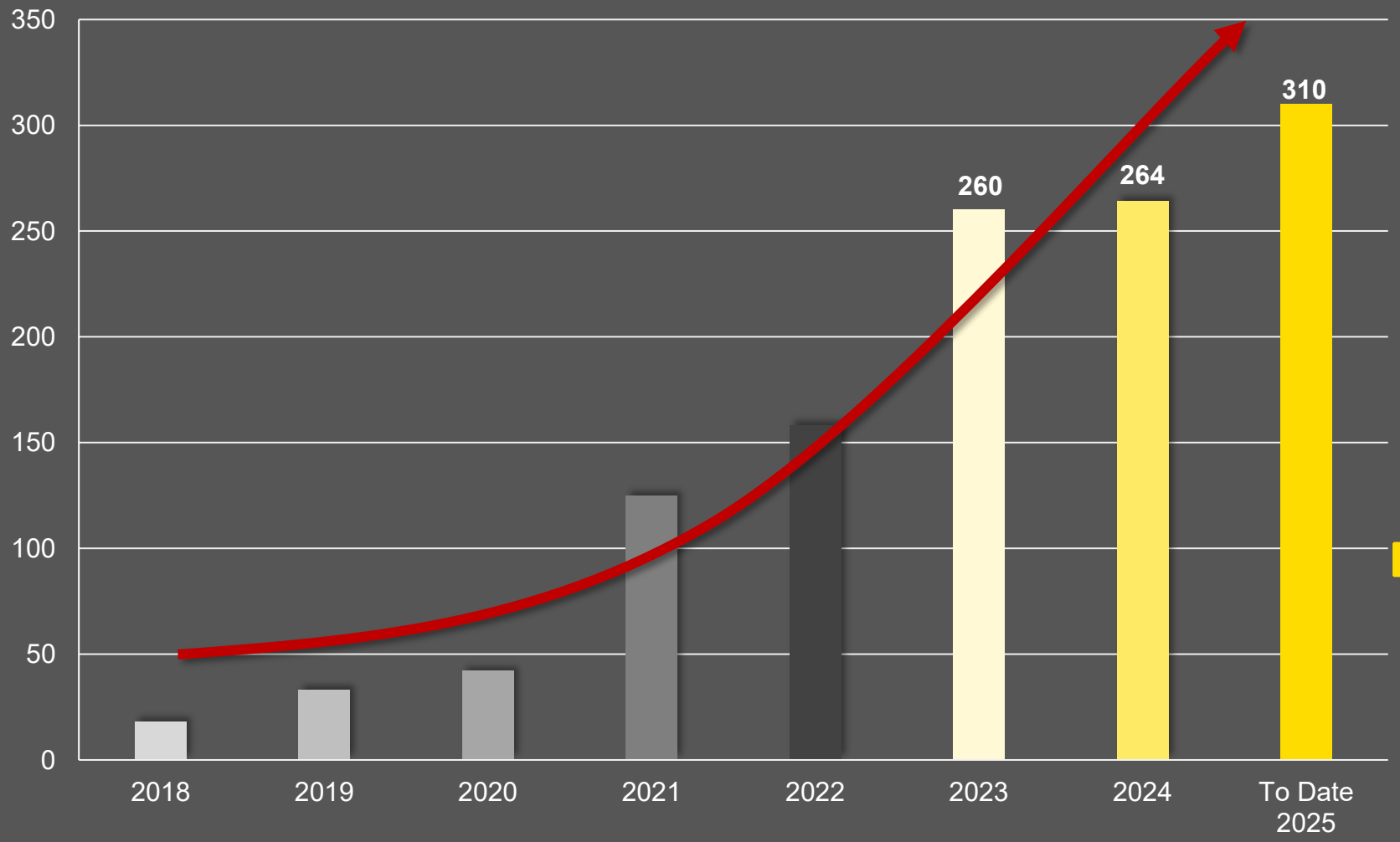
InfoGuard
SWISS CYBER SECURITY

Cyber Crime Insights aus der DACH-Region: Wenn Cyberangriffe Realität werden

Ernesto Hartmann, Chief Cyber Defence Officer, InfoGuard AG

InfoGuard Computer Security Incident Response Team
CSIRT Vorfälle 2018 – 2025 H1

InfoGuard
SWISS CYBER SECURITY

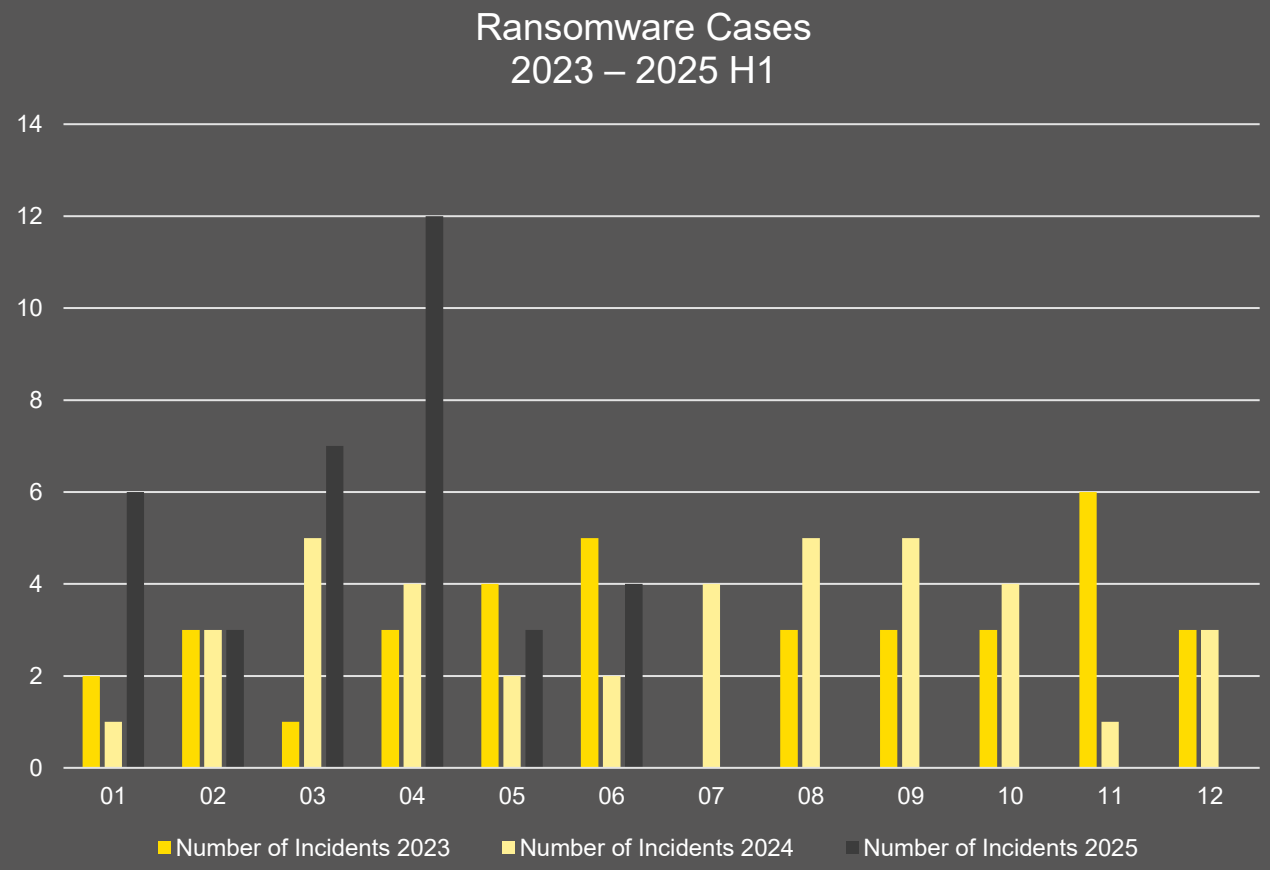


Hohe Fallzahlen ermöglichen tagesaktuelle Informationen über die Bedrohungslage.

Wir beobachten einen deutlichen Anstieg von Ransomware-Fällen.

Source InfoGuard Intelligence

Ransomware Trends H1 2025

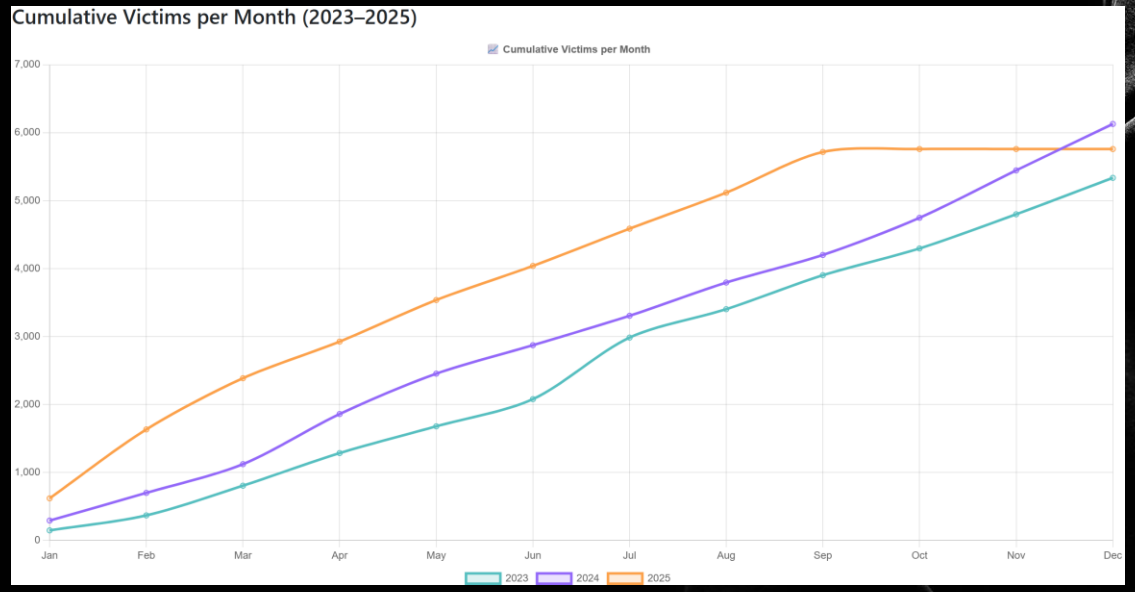


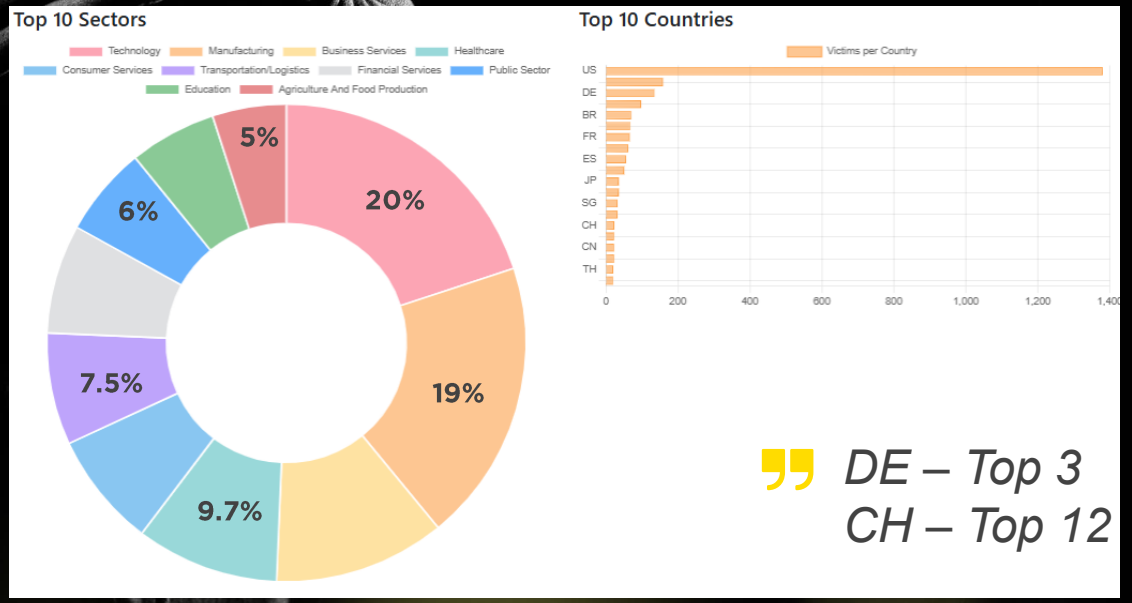
2025 Der Trend geht weiter!

In der ersten Jahreshälfte wurden **36** Ransomware Incidents durch das InfoGuard CSIRT bearbeitet.

Source InfoGuard Intelligence

Ransomware Global Trends 2025





DE – Top 3
CH – Top 12

Source https://www.ransomware.live/statistics

Cyber Crime –
Die Entwicklung von Ransomware-Angriffen

InfoGuard
SWISS CYBER SECURITY

2018+

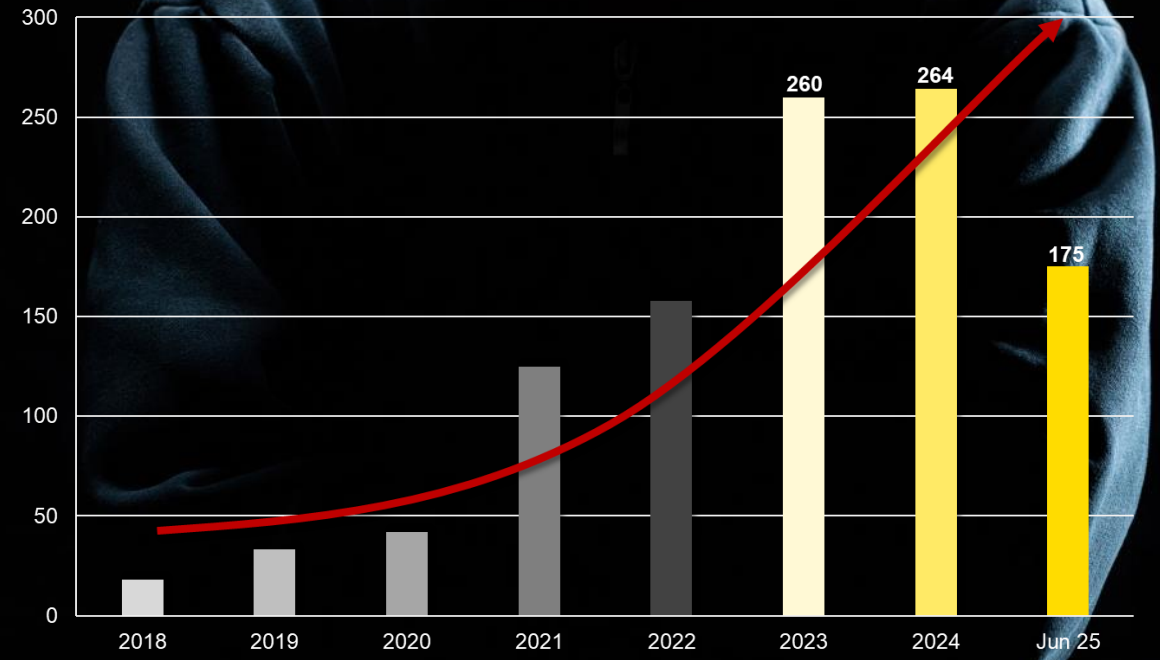
Single Extortion
Verschlüsselung von Systemen und Daten

2020+

Double Extortion
Verschlüsselung von Systemen und Daten, sowie Datenexfiltration

2025

Rückkehr zur Single Extortion
Exfiltration von Daten unter Einsatz ausgeklügelter Tarnmethoden im Zentrum



THE RISE OF VIBE HACKING!

InfoGuard
SWISS CYBER SECURITY

> Der Anthropic Threat Intelligence Bericht zeigt, wie ein Individuum parallel mit „Natural Language Prompts“ Daten von 17 Unternehmen exfiltiert hat!

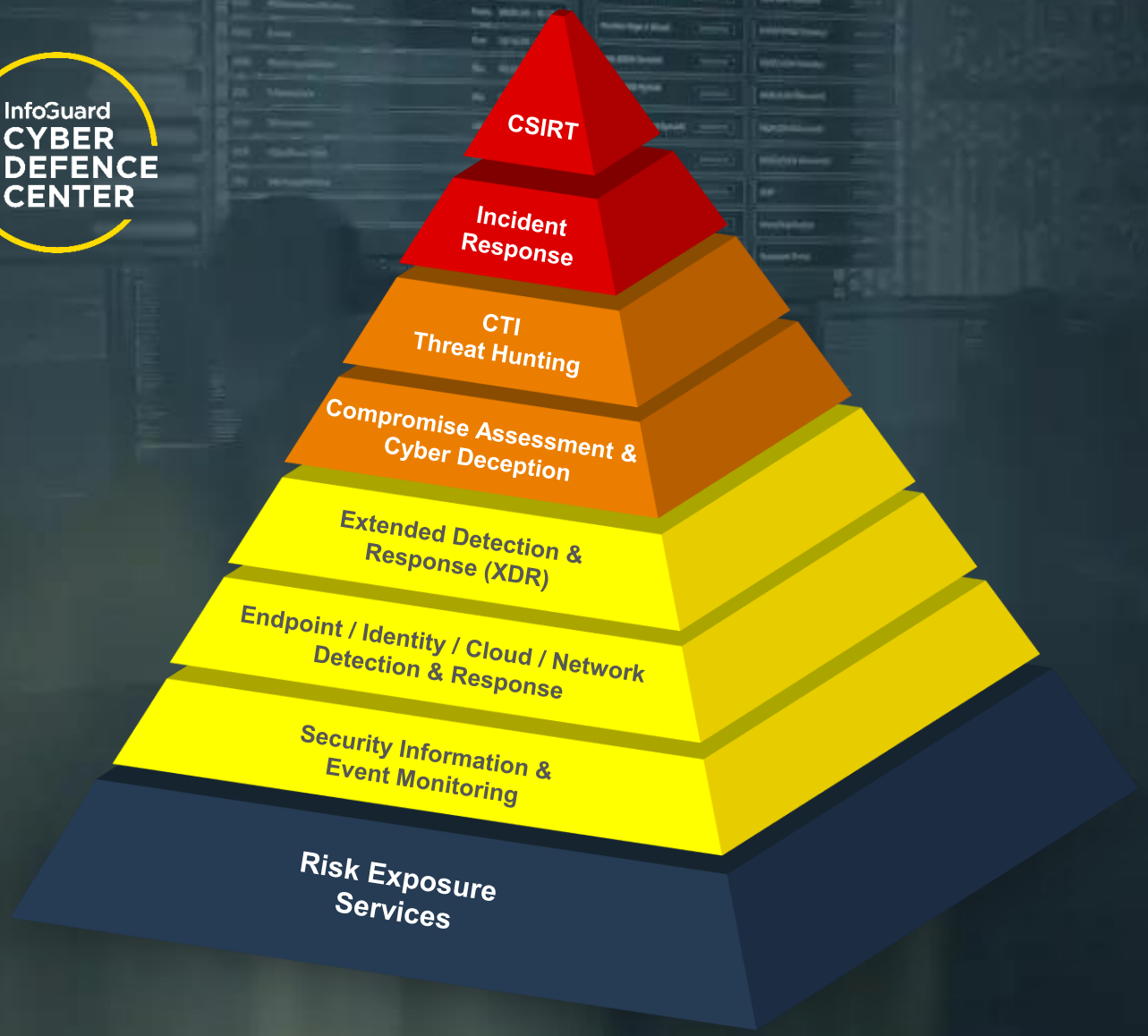
AI- Automated stages

- Reconnaissance: Generate OSINT queries for subdomains, exposed services, and weak portals.
- Infiltration: Produce PowerShell or Python loaders tuned to the environment.
- Exfiltration: Stage archives and ship via HTTPS to attacker-controlled endpoints.
- Extortion: Draft notes with financial language calibrated to each sector.

24/7 Cyber Defence & Incident Response Services – Umfassender Schutz vor Cyberangriffen

InfoGuard SWISS CYBER SECURITY

InfoGuard CYBER DEFENCE CENTER



CSIRT

INCIDENT RESPONSE & RECOVERY

- Incident Response / CSIRT
- Forensics
- Crisis & Incident Response Readiness

MDR

HUNTING & INTELLIGENCE

- Cyber Threat Intelligence (CTI)
- Threat Hunting
- Compromise Assessment
- Cyber Deception

MANAGED DETECTION & RESPONSE

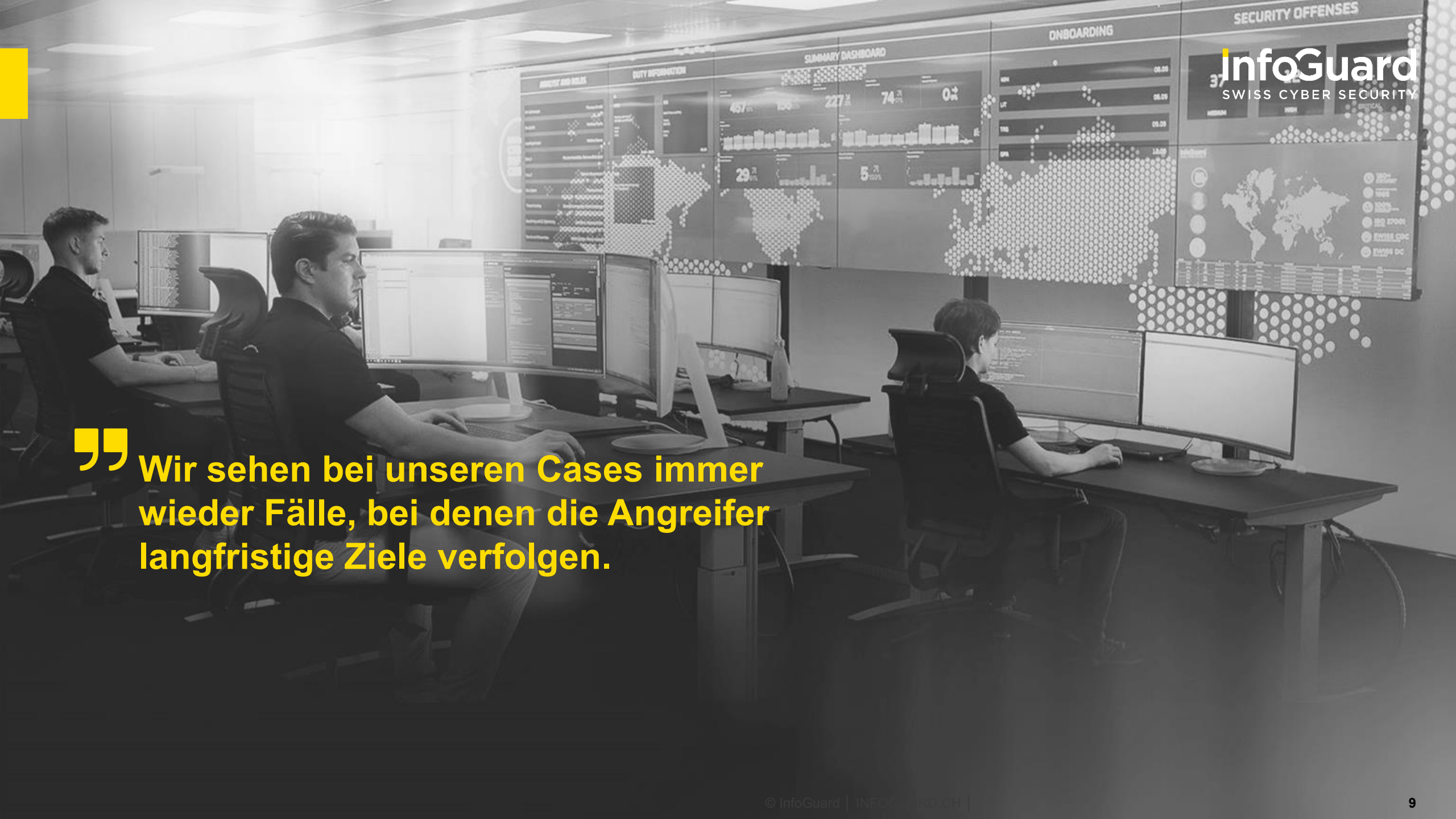
- Extended Detection & Response (XDR)
- Endpoint & Identity Detection & Response (EDR & IDR)
- Cloud & Network Detection & Response (CDR & NDR)
- Security Information & Event Monitoring (SIEM)

MSS

SECURITY & RISK OPERATIONS

- Managed XDR & SIEM
- Risk Exposure Services

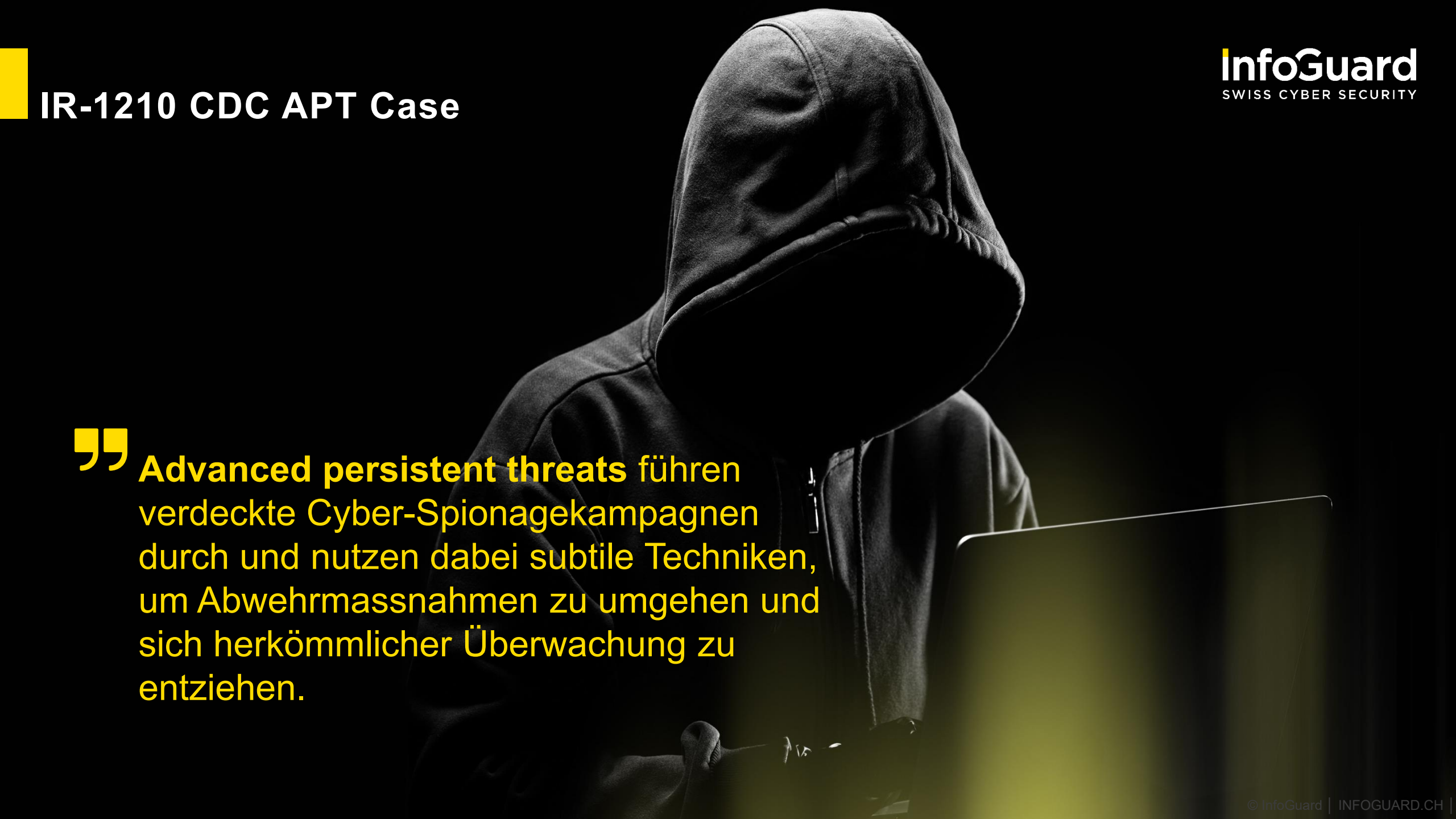
Professionelle Unterstützung bei einem Sicherheitsvorfall



> **Wir sehen bei unseren Cases immer wieder Fälle, bei denen die Angreifer langfristige Ziele verfolgen.**

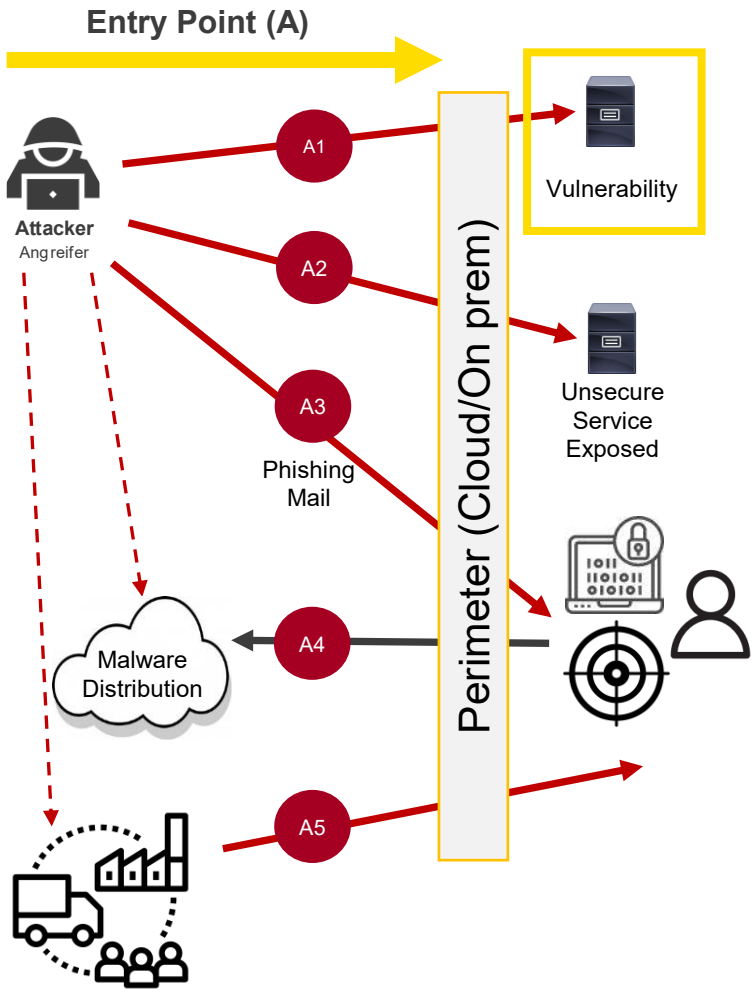
IR-1210 CDC APT Case

InfoGuard
SWISS CYBER SECURITY



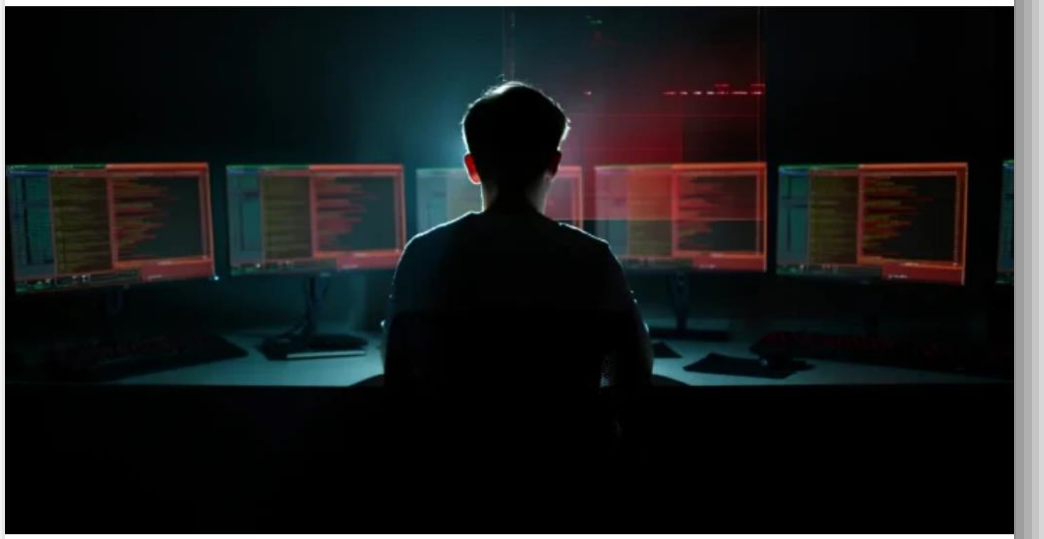
> **Advanced persistent threats** führen verdeckte Cyber-Spionagekampagnen durch und nutzen dabei subtile Techniken, um Abwehrmassnahmen zu umgehen und sich herkömmlicher Überwachung zu entziehen.

IR-1210 CDC APT Case
Eine offene Türe ermöglichte dem APT den Einstieg.



Chinese Hackers Exploit Ivanti EPMM Bugs in Global Enterprise Network Attacks

May 22, 2025 Ravie Lakshmanan



A recently patched pair of security flaws affecting Ivanti Endpoint Manager Mobile (EPMM) software has been exploited by a China-nexus threat actor to target a wide range of sectors across Europe, North America, and the Asia-Pacific region.

The vulnerabilities, tracked as CVE-2025-4427 (CVSS score: 5.3) and CVE-2025-4428 (CVSS score: 7.2), could be chained to execute arbitrary code on a vulnerable device without requiring any authentication. They were addressed by Ivanti last week.

Day 1
Initial Compromise

InfoGuard
SWISS CYBER SECURITY

CVE-2025-4427 PUBLISHED

Required CVE Record Information

CNA: Ivanti –

Published: 2025-05-13 **Updated:** 2025-05-13
Title: Authentication Bypass

Description

An authentication bypass in the API component of Ivanti Endpoint Manager Mobile 12.5.0.0 and prior allows attackers to access protected resources without proper credentials via the API.

Score	Severity	Version	Vector String
5.3	MEDIUM	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2025-4428 PUBLISHED

Required CVE Record Information

CNA: Ivanti –

Published: 2025-05-13 **Updated:** 2025-05-13
Title: Remote Code Execution

Description

Remote Code Execution in API component in Ivanti Endpoint Manager Mobile 12.5.0.0 and prior on unspecified platforms allows authenticated attackers to execute arbitrary code via crafted API requests.

Score	Severity	Version	Vector String
7.2	HIGH	3.1	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

> Schwachstellen wie Remote Code Execution oder Authentication Bypass sind oft die Hauptziele von Bedrohungsakteuren!

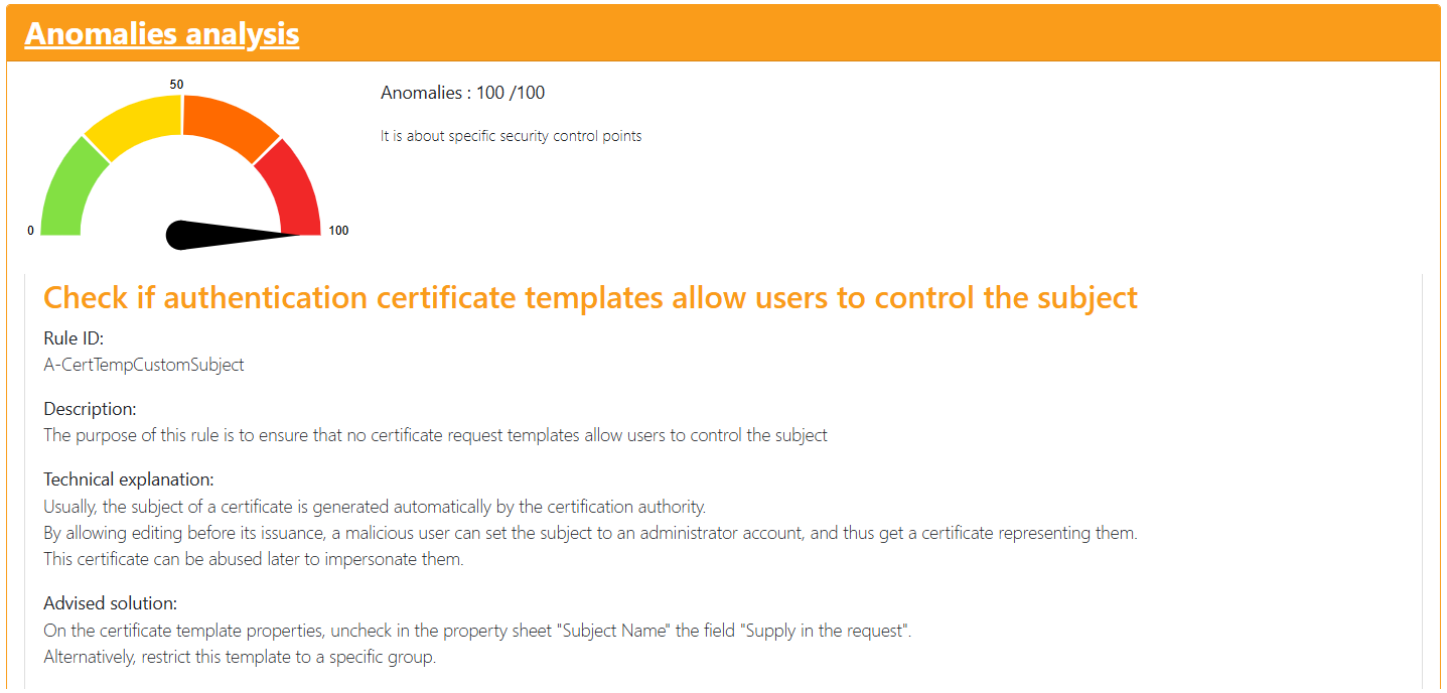
Opportunitäten werden sofort global ausgenutzt!

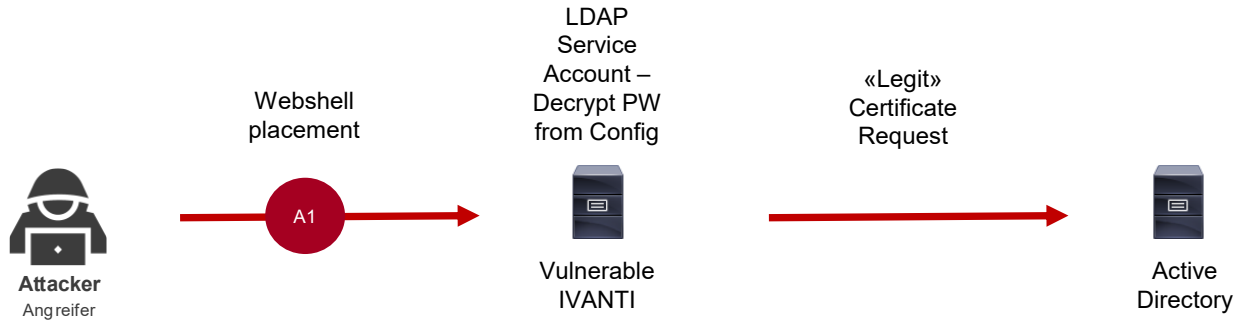
InfoGuard
SWISS CYBER SECURITY

Wer nach dem Patchen kritischer Sicherheitslücken nicht sofort eine umfassende Analyse durchführt, öffnet Cyber-Angreifern Tür und Tor, Cybercrime-Gruppierungen stürzen sich gnadenlos auf jede verwundbare Stelle!

Day 1
Privilege Escalation & Persistence

InfoGuard
SWISS CYBER SECURITY

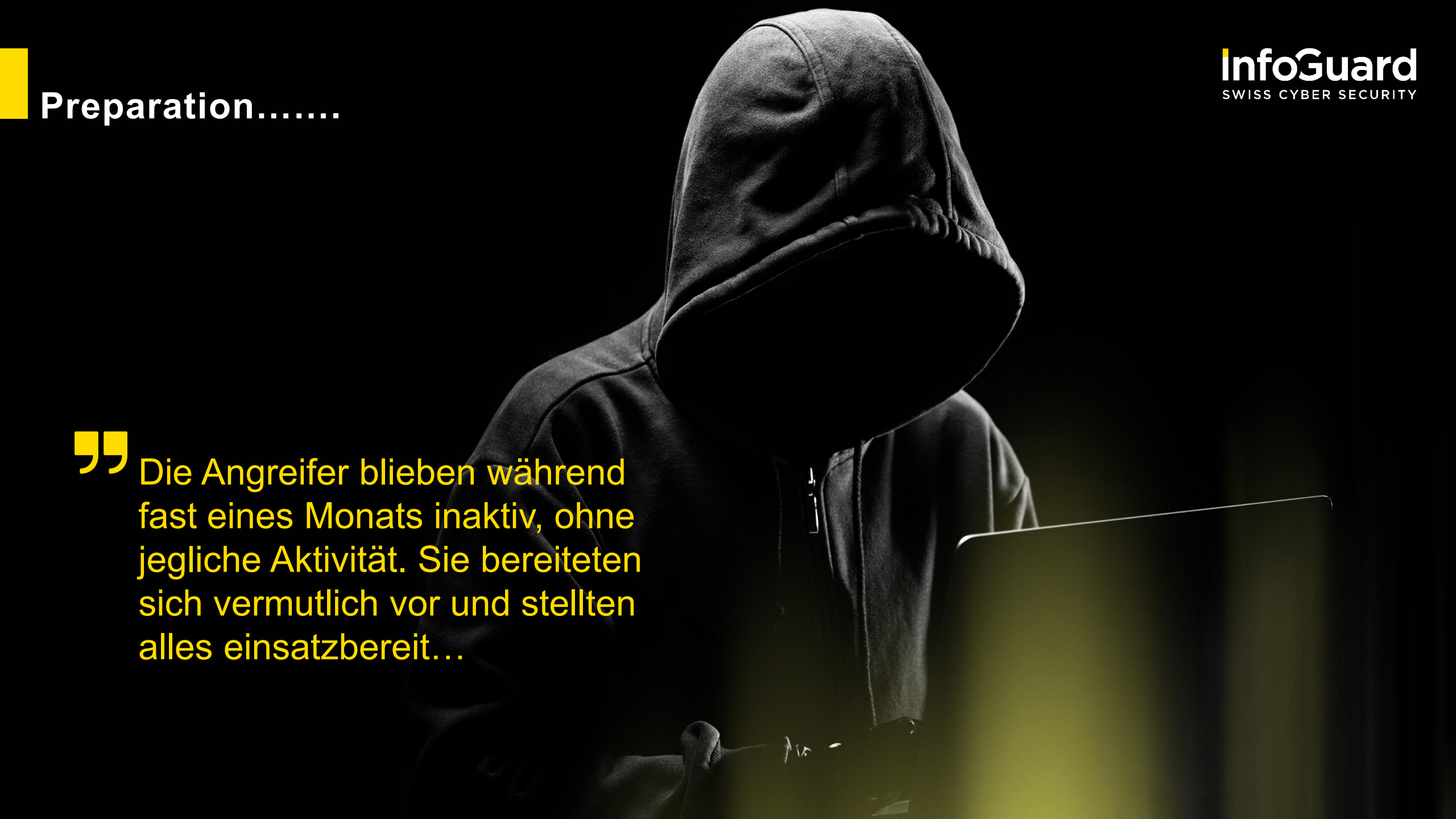




> Exploitation und Privilegienerweiterung durch Schwachstellen und unsichere Active-Directory-Konfigurationen sind sehr schwer zu erkennen.

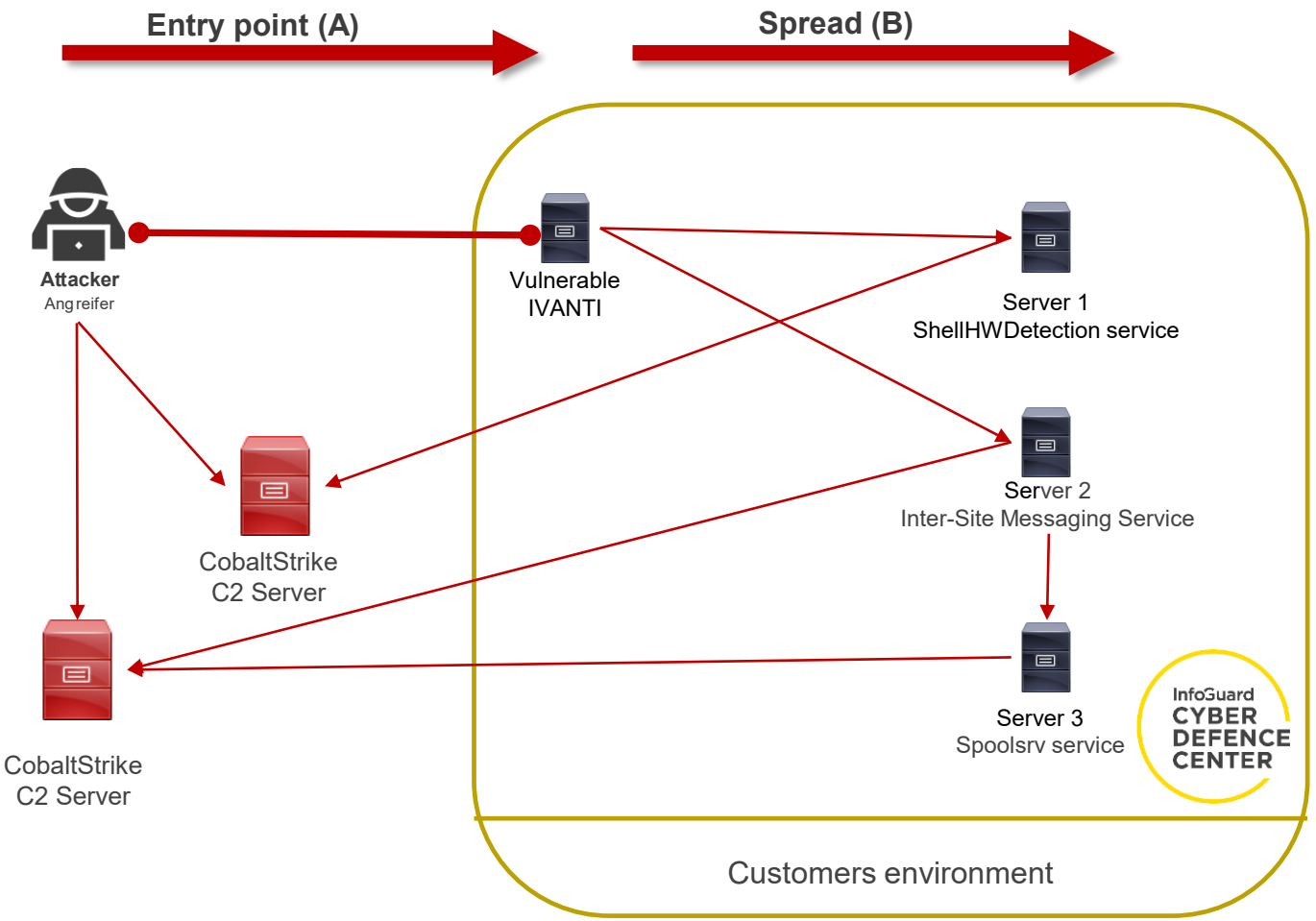
Preparation…….

InfoGuard
SWISS CYBER SECURITY



> Die Angreifer blieben während fast eines Monats inaktiv, ohne jegliche Aktivität. Sie bereiteten sich vermutlich vor und stellten alles einsatzbereit…

1 Month later
Lateral Movement

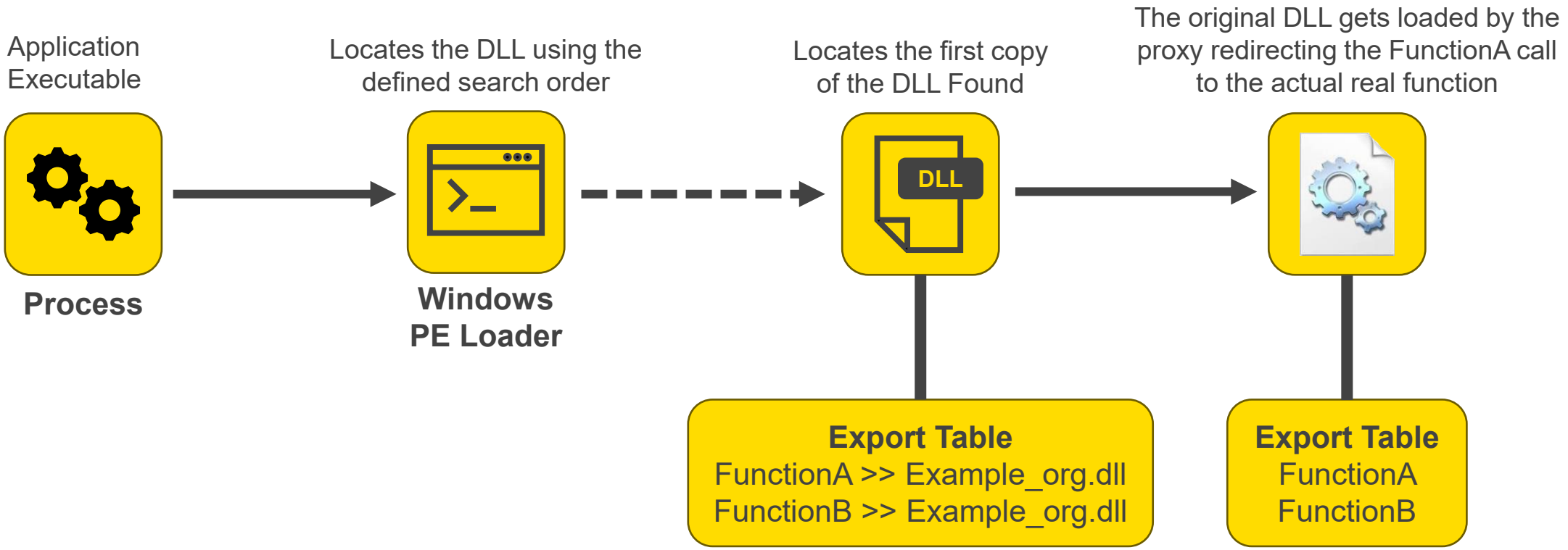


Timeline

1. Day 1 – Infection & Persistence @ Ivanti
2. Day 30 00:04 – Backdoor 1 on Server 1
3. Day 30 05:45 – Backdoor 2 on Server 2
4. Day 35 08:36 – Attempt to compromise Server 3
   - blocked by Cortex
5. **CDC ALERT & ESCALATION**
6. Day 35 08:48 – Succesfull Backdoor 3 on Server 3

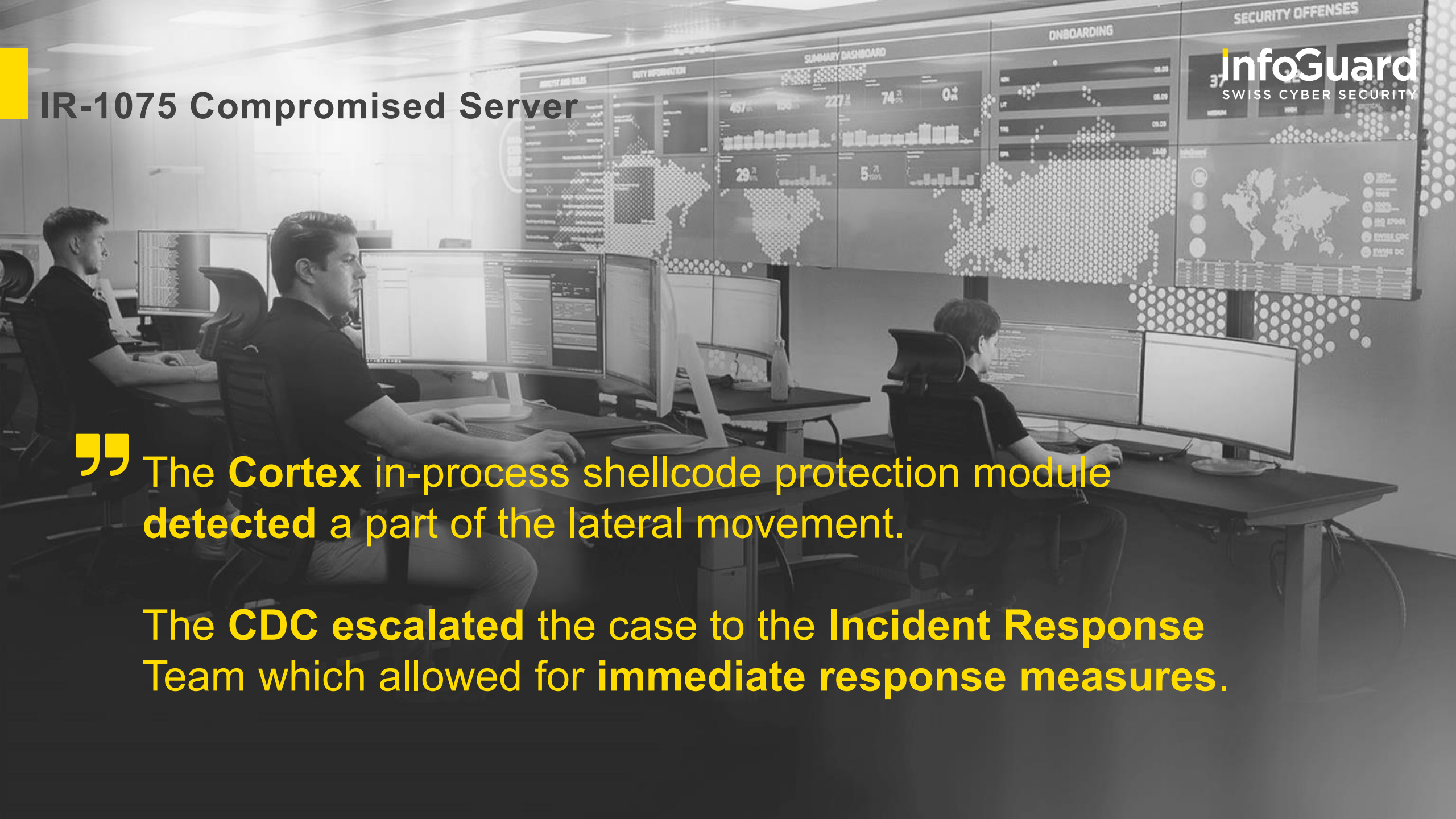
> Der Angreifer nutzte drei verschiedene legitime Dienste, um Backdoor-DLLs zu installieren.

Persistenz durch DLL Hijacking



https://www.geeksforgeeks.org/ethical-hacking/what-is-dll-hijacking/

IR-1075 Compromised Server



InfoGuard
SWISS CYBER SECURITY

> The **Cortex** in-process shellcode protection module **detected** a part of the lateral movement.

The **CDC escalated** the case to the **Incident Response** Team which allowed for **immediate response measures**.

Professionelle Unterstützung bei einem Sicherheitsvorfall

InfoGuard
SWISS CYBER SECURITY

- Isolating the devices
- Deleting DLL from devices
- Rebuilding Ivanti appliance
- Reverse engineering the DLL
- Restaging the devices
- Removing the abused certificates and revoking the certificate template
- KRBTGT password change
- Reseting all users and service account passwords

Angriff

Übernahme / Coaching Krisenstab

Forensische Untersuchung

Eindämmung der Situation

Unterstützung bei Bezahlung

Learnings & Verbesserung

Schutz vor einem Geschäftsausfall | **Gesicherter Wiederanlauf / Aufbau**


InfoGuard
SWISS CYBER SECURITY
Lessons Learned

Prevention, effektive Response und eine effiziente Recovery gehören zu einem MDR/SOC-Dispositiv!

InfoGuard
SWISS CYBER SECURITY

NIST Cybersecurity Framework 2.0

GOVERN

Evolution der Verteidigung 1# Phase

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Risk Assessment • Improvement	• Identity Management, Authentication & Access Control • Awareness and Training • Data Security • Platform Security	• Continuous Monitoring • Adverse Event Analysis	• Incident Management • Incident Analysis • Incident Response Reporting & Communication • Incident Mitigation	• Incident Recovery Plan Execution • Incident Recovery Communications

Evolution der Verteidigung 2# Phase

Cyber Defence Maturity

Fokus gestern

Fokus heute

INFOGUARD MDR **CSIRT**

> Der nächste Angriff kommt bestimmt, wir schützen Sie!

2xSOC
24/7 Security Operations Center in der Schweiz und Deutschland

90+
Experten im SOC & CSIRT

400+
CDC- & CSIRT-Kunden

13+
Jahre Erfahrung & SOC-Kompetenz

ISO 27001
ISO 14001
ISAE 3000 Typ2

CSIRT
Computer Security Incident Response Team
BSI-qualifizierter APT-Response-Dienstleister und FIRST-Mitglied

WHEN IT MATTERS, WE ARE THERE FOR YOU!

InfoGuard CYBER DEFENCE CENTER

7x24 Hotline: +41 41 749 19 99
E-Mail: soc@infoguard.ch

Please note, that in urgent cases and out of office hours the hotline has to be called.