware** zu tun.

**4,54 Mio. USD**

**kostet Unternehmen ein erfolgreicher Ransomware-Angriff** durchschnittlich – das Lösegeld nicht einberechnet.

**x 2**

**2023 verdoppelte** sich die Anzahl an **Opfern von Ransomware-Angriffen** im Vergleich zum Vorjahr.

**Ransomware-as-a-Service**: Angreifende brauchen heutzutage keine IT- oder Hacking-Kenntnisse mehr – eine kurze Suche im Darkweb und eine schnelle Kryptozahlung reichen aus, um weitreichende Ransomware-Angriffe auszuführen:

heise online

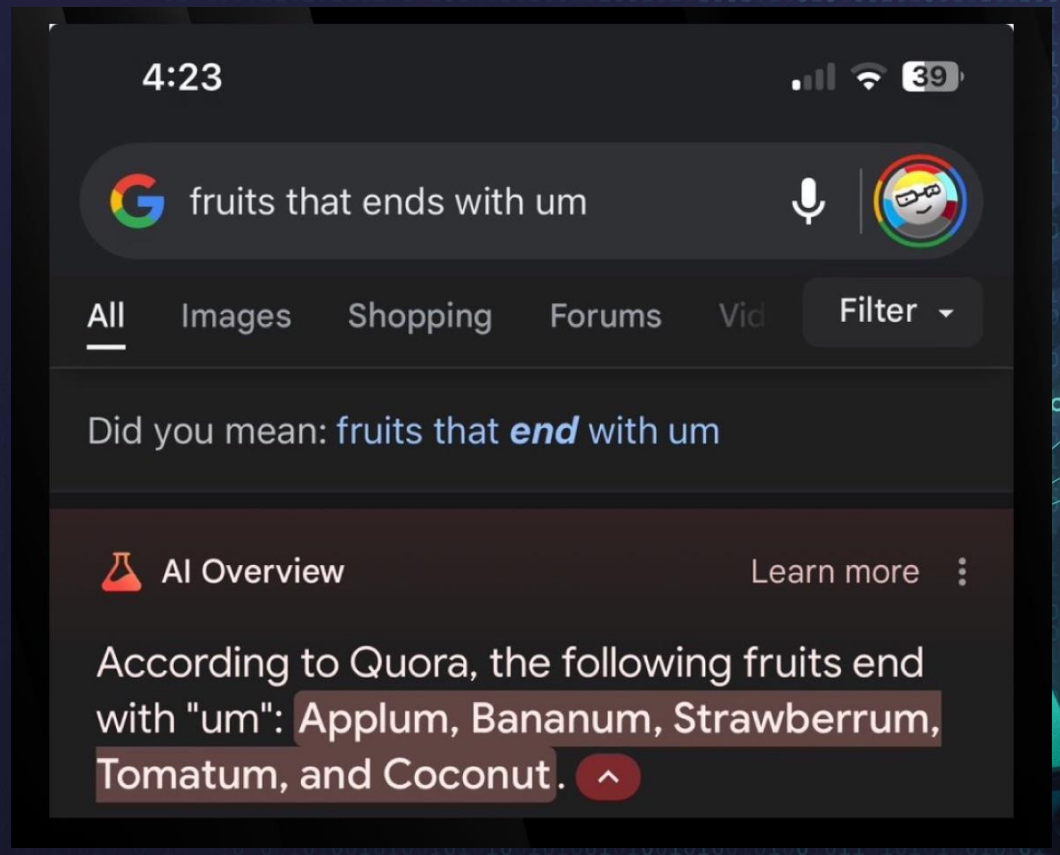
Cybercrime: US-Versicherung zahlte angeblich 40 Millionen als Lösegeld

PC-WELT

**Kaseya: Erpresser fordern 70 Millionen Dollar Lösegeld**

Quellen: Human Risk Review 2023, IBM's Cost of a data breach 2022; Back Kite, 2023.

# Es gibt noch Hoffnung 😎






sosafe

# Wie nutzen Angreifende die Verhaltenspsychologie, um uns zu manipulieren?



DIE TYPISCHE VORGEHENSWEISE

# Globale Ereignisse bieten perfekte Voraussetzungen für Phishing-Angriffe...

(Geopolitische) Krisen

zdf heute

"Neue Eskalationsstufe" bei USA und China

TAGESSPIEGEL

**Vor Besuch von Nancy Pelosi** Hacker legen Webseite der taiwanischen Präsidentin lahm

Süddeutsche Zeitung

**Der erste echte Cyberkrieg**

Cyber-Kriegsführung

ntv

Israel und der Iran

**Der Schattenkrieg tritt in eine neue Phase**

Handelsblatt

**Wie die KI für Hacker zur Waffe wird**

Deglobalisierung

Technologische Innovationen

ZDNET

**VALL-E: AI-Modell für Text-to-Speech von Microsoft simuliert Stimmen**

ZDNET

**Kaseya-Ransomware-Angriff: Rund 1500 Unternehmen betroffen**

heise online

Ransomware: Wachsende Bedrohung durch Professionalisierung

Professionalisierung von Cybercrime

sosafe

EMOTIONAL AUFGELADEN

# … und die Angriffe spielen erfolgreich mit unseren Emotionen und Reaktionen.

BBC

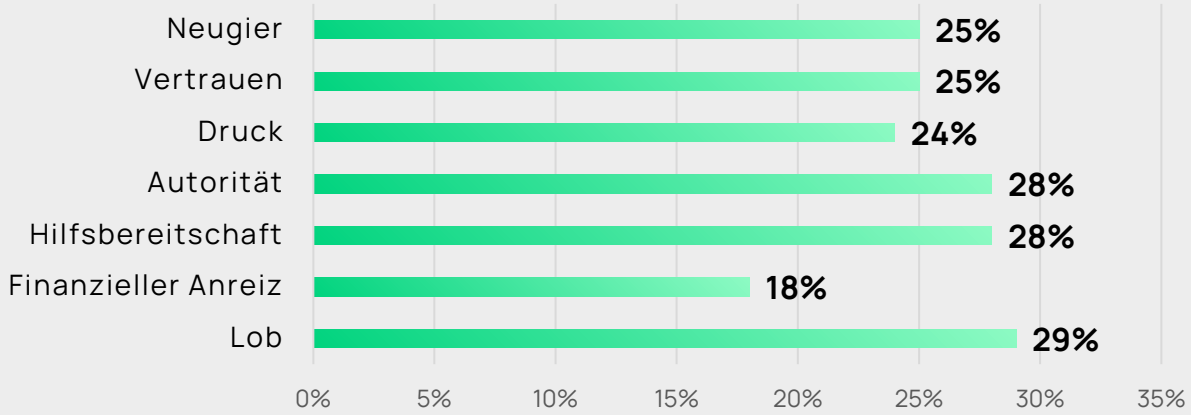
**Ukraine war: Investigation finds hundreds of fake charity websites**

Mit jeder neuen Krise kommt es zu einer **emotionalen Reaktion** der Öffentlichkeit – Menschen wollen an wohltätige und humanitäre Organisationen spenden.
Da **Kriminelle von Geld angezogen** werden, nehmen sie genau den Sektor ins Visier, der ohnehin nicht über die nötigen Ressourcen für Cybersicherheitsmaßnahmen verfügt.“

**Stéphane Duguin**
CEO des CyberPeace Institute

CyberPeace Institute

Klickraten **nach emotionalen Manipulationstechniken** 2022



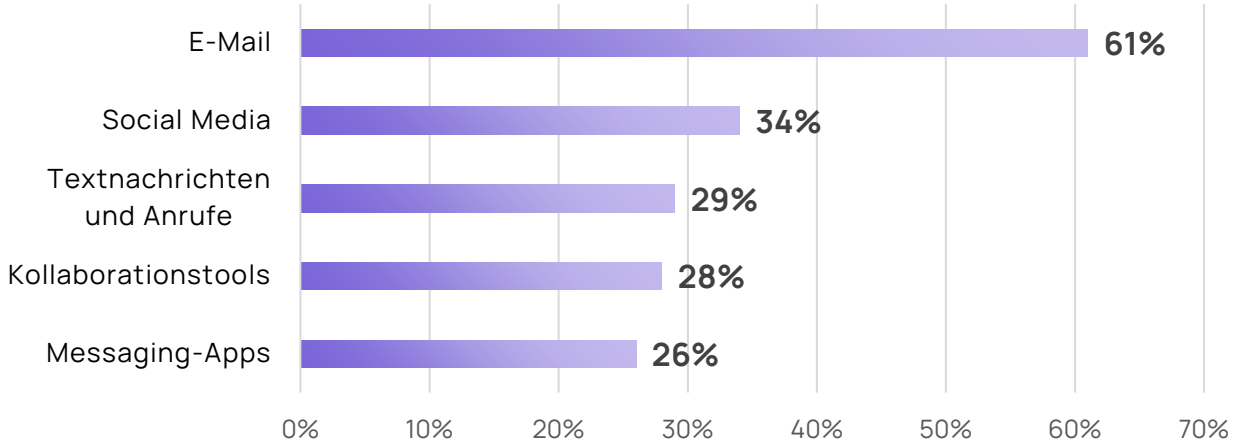

Die **Top 5** Phishing-Betreffzeilen 2022

1. **Auto beschädigt** Druck/Neugier
2. **Teams-Einladung** Neugier
3. **Fehler in der Gehaltsabrechnung** Druck/Neugier
4. **Ihr Office Passwort läuft heute ab** Druck
5. **Teams verpasste Chatnachricht** Druck/Neugier

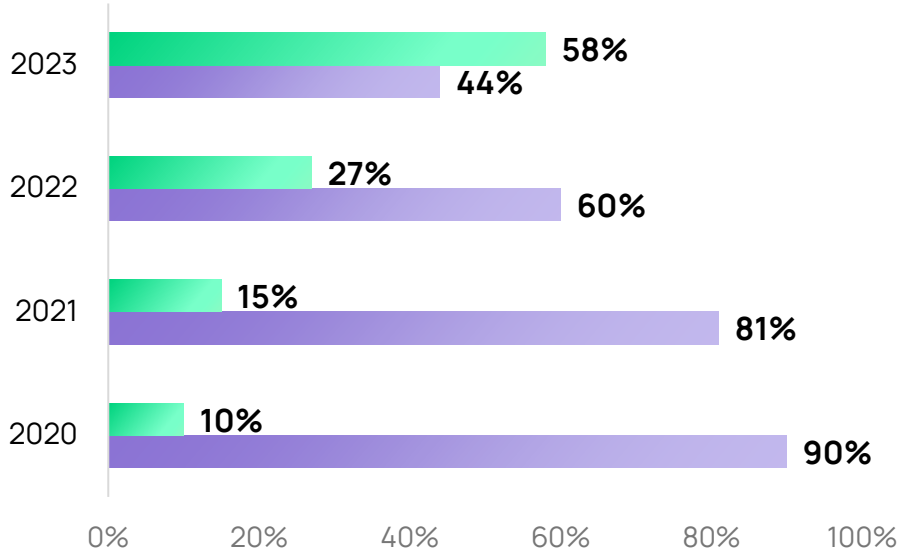
sosafe

# Neue Kommunikationskanäle bieten neue Eingangstore für Cyberkriminelle

**Kanäle**, über die Organisationen 2022 angegriffen wurden



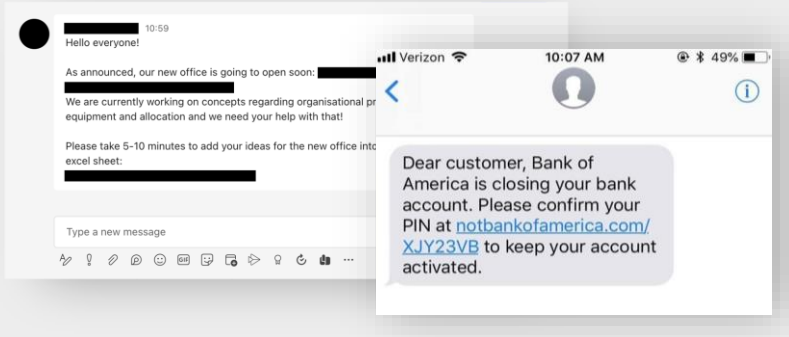

Pretexting doppelt so hoch und jetzt
**Nr. 1 der Social-Engineering-Methoden**




Verschiedene Strategien bei Social-Engineering-Angriffen

Pretexting Phishing

Betrug über Messaging-Apps




Text-nachrichten

sosafe



Quellen: Human Risk Review 2023; Verizon data breach reports 2020-2023; Digital Information World, 2022; Reader's Digest, 2023; We Live Security, 2022

TECHNOLOGISCHE INNOVATION MIT EXPLOSIVEN FOLGEN

# Generative KI macht es noch schwerer, Täuschungen zu erkennen

## Beispiel: Voice Cloning wird zu einer unmittelbaren Gefahr

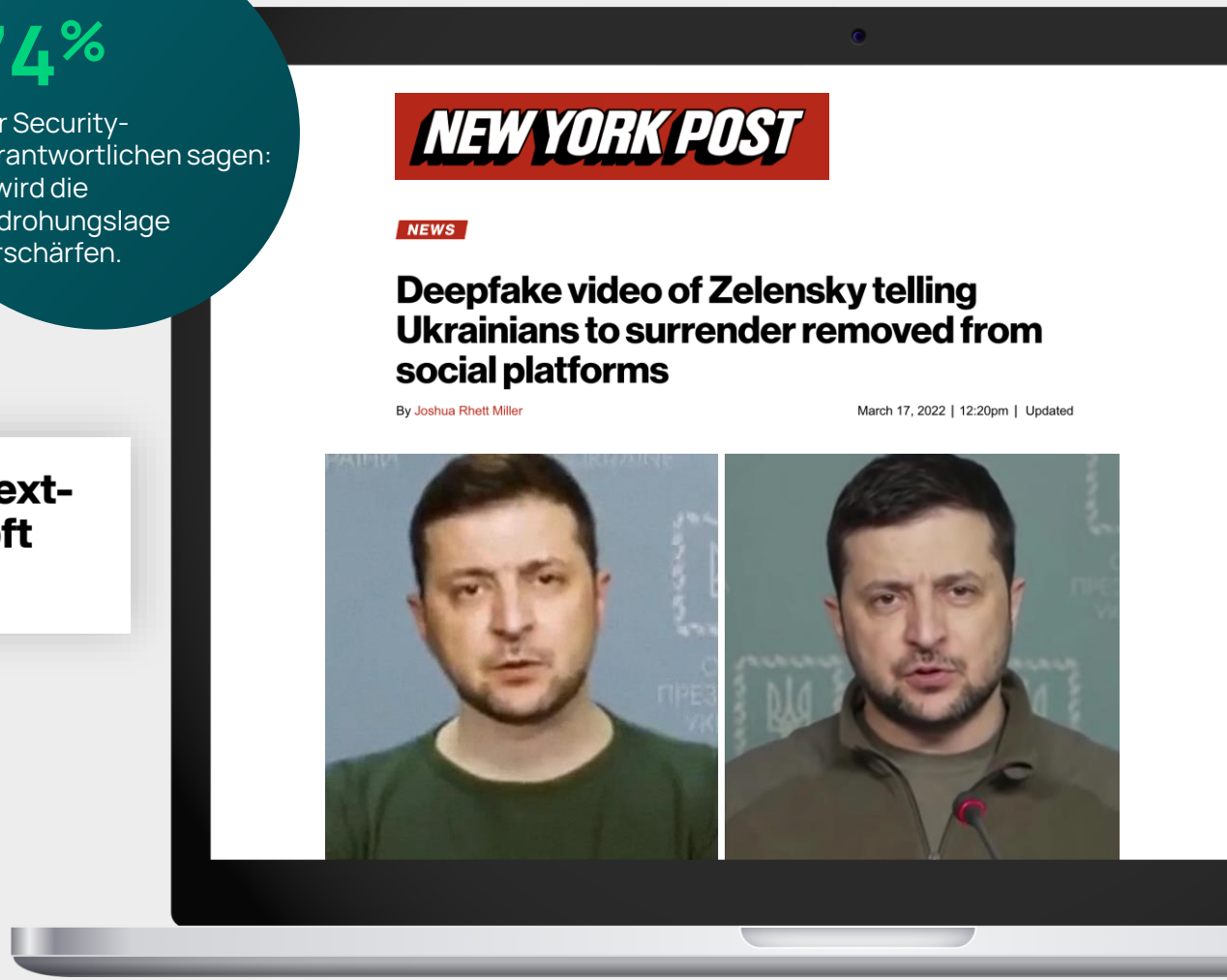
Angreifende imitieren Stimmen von Kolleginnen/Kollegen oder Vorgesetzten und:

→ Greifen **sensible Informationen** ab

→ Animieren die Opfer zu **Zahlungen per Telefon**

**74%**

Der Security-Verantwortlichen sagen: KI wird die Bedrohungslage verschärfen.




ZDNET **VALL-E: AI-Modell für Text-to-Speech von Microsoft simuliert Stimmen**

heise Betrugsmasche: Abzocke mit KI-generierter Stimme

Forbes Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

DAS FAZIT

## 2024 rückt der Faktor Mensch bei Cyberangriffen weiter in den Fokus

Allianz

**Cybervorfälle** sind laut Allianz Risk Barometer 2024 das **größte Geschäftsrisiko**

FORRESTER®

**An 90 % der Datenschutzverstöße wird der Faktor Mensch beteiligt sein**

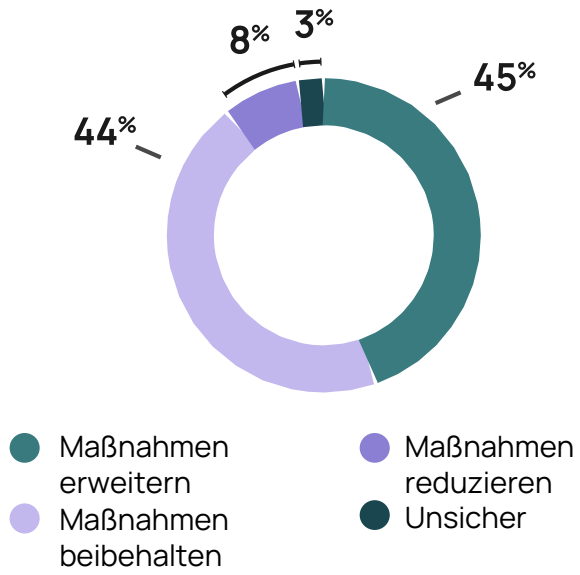
# Unsere Sicherheitsmaßnahmen werden erst dann wirklich wirksam, wenn wir uns – genau wie die Angreifenden – auf den Faktor Mensch fokussieren.

DIE GUTE NACHRICHT

# Organisationen binden Mitarbeitende verstärkt in ihre Verteidigung mit ein

**Die 3 höchsten Prioritäten Sicherheitsbeauftragter**

1. Security Awareness der Mitarbeitenden steigern
2. Identity und Access Management
3. Sicherheit von Hybrid Work verbessern




9 von 10 Organisationen werden die Security-Awareness-Maßnahmen im nächsten Jahr erhalten oder sogar steigern.

**Die effektivsten Hebel zur Steigerung der Security Awareness laut Sicherheits-verantwortlichen**

1. Awareness-Maßnahmen via Kommunikationstools
2. Personalisierte Lernmöglichkeiten
3. Customization des Awareness-Programms

DIE GUTE NACHRICHT

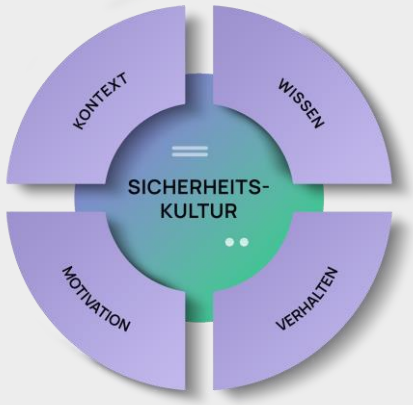
# Sicheres Verhalten geht „in Fleisch und Blut“ über

**Sicheres Verhalten ist das zentrale Element einer starken Sicherheitskultur:**

- Bildschirme sperren
- E-Mails scannen
- Risiken und Zwischenfälle zeitnah melden

**Sicheres Verhalten kann erreicht werden,** indem die vier Dimensionen einer auf den Faktor Mensch ausgerichteten Sicherheitsstrategie angewendet werden :

1. Wissen in Bezug auf Cybersicherheit
2. Kontextuelles Lernen und Tools
3. Intrinsische Motivation
4. Ganzheitlich sicheres Verhalten




## Die Ergebnisse von Sport-Thieme nach 1 Jahr mit SoSafe

- → Meldequote über 70 %
- → Klickrate auf 6 % gesunken
- → Zufriedenheit der Mitarbeitenden: 4,9/5

## Successful training at Natsana

„Bei SoSafe können wir sicher sein, dass das Gelernte langfristig hängen bleibt. Denn das kontinuierliche Training in Kombination mit der Lernpsychologie – das ist es, was am Ende wirklich hilft.“



**Lea Kehrmann**
Referentin der Geschäftsführung, Natsana

natsana.

CYBER-HEROES

# Reddit: Wie reale Menschen die Tragweite von Cyberangriffen einschränken können




**Vor 5. Februar 2023**

Ein Reddit-Mitarbeiter fällt auf einen ausgeklügelten Spear-Phishing-Angriff herein

**5. Februar 2023**

Nach weiterer Überlegung meldet er den Angriff an das Security-Team

**9. Februar 2023**

Nach den nötigen Eindämmungs- und Untersuchungsmaßnahmen macht Reddit den Verstoß öffentlich bekannt

CYBER-HEROES

# Reddit: Wie reale Menschen die Tragweite von Cyberangriffen einschränken können




## Entscheidende Faktoren

- → Starke Meldekultur: Schweigen verschlimmert das Ausmaß
- → Schnelles Erkennen des Vorfalls
- → Reddits transparenter Umgang mit dem Zwischenfall

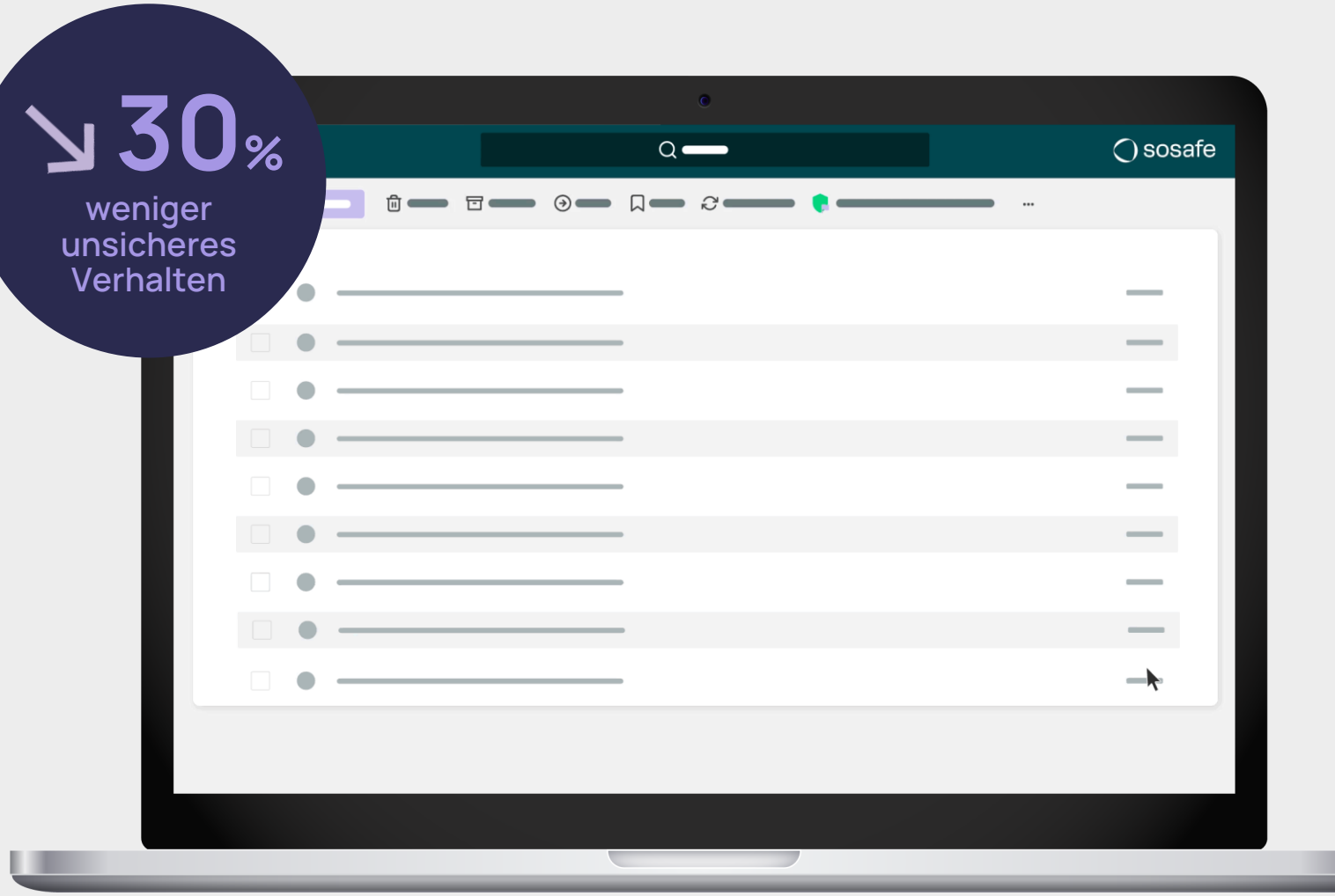
SICHERHEITSKULTUR

# PhishAssist: Situationsbezogene Awareness-Maßnahmen stärken die Meldekultur

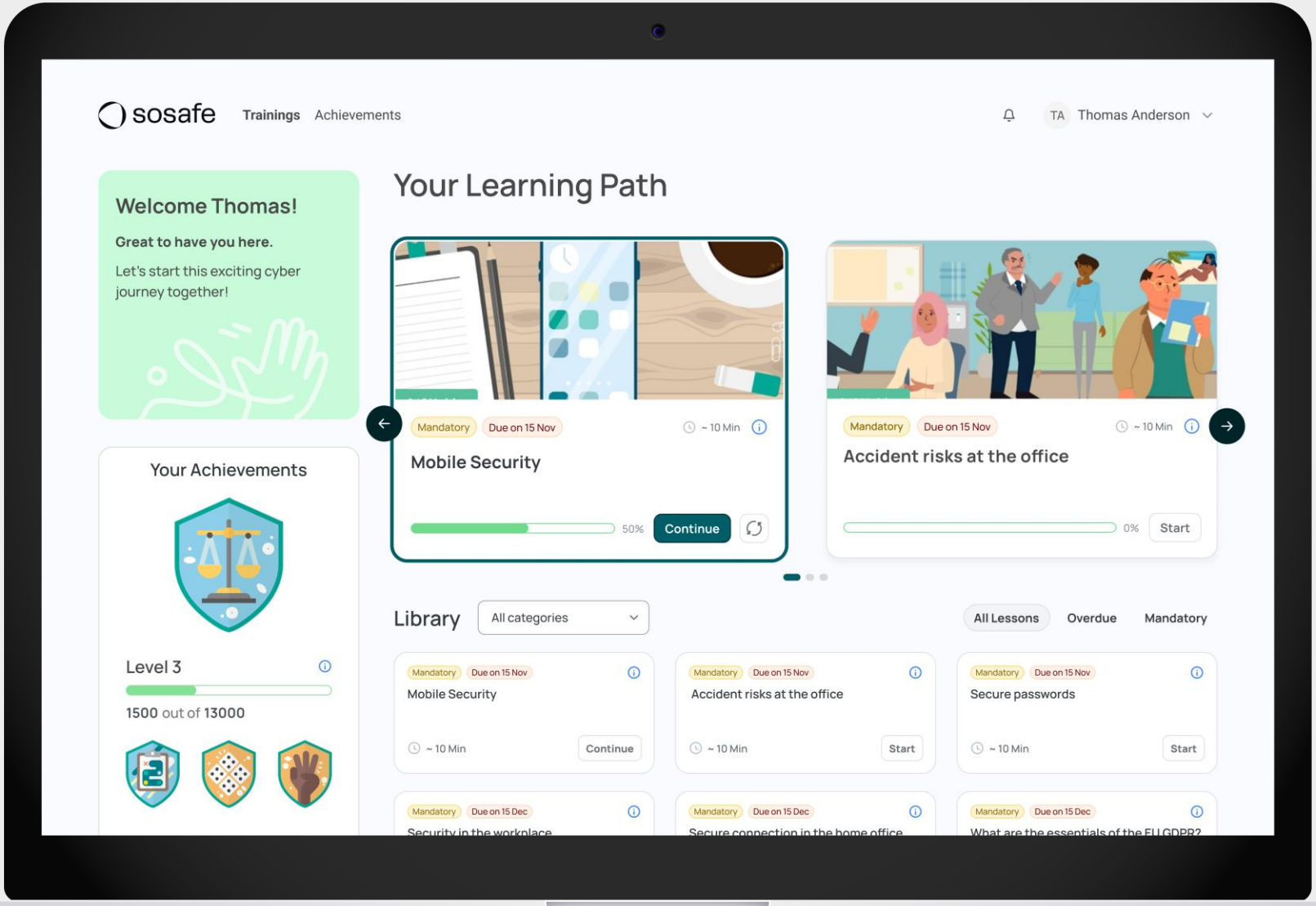
Bessere Meldequalität

Reduktion von Falschmeldungen

Kürzere Reaktionszeit bei realen Angriffen



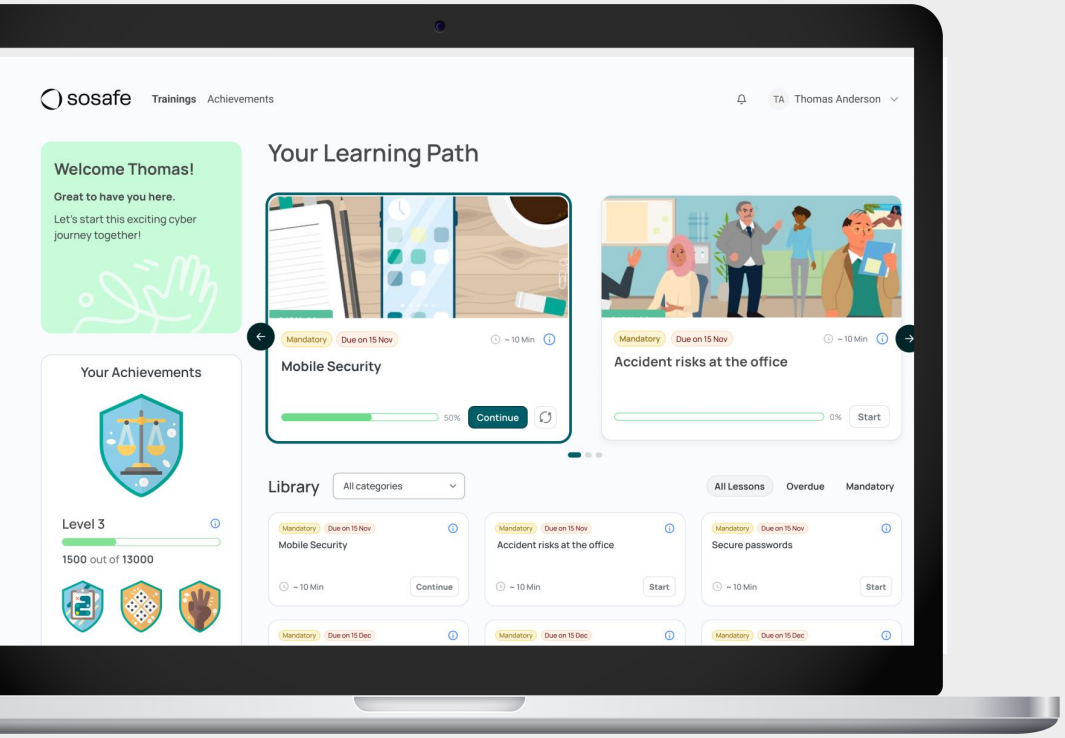

Quelle: Daten der SoSafe-Plattform




# Wir vereinfachen was andere kompliziert machen.

ZEITEFFIZIENTE RISIKOMINDERUNG

# Personalisiertes Lernen mit SoSafe: der schnellste Weg zur Verhaltensänderung




**JAHR 1**

↘ **30%**

weniger Zeitbedarf **bis zur Verhaltensänderung**

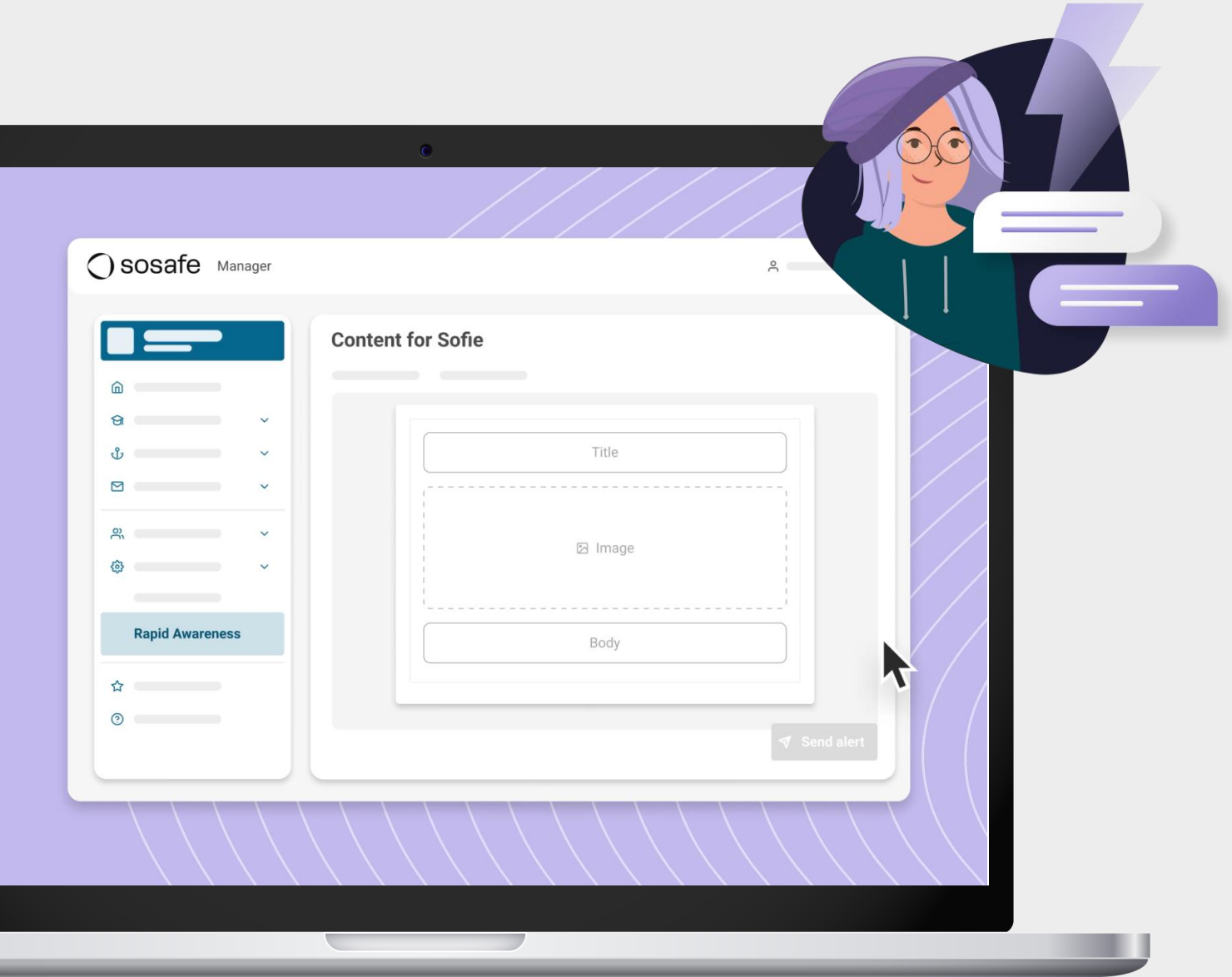
**AB JAHR 2**

↘ **50%**

weniger Zeitbedarf, um **neues Verhalten beizubehalten**

EIN DIREKTER DRAHT ZU IHREN MITARBEITENDEN

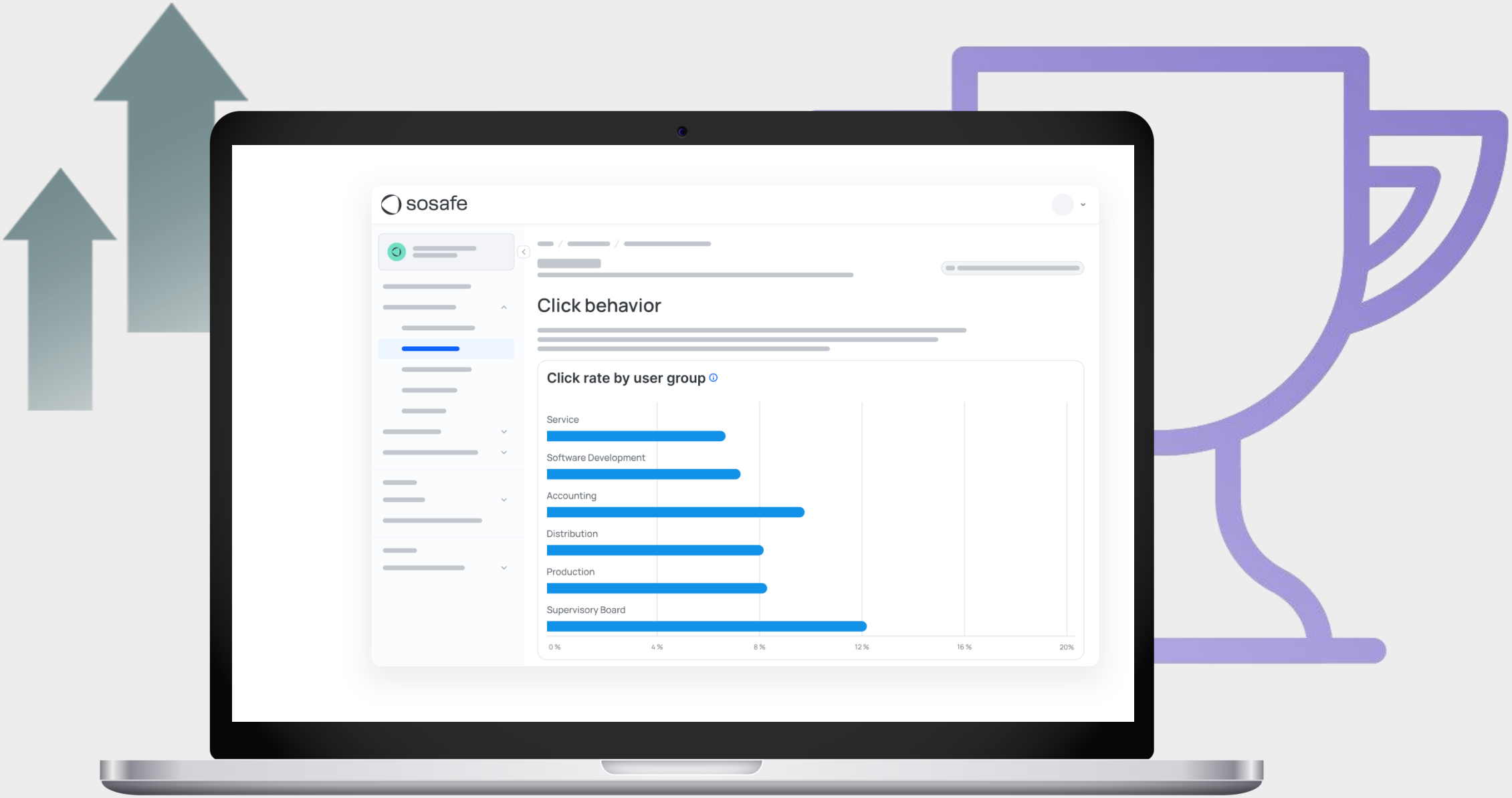
# Stärken Sie Ihre Cybersecurity durch mühelose Sicherheitskommunikation




- **Mühelose Kommunikation:** Ermöglicht schnelles Handeln und direktes Feedback
- **Kontextbezogene Insights:** Vermitteln Sie praktisches und theoretisches Wissen in realen Situationen
- **Adaptives Lernen:** Durch kontinuierliche Awareness-Maßnahmen bleibt die Cybersicherheit jederzeit präsent
- **Benutzerfreundliche Umgebung:** Greifen Sie mühelos auf wichtige Richtlinien und Prozesse zu

HIN ZU EINER STARKEN SICHERHEITSKULTUR

# … und erschaffen Sie mit unserer Hilfe mehr Security-Champions



ALLES WAS SIE BRAUCHEN

# um Ihr **menschliches Risiko** schnell zu **reduzieren**

## Für Mitarbeitende



**Resilienz steigern**
Erzielen Sie Verhaltensänderung 2x schneller als traditionelle Awareness-Programme



**Kultur stärken**
Steigern Sie das User-Engagement um >50 % durch immersive Storytelling- und Gaming-Elemente



**Risiko reduzieren**
Senken Sie Klick- und Interaktionsraten schon im ersten Jahr um 80 %

## Für Organisationen



**Garantierte Compliance**
100 %-ige Compliance mit globalen Sicherheits- und Datenschutzrichtlinien



**Ressourcen sparen**
Implementierung in 20 Tagen, mit 20 Minuten pro Monat zu einer starken Sicherheitskultur



**Aufmerksamkeit erhöhen**
>70 % der User zeigen aktives Meldeverhalten innerhalb der ersten sechs Monate



Klingt spannend?

Wir freuen uns, von Ihnen zu hören.

**Amin Motalebi**
Awareness Specialist
SoSafe

amin.motalebi@sosafe.de

**LinkedIn**




powered by sosafe

# Human Firewall Conference 2024

Die führende Security-Konferenz
mit Fokus auf dem Faktor Mensch

14.-15. November 2024

Melden Sie sich
zur HuFiCon24 an

8COM ACADEMY

# Kulturwandel & Auswirkung der Demografie auf die Informationssicherheit

→ Effektive Awareness-Maßnahmen

# 8com KENNZAHLEN

Stand März 2024



**98**
Mitarbeiter

**102**
Kunden im Security Operations Center

seit **2004**
Cyber Security

**30.000.000.000**
Security Events am Tag

**> 600**
IT-Forensik, Incident Response, Penetration Testing und Awareness-Kunden

**24/7/365**
für Sie da!

3-Schicht-Modell, ausschließlich aus Deutschland, RC4-Hochsicherheitsbereich, kein Home-Office für SOC-Mitarbeiter

**40 Länder**

8COM CYBER SECURITY

# Herausforderungen Demografische Veränderungen

- Alternde Belegschaft
  - Wissenstransfer
  - Anpassung an neue Technologien



# Herausforderungen Demografische Veränderungen

- Alternde Belegschaft
- Zunahme der digitalen Generation
  - Technologieaffinität
  - Bring Your Own Device



# Herausforderungen Demografische Veränderungen

- Alternde Belegschaft
- Zunahme der digitalen Generation
- Globale Belegschaft und kulturelle Unterschiede
  - Unterschiedliche Sicherheitskulturen
  - Remote-Arbeit



# Herausforderungen Demografische Veränderungen

- Alternde Belegschaft
- Zunahme der digitalen Generation
- Globale Belegschaft und kulturelle Unterschiede
- Zunehmende Mobilität der Arbeitskräfte
  - Häufige Jobwechsel
  - Verstärkte Nutzung von Cloud-Diensten



# Einfluss des Kulturwandels auf die IS

- Erhöhtes Risiko durch Remote-Arbeit
- Anpassung der Schulungsmaßnahmen
- Stärkung der Sicherheitskultur
- Agilität und Sicherheit

# Strategien zur Bewältigung der Herausforderungen

- Analyse und Verständnis der bestehenden Kultur
- Schulung und Sensibilisierung
- Kommunikation und Bewusstseinsbildung
- Führung und Vorbildfunktion
- Policies und Richtlinien
- Feedback und kontinuierliche Verbesserung
- Messung und Erfolgskontrolle
- Technologische Schutzmaßnahmen

# Fazit

- Viele Herausforderungen
- Viele Maßnahmen, um diese zu bewältigen
- Analyse und Verständnis des tatsächlichen Bedarfs sind essentiell
- Mitarbeiterbefragungen – sammeln Sie Feedback
- Regelmäßige Audits

# Danke für Ihre Aufmerksamkeit!

**8com Academy**

das E-Learning-Portal der 8COM GmbH & Co. KG


Frederik Kaiser
Head of 8com Academy

frederik.kaiser@8com.de

+49 6321 48446 2031