Anatomie des Cyberangriffs: Häufigste Beobachtungen und typische Vorgehensmuster

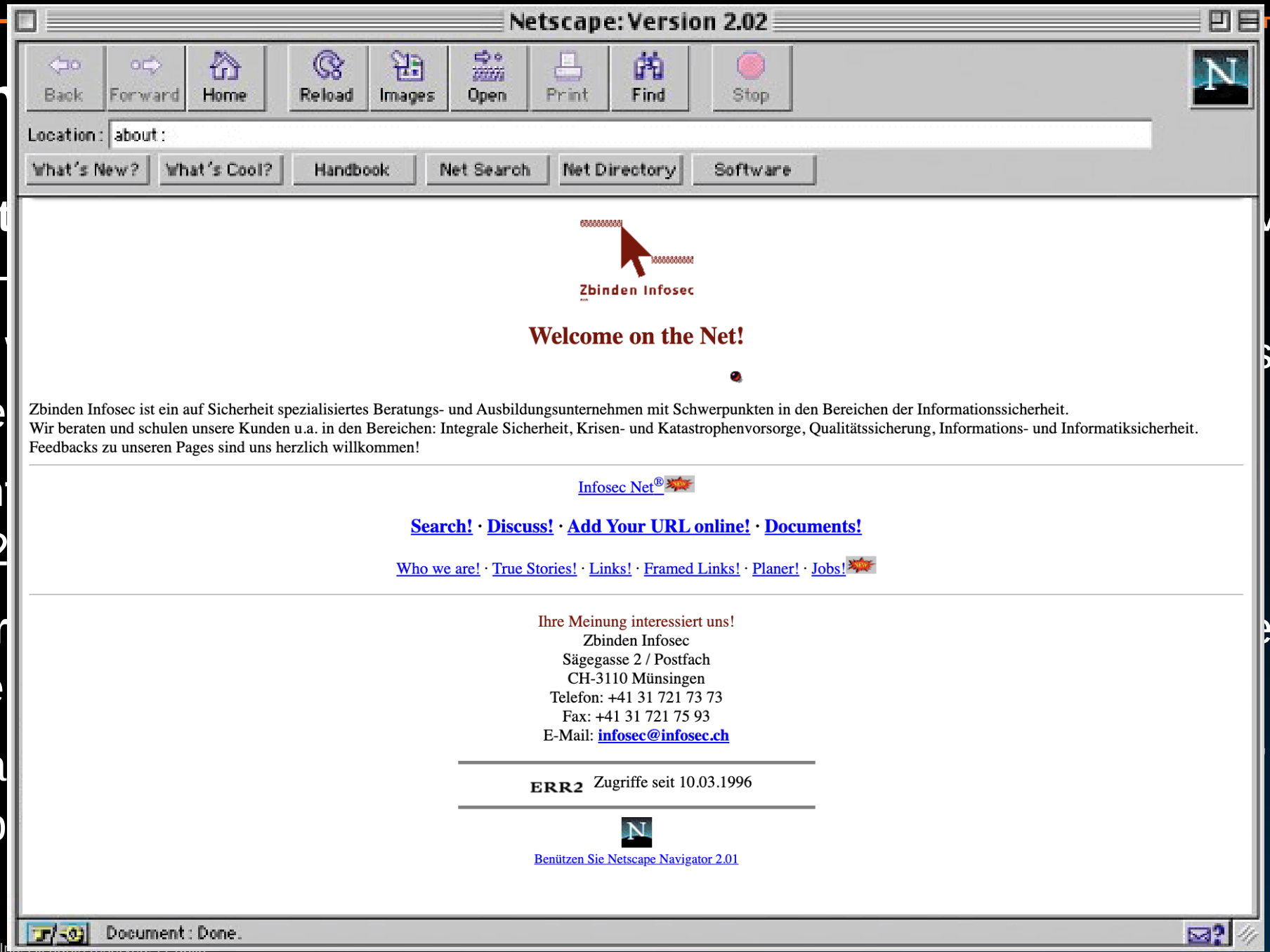
Felix Guggenheim, Sr. Solutions Engineer, CISSP

46. MEET SWISS INFOSEC! Swiss Infosec on Fire

THE LEADER IN SECURITY OPERATIONS

1989 in

- Der **Dat** …Viren viel Presse-
- **WANK** …sich via DECNe
- **Aids In** … via Post (!) auf 2
- **IBM Vir** …ersten Antivire
- In Holla… (letzte Ausgab




HAPPPY 3ᵈ ANNNIVERSARY 3NT
SWISS INFOSEC
35
ARCTIC WOLF | CELEBRTED
WITH EATTING THE PPPLLLERS.

Kurzvorstellung Arctic Wolf

SOC-Partner für über 7000 Kunden in der Schweiz, Europa, Nordamerika und Australien:

- 24/7 Monitoring von Netzwerk, Endpunkten, Identitäts- und Cloudsystemen (“MDR”)
- Erarbeiten und Durchführen von Security-Strategien zur Härtung von Kundenumgebungen durch persönliche Betreuung (“Concierge Team”)
- Weitere SOC-Leistungen wie Threat Research, Schwachstellen-Management, User-Awareness-Trainings, Toolings für Assessments, Versicherbarkeitsabschätzung, Incident Response Planung, etc

Incident Response Team mit über 100 Spezialisten zur Unterstützung im Notfall:

- 24/7 Rufbereitschaft für Notfälle, auch mit 1h SLA
- Verhandlungsführerschaft, Digitale Forensik, Systemwiederherstellungen mit viel Erfahrung (1000+ Fälle / Jahr)

01 Review: Häufigste Angriffsarten

02 Review: Ursachen und Methoden

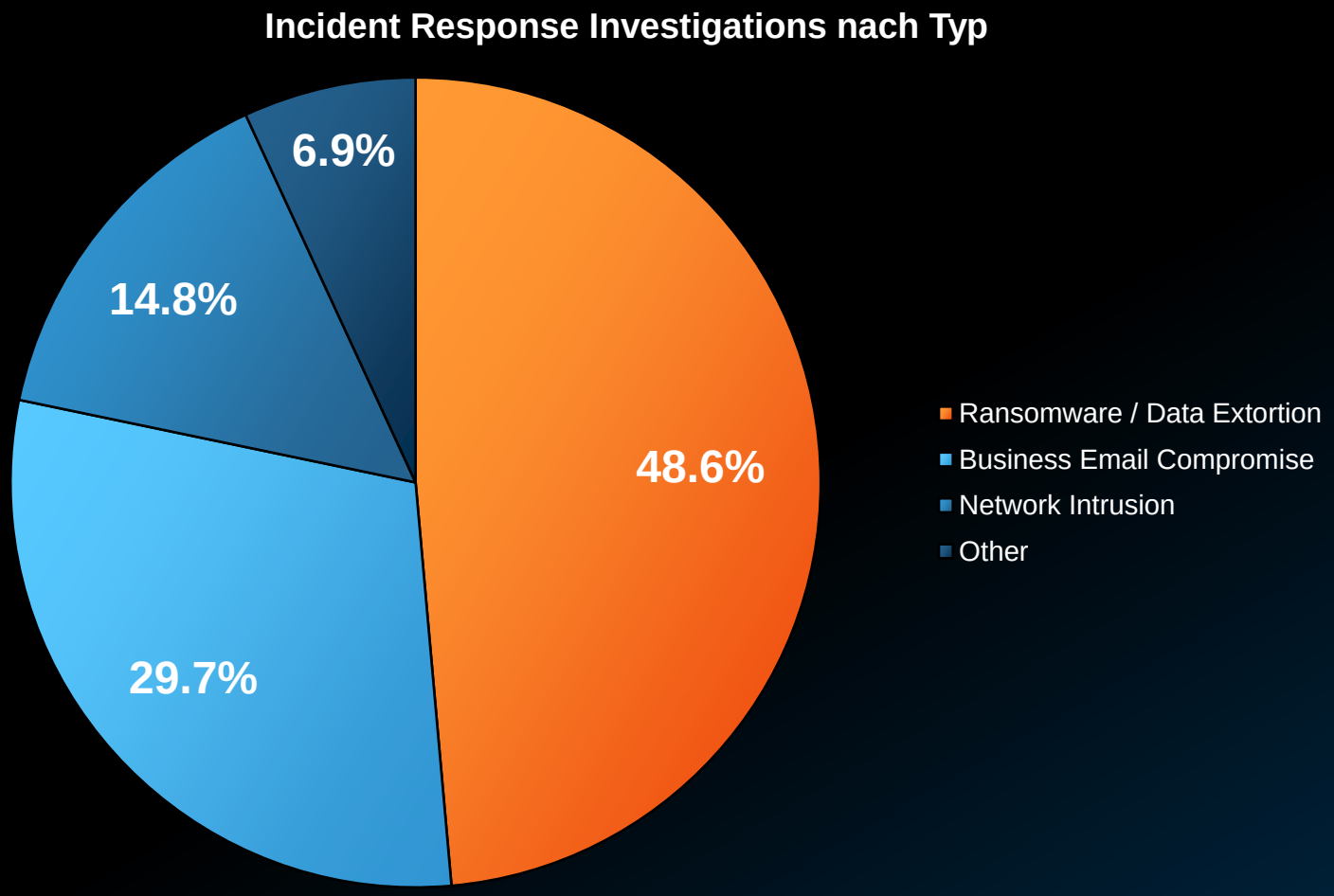
03 Case: Fluggesellschaft (Negativbeispiel)

04 Empfehlungen

Threat Report 2024: Angriffsarten

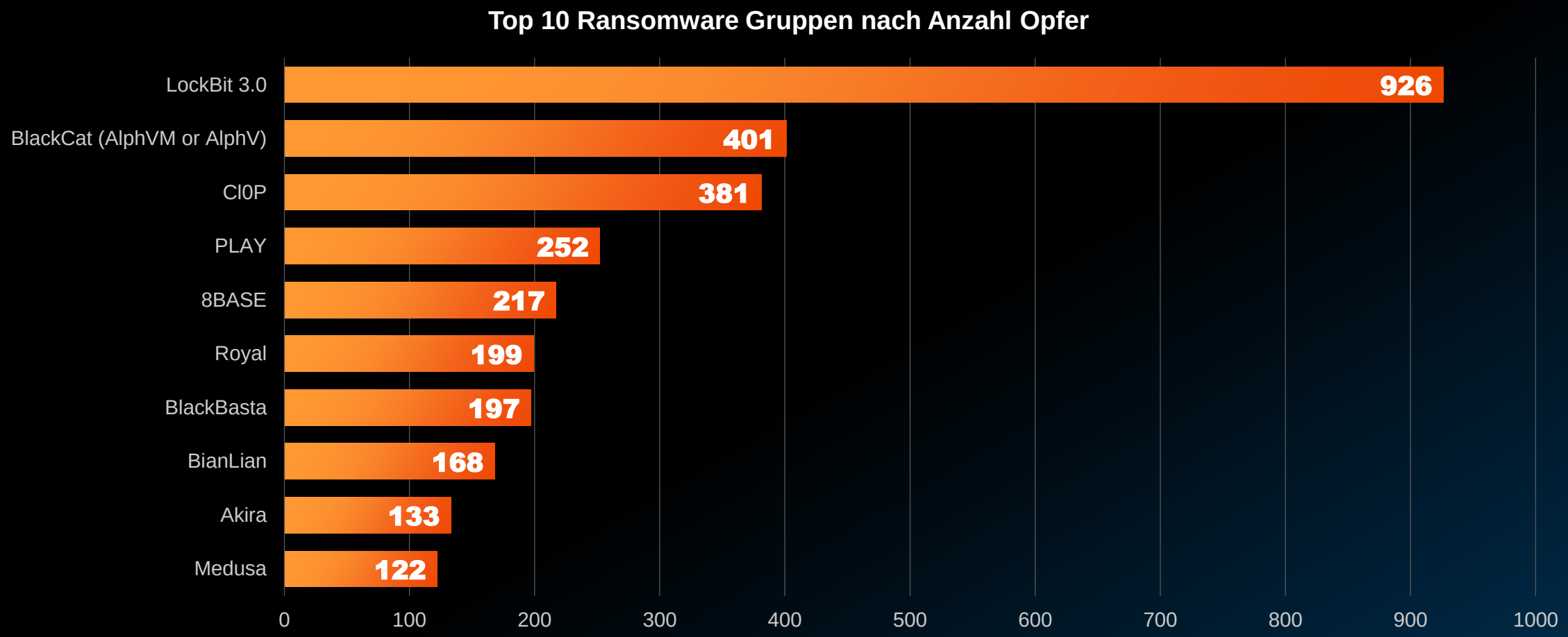
Incident Response Investigations

Was haben wir bearbeitet?



Ransomware Groups

Wiederholungstätger, Newcomers, Leavers...



Lösungsgeldforderungen nach Branche

20 Prozent Steigerung (Median) gegenüber Vorjahr

	2022	2023
Healthcare	$275,000	$450,000
Construction	$375,000	$500,000
All Industries	$500,000	$600,000
Finance & Insurance	$500,000	$900,000
Legal & Government	$420,000	$1,000,000
Retail	$627,500	$1,500,000

Business Email Compromise

Business Email Compromise ursächlich für über einen Viertel (29.7%) aller Incident Response Fälle im letzten Jahr.

Warum ist Business Email Compromise (BEC) attraktiv für Threat Actors?

- BEC ist einfach auszuführen
- BEC funktioniert

Meist-betroffene Branchen

01 **Finance & Insurance**

02 **Construction**

03 **Education & Non-Profit**

04 **Manufacturing**

05 **Legal & Government Healthcare**

(Gleichermassen)

Threat Report 2024: Ursachen und Methoden

Root Cause

(Fälle ohne BEC)

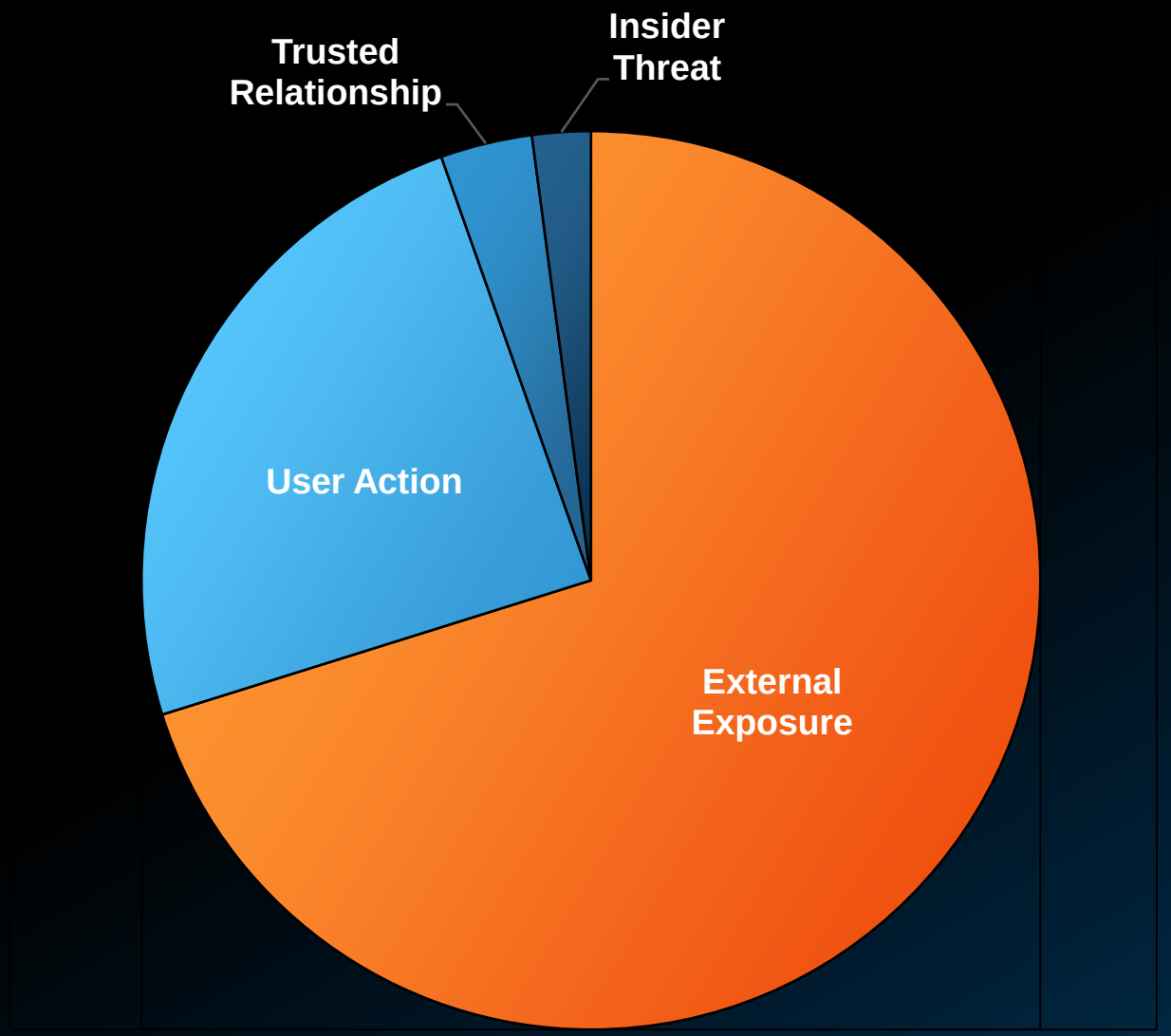
Die Ursache der Incidents fiel jeweils in eine dieser vier Kategorien:

70.1% External Exposure

24.4% User Action

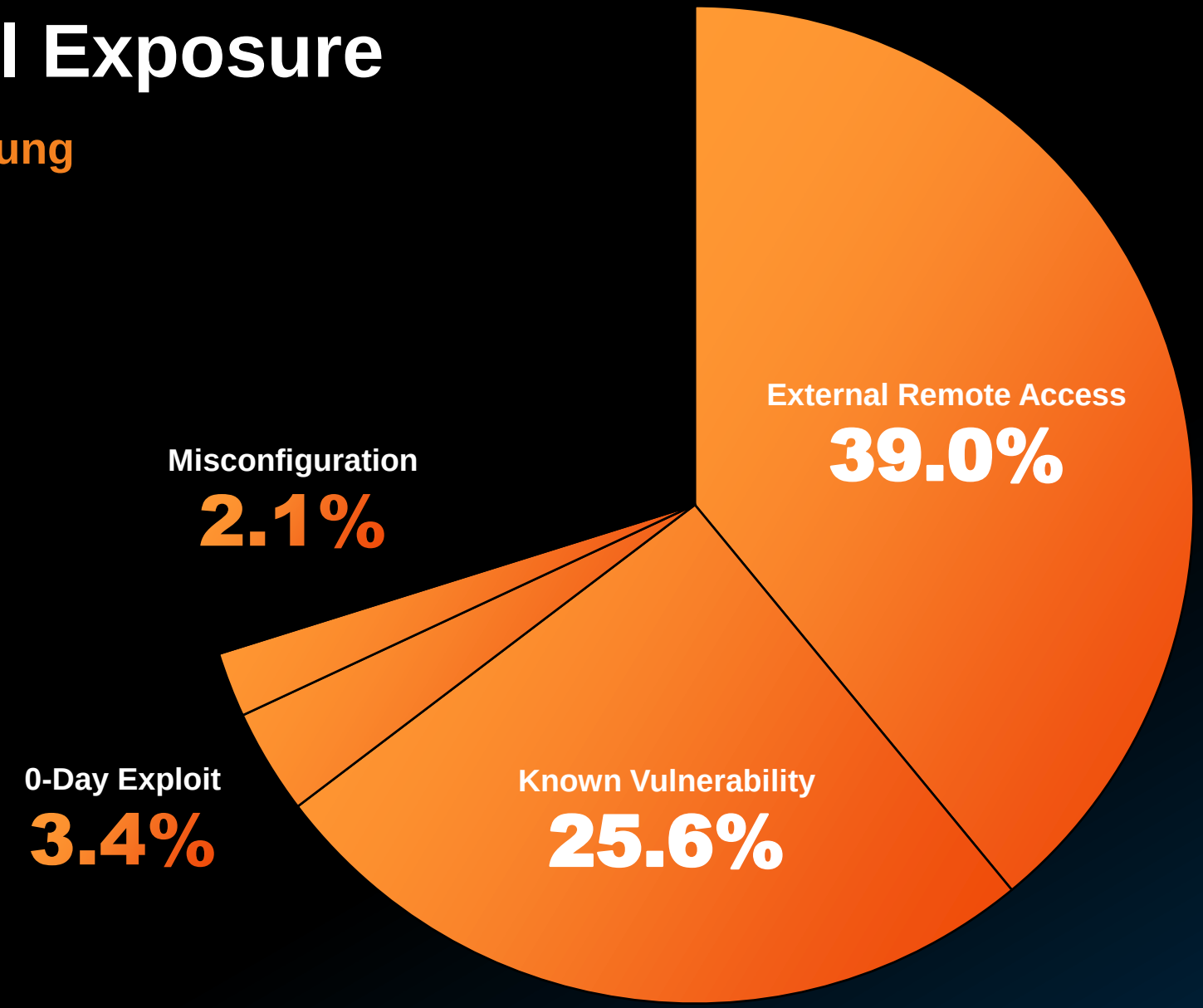
3.3% Trusted Relationship

2.1% Insider Threat



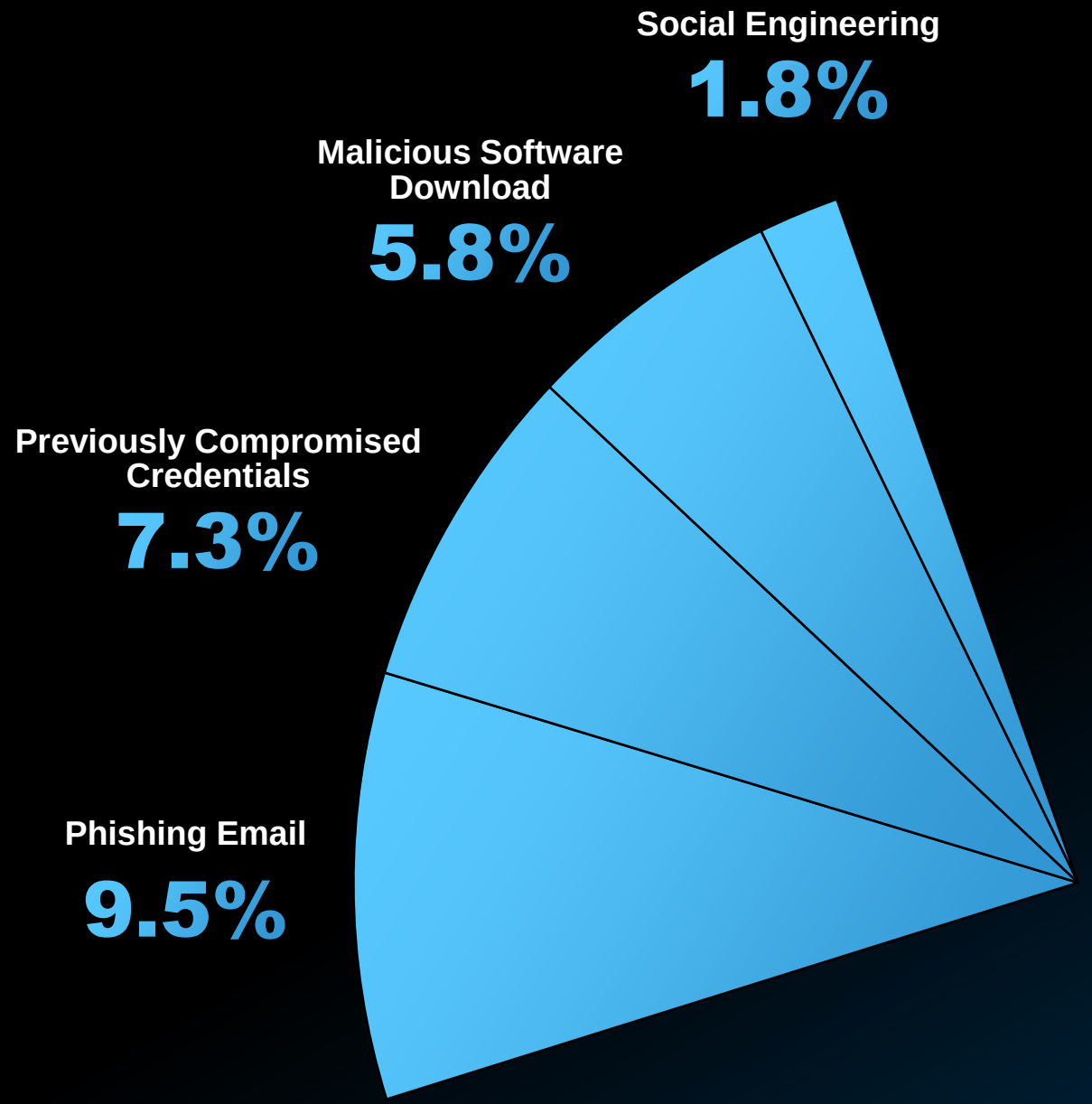
External Exposure

Aufschlüsselung

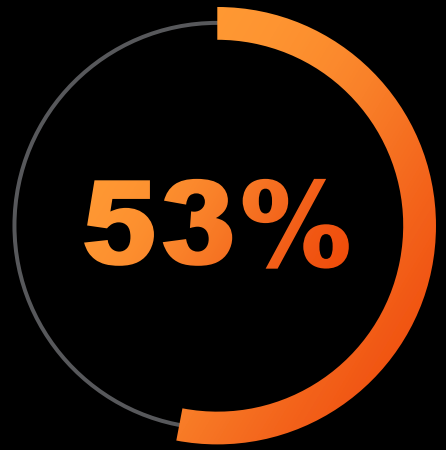


User Action

Aufschlüsselung



Top Vulnerabilities



In über der Hälfte der Incidents (53%) war mindestens eine von **10 spezifischen Schwachstellen involviert**

Drei dieser 10 Schwachstellen wurden in 25% der Intrustions genutzt:

CVE-2023-34362 – MOVEit Transfer

CVE-2022-47966 – ManageEngine

CVE-2022-41080 & 41082 – Microsoft Exchange

60% der Incidents beinhalteten eine Schwachstelle mit **einer CVE-Zuweisung vor 2023**

TTPs to Watch

T1059.001 – Command and Scripting Interpreter: PowerShell

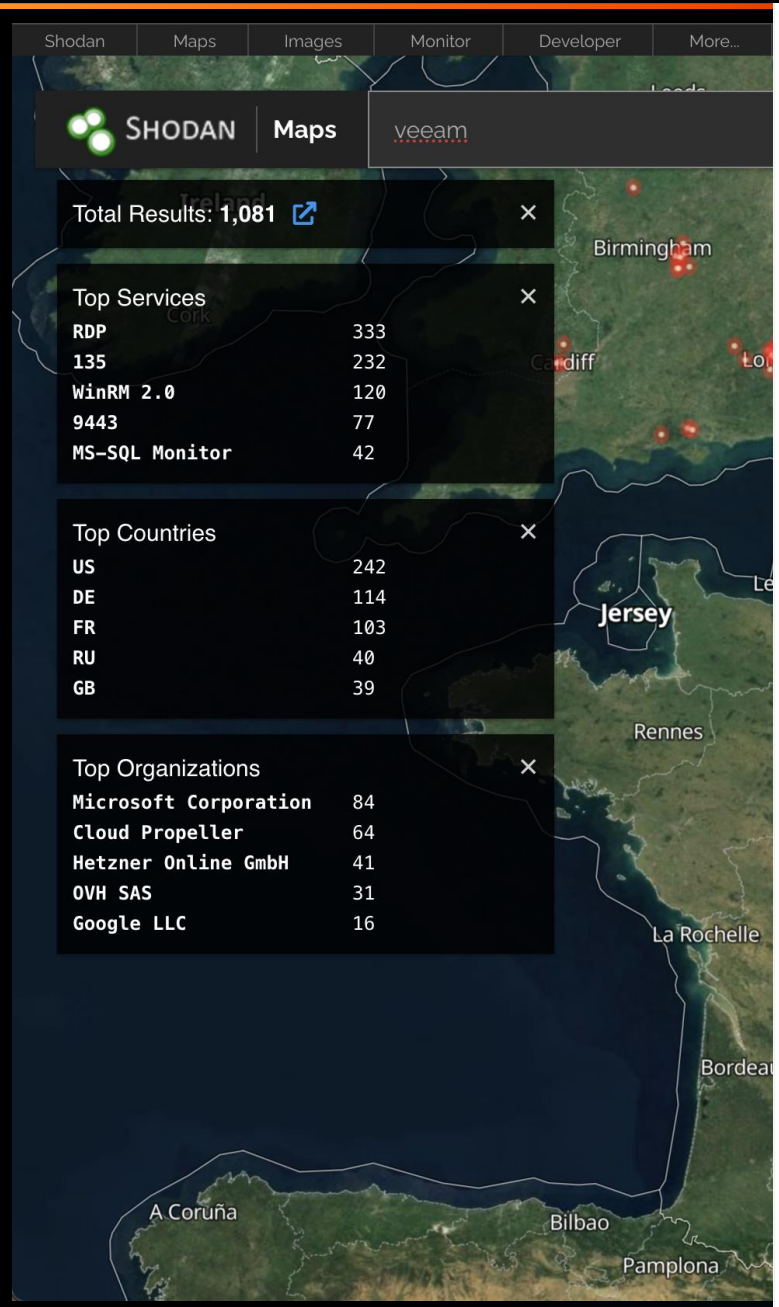
T1105 – Ingress Tool Transfer

T1047 – Windows Management Instrumentation

T1027.010 – Obfuscated Files or Information: Command Obfuscation

T1608.006 – Stage Capabilities: SEO Poisoning

Case: Negativbeispiel Ransomware / Fluggesellschaft



Stephan Berger
Head of Investigations at InfoGuard AG
3w

During a recent Incident Response case, it was evident that the attacker disabled Defender on various hosts during a timeframe of a few hours.

Would you detect such behavior in your environment? Do you monitor for AV disabling and, on top of that, monitor for a threshold of systems left unprotected within a certain period?

Windows Defender creates the EventID 5001 = "Real-time protection is disabled."

https://lnkd.in/e8SNdkMZ


```
{
  "Provider": {
    "Name": "Microsoft-Windows-Windows Defender",
    "Guid": "11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78"
  },
  "EventID": {
    "Value": 5001
  },
  "Version": 0,
  "Level": 4,
  "Task": 0,
  "Opcode": 0,
  "Keywords": 9223372036854775808,
  "TimeCreated": {
    "SystemTime": 1717799555.6239376
  },
```


1,473 · 72 Comments

Like Comment Share

Jackson Draper 3w
Detection and Response at Anduril

Depending on the operating system, an attacker could just tamper with the EDR and overwrite it to stop functioning while the process still technically is running on the system. A wholistic approach to this could be to monitor check-ins to your various tools. If the host is checking in to your other tools, but not your

https://blogs.blackberry.com/en/2024/07/akira-ransomware-targets-the-latam-airline-industry

Empfehlungen

Wichtigste Safeguards

Empfehlungen bezogen auf bearbeitete Fälle

Ein solides Verständnis für die eigene Angriffsoberfläche entwickeln

Visibilität! Breite und Schnelligkeit vor Tiefe, in die Umgebung und in die einzelnen Assets

Identity Controls: Ohne Ausnahmen

Zero-Trust für Identitäten und Netzwerk

Cloud: Verantwortung wahrnehmen

Etablieren einer Sicherheitskultur

Weitere Ressourcen

Threat Report

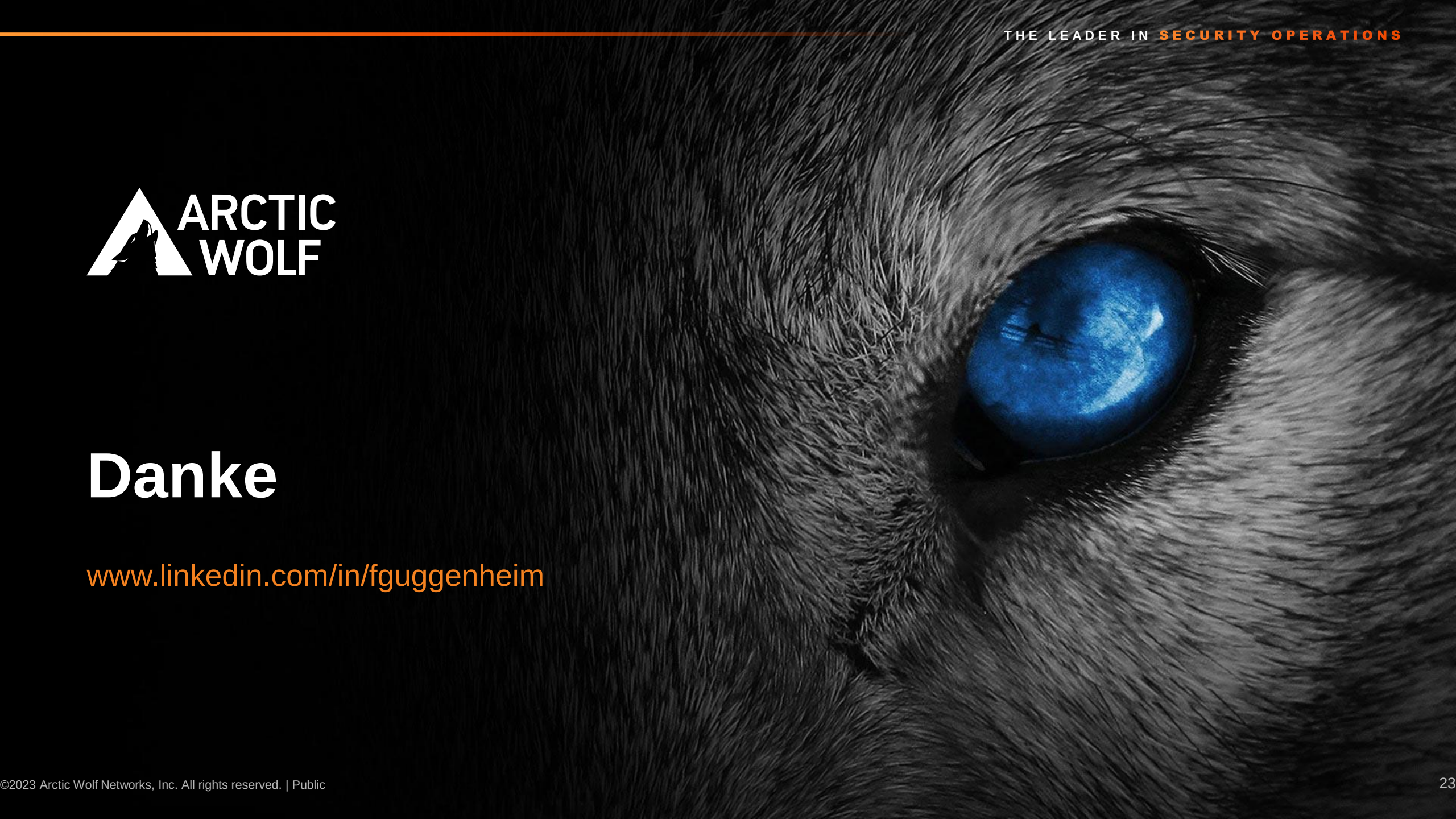
arcticwolf.com/2024threatreport

Predictions Report

arcticwolf.com/2024predictions

Trials für Cyberplanung

arcticwolf.com/solutions/cyber-jumpstart/



Danke

www.linkedin.com/in/fguggenheim