END CYBER RISK

Pierre Flammer, Director Sales Engineering DACH

Technologie-Trends haben die Cyber-Risiken dramatisch erhöht

Die “Cloud“
zerstört die Perimeter

Explodierende
Angriffsziele

Raffinierte
Angreifer & **Massen**
an Attacken

Ansteigendes Risiko

90%

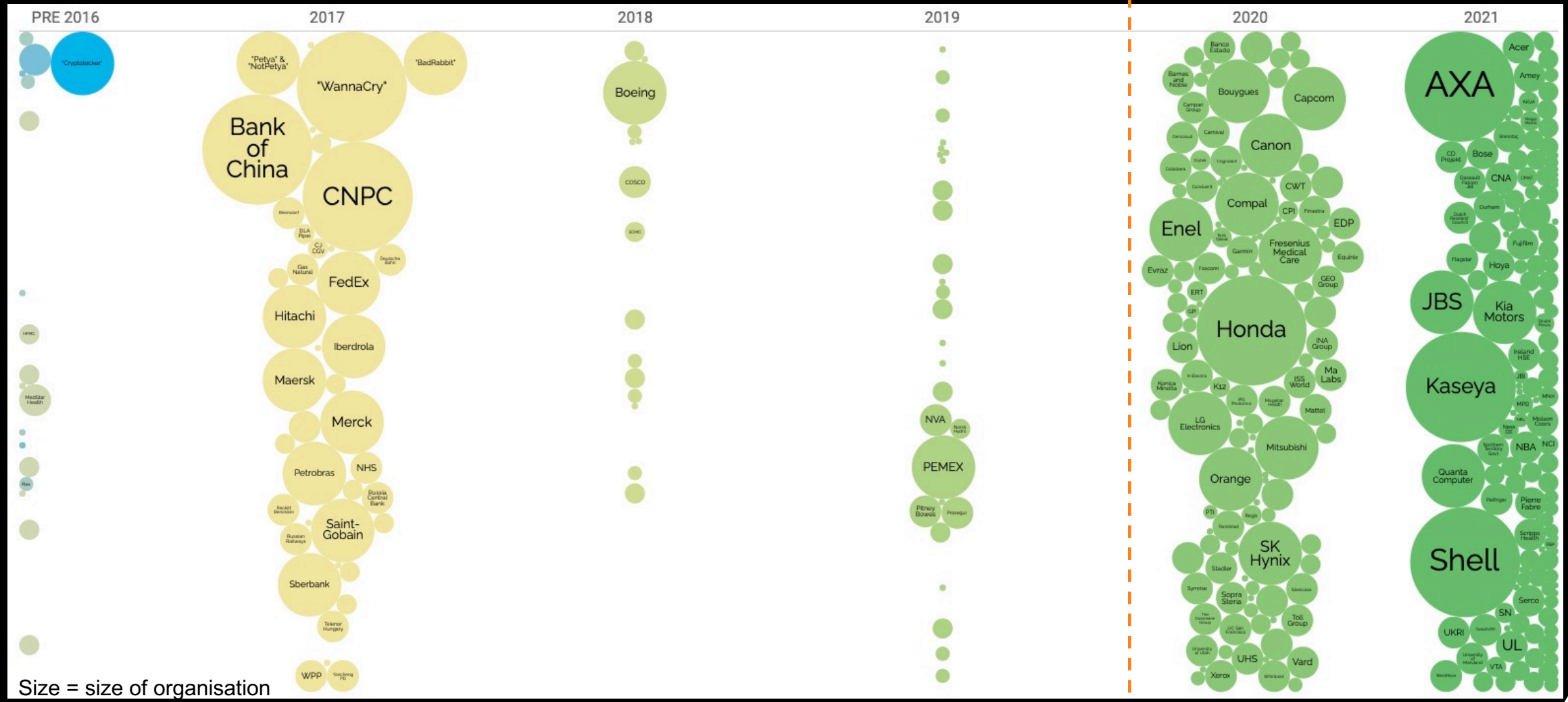
der IT-Verantwortlichen glauben Ihre Organisation wird den Anforderungen nicht gerecht.

Source: Foundry 2021 Security Priorities Study.

Visualisation – Ransomware Attacks

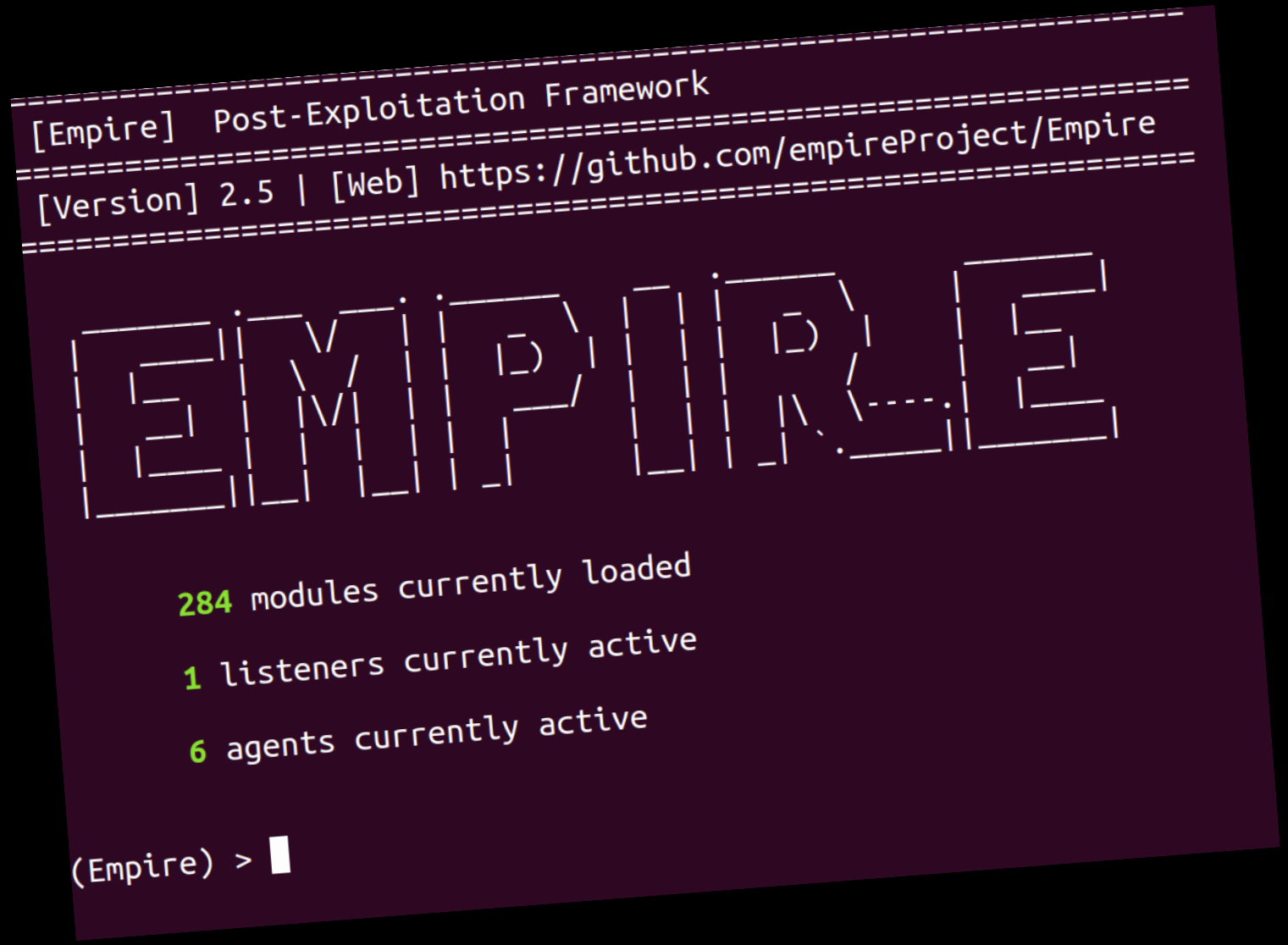
https://informationisbeautiful.net/visualizations/ransomware-attacks/

Covid / Home Office
Cloud Anywhere

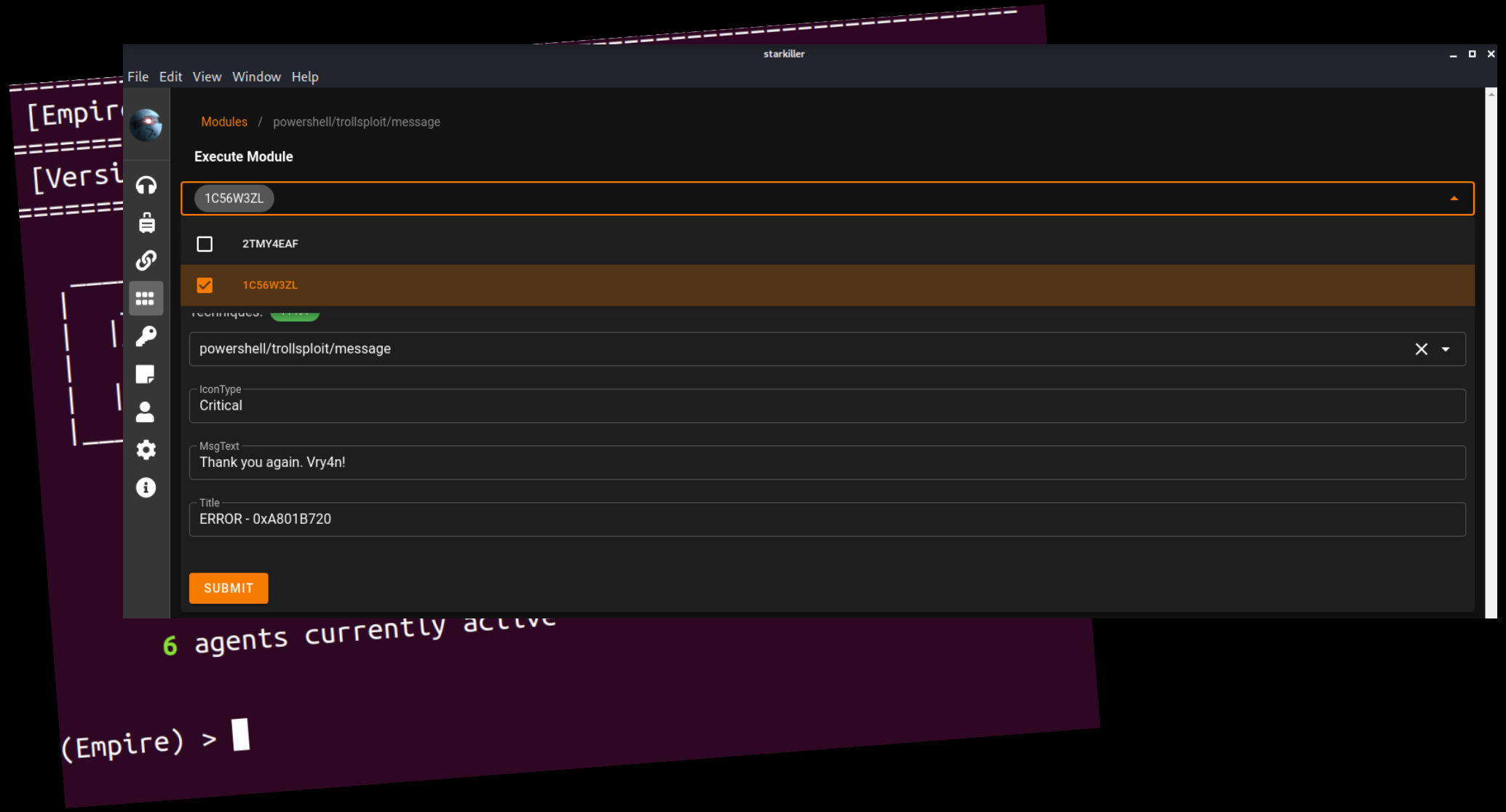


Size = size of organisation

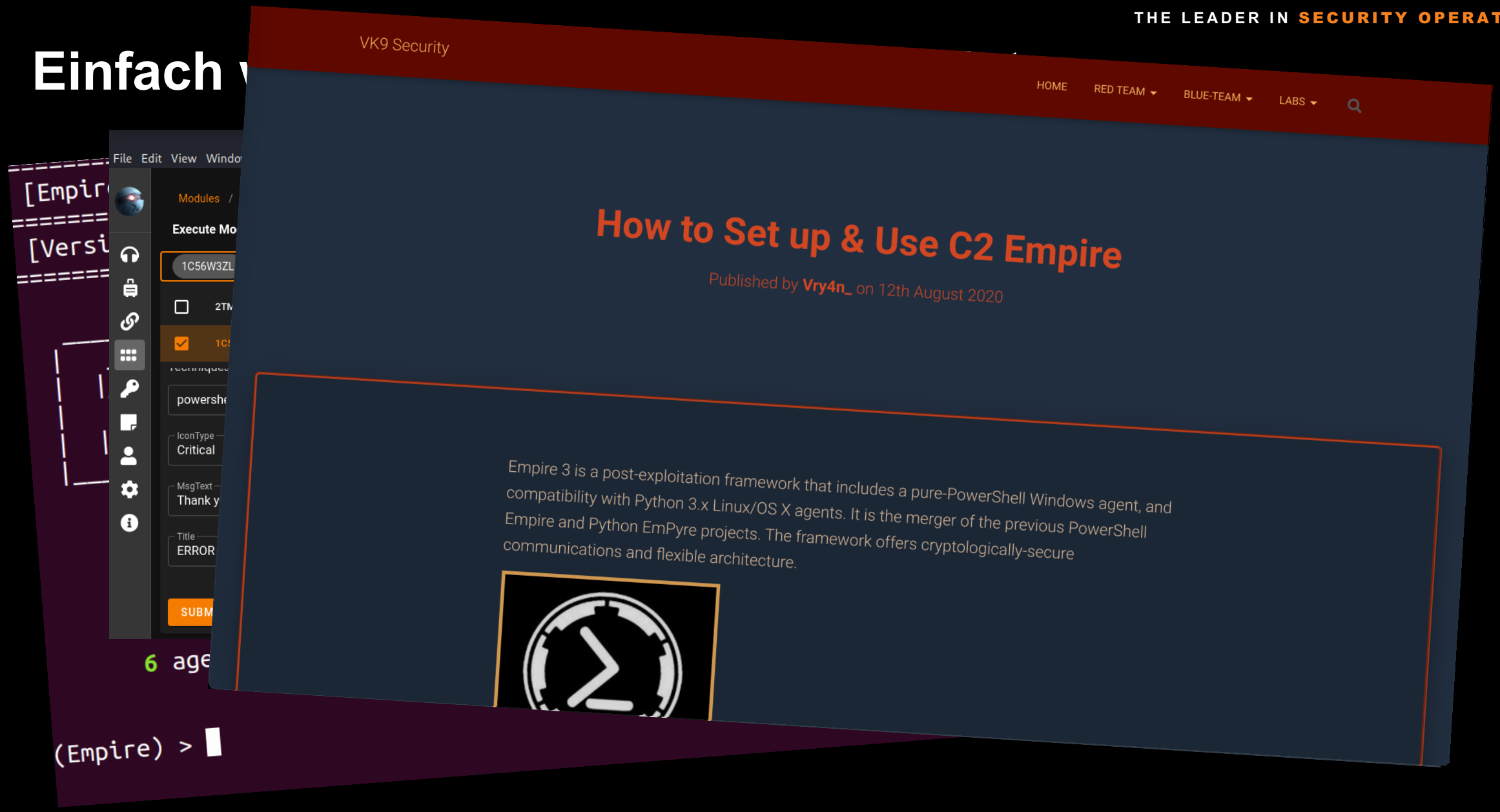
Einfach weil einfach einfach einfach ist



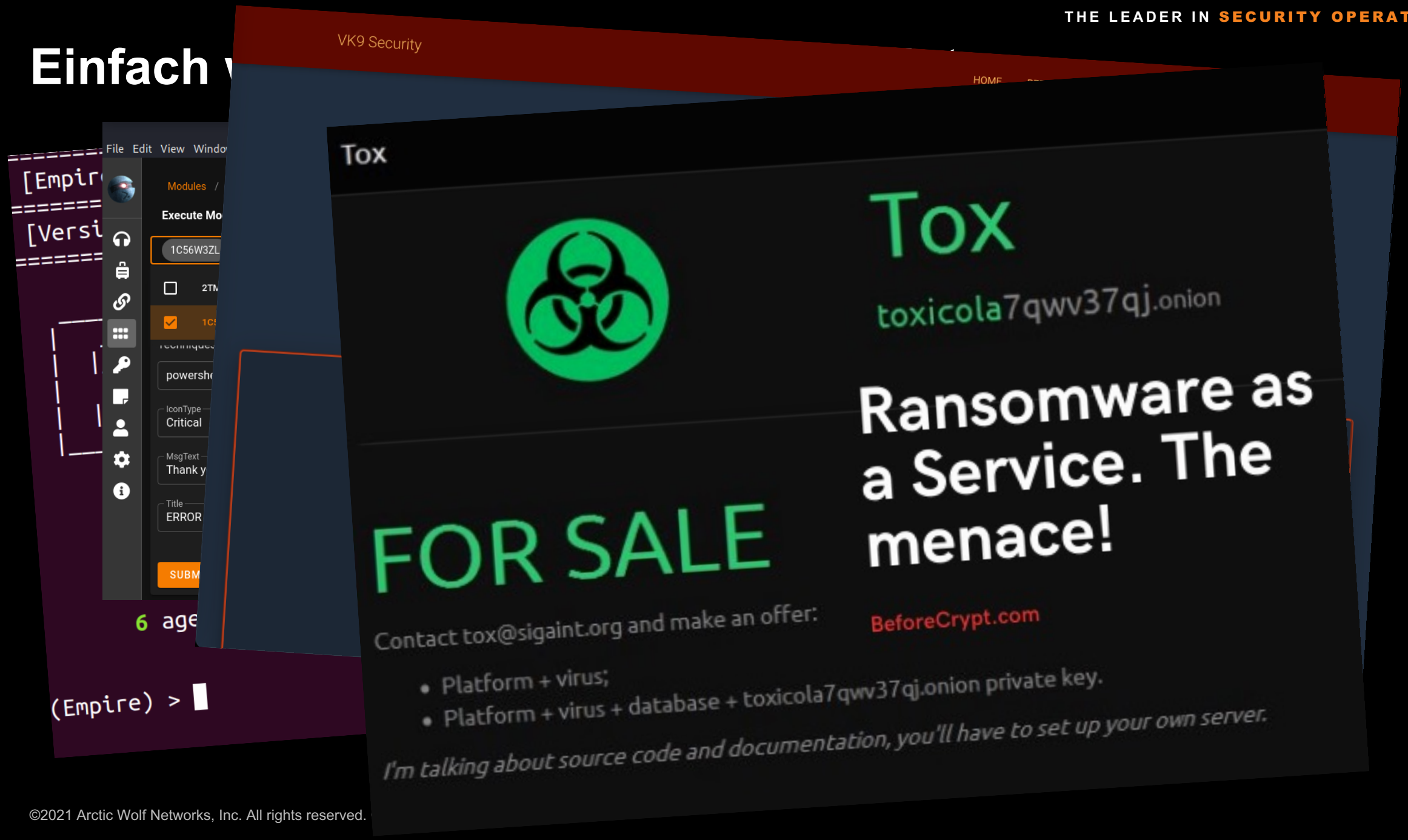
Einfach weil einfach einfach einfach ist



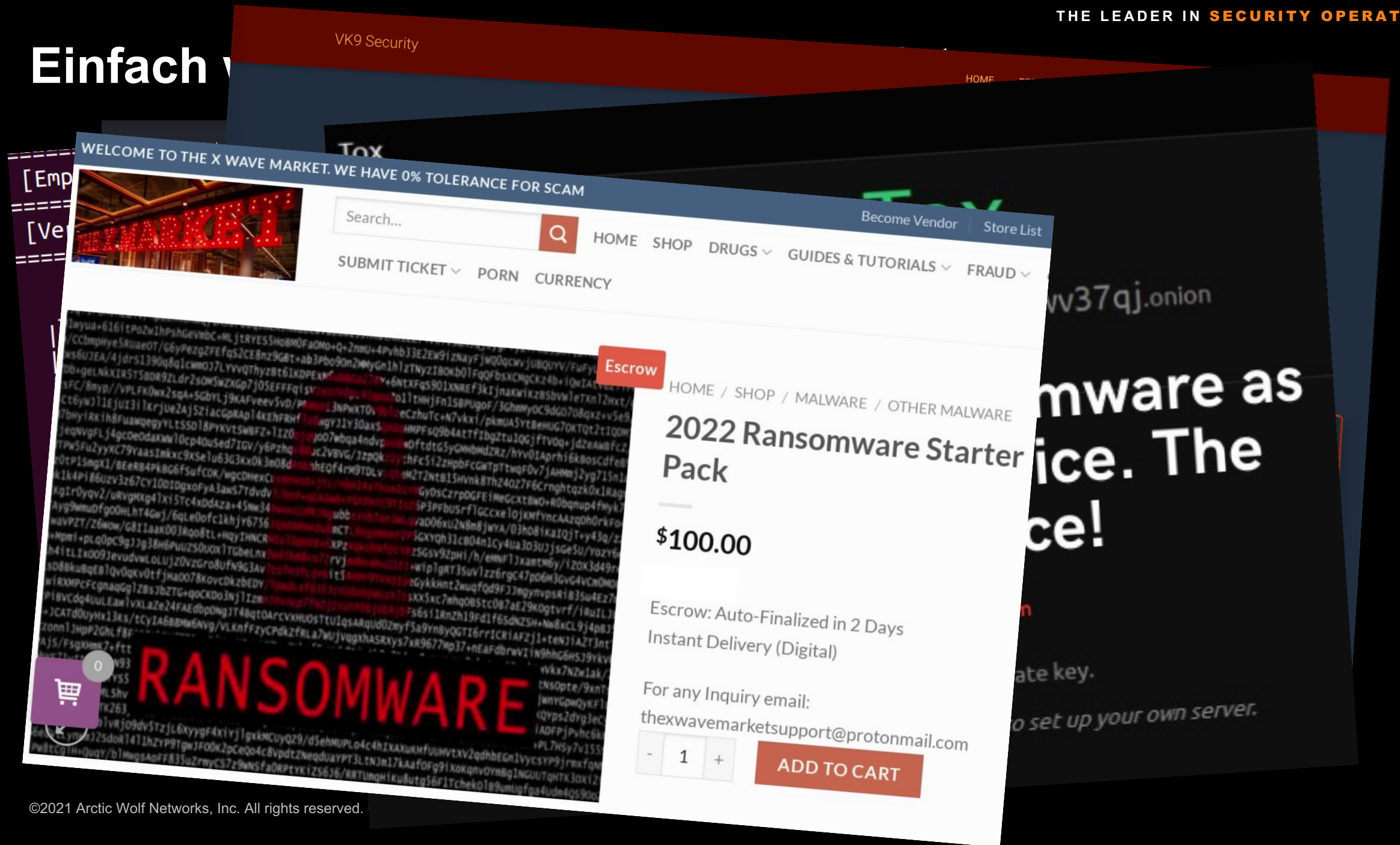
Einfach



Einfach



Einfach v



Einfach

VK9 Security

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Inside Trickbot, Russia's Notorious Ransomware Gang

Internal messages WIRED has viewed shed new light on the operators of one of the world's biggest botnets.

PHOTOGRAPH: KATLEHO SEISA/GETTY IMAGES

Vendor | Store List

ALS FRAUD

wv37qj.onion

MALWARE

mware as
ice. The
ce!

ate key.

o set up your own server.

avemarketsupport@protonmail.com

- 1 +

ADD TO CART

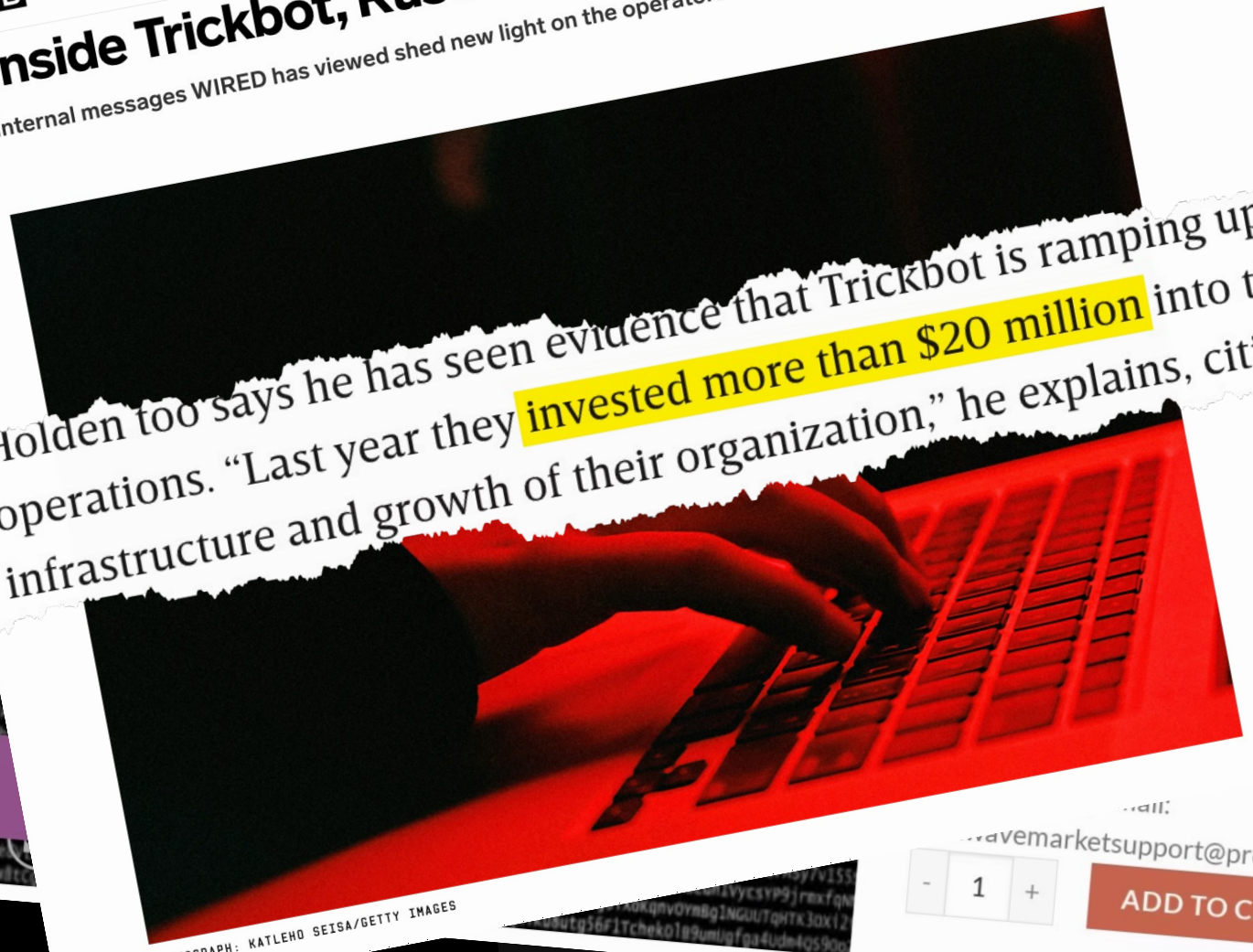
Einfach

VK9 Security

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Inside Trickbot, Russia's Notorious Ransomware Gang

Internal messages WIRED has viewed shed new light on the operators of one of the world's biggest botnets.



Holden too says he has seen evidence that Trickbot is ramping up its operations. "Last year they invested more than $20 million into their infrastructure and growth of their organization," he explains, citing

PHOTOGRAPH: KATLEHO SEISA/GETTY IMAGES

Vendor | Store List

ALS FRAUD

wv37qj.onion

mware as
ice. The
ce!

ate key.

o set up your own server.

WARE

arter

avemarketsupport@protonmail.com

1

ADD TO CART

Einfach

VK9 Security

WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Inside Trickbot, Russia's Notorious Ransomware Gang

Internal messages WIRED has viewed shed new light on the operators of one of the world's biggest botnets.

Holden too says he has seen evidence that Trickbot is rampin
operations. "Last year they invested more than $20 million i
infrastructure and growth of their organization," he explain

PHOTOGRAPH: KATLEHO SEISA/GETTY IMAGES

HOME

CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV INVESTING CLUB PRO

Search quotes, news & videos WATCHLIST

TECH

Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'

PUBLISHED WED, APR 13 2022·9:49 PM EDT | UPDATED WED, APR 13 2022·9:55 PM EDT

Monica Buchanan Pitrelli
@MONICAPITRELLI

SHARE

KEY POINTS

- A huge leak of internal documents — thought to be an act of revenge over Conti's pro-Russia stance — revealed details about the notorious hacker group's size, leadership and operations.
- The messages show that Conti operates much like a regular company, with salaried workers, bonuses, performance reviews and even "employees of the month."
- Cybersecurity experts say some workers were told they were working for an ad company and likely were unaware who was employing them.

In this article CHKP UNCH

TV Graduation Night UP NEXT | Dateline 03:00 am ET

TRENDING NOW

1 A psychologi... 7 signs of a ... parent: 'It's a... raise your kid...

2 The 10 most ... work-from-a... companies a... in 2022

3 Mark Zucker... like your scr... Social media ... 'building rela...

4 Why China's ... is shoring up...

EU warns of ... weapon stoc... urges French...

...vavemarketsupport@protonmail.com

- 1 +

ADD TO CART

Einfach

VK9 Security

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Inside Trickbot, Russia's Notorious Ransomware Gang

Internal messages WIRED has viewed shed new light on t

of the world's biggest botnets.

Holden too says he has seen ev
operations. "Last year they inv
infrastructure and growth of th

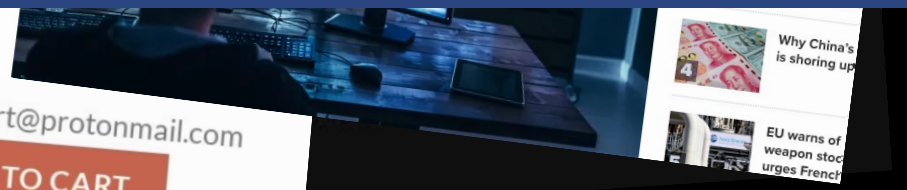
PHOTOGRAPH: KATLEHO SEISA/GETTY IMAGES

CNBC MARKETS BUSINESS INVESTING TECH

Cyber Risk

Double Extortion Ransomware Attacks

OLLIS/AKERS/ARNEY
INSURANCE & BUSINESS ADVISORS
PROTECTING TOMORROW...TODAY.



Why China's is shoring up

EU warns of weapon stoc urges French

avemarketsupport@protonmail.com

- 1 +

ADD TO CART

Die 5 Phasen eines Cyberangriffs

(Passives) Sammeln von Informationen

- Zielidentifikation und -definition
- OSINT (Open-Source Intelligence)

Aktive Informations-Gewinnung

- Network Scans
- Vulnerability Scans
- Mapping

Zugang zum Ziel

- Exploits von Schwachstellen
- Ausnutzung von Konfigurations-Fehlern
- Phishing von Accounts
- Kauf von Zugängen im Darkweb

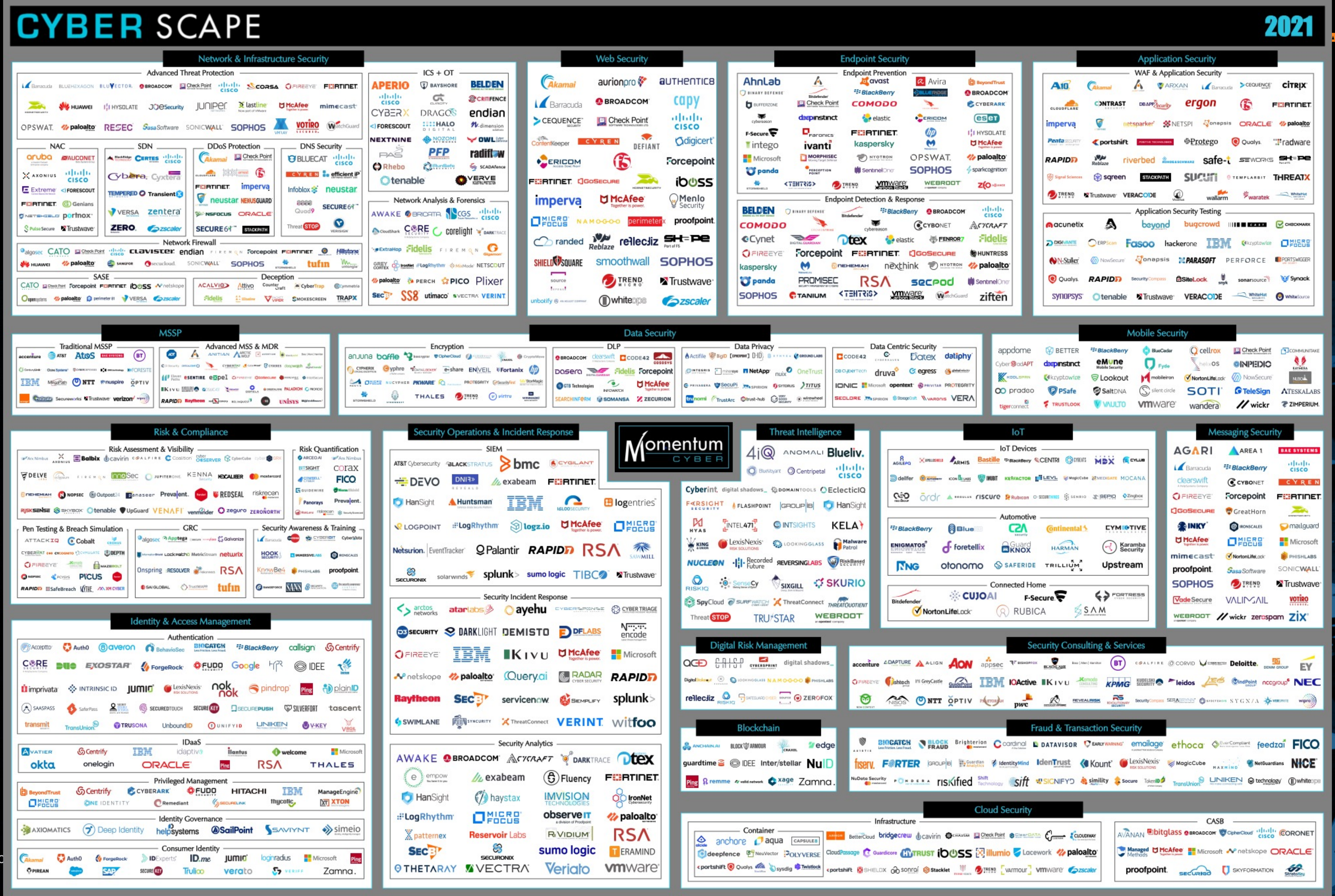
Zugang Absichern und Verursachen des Schadens

- Lateral Movement
- Privilege Escalation
- Einbau von Backdoors
- Erstellung zusätzlicher Nutzer
- Manipulation von Backup
- Datendiebstahl
- Datenlöschung oder -verschlüsselung

Verwischen von Spuren

- Löschung von Logs und Protokollen

ATIONS



©2021 Arc

AI&ML kann den Mensch nicht ersetzten

Was ist das eigentliche Problem?

Presseinformation

IT-Fachkräftelücke wird größer: 96.000 offene Jobs

- **Anzahl freier Stellen für IT-Expertinnen und -Experten nimmt um 12 Prozent zu**
- **Zwei von drei Unternehmen erwarten weitere Verschärfung der Personalnot**

Berlin, 3. Januar 2022 – Für die Digitalisierung der Wirtschaft fehlt immer mehr Personal. Branchenübergreifend ist die Zahl freier Stellen für IT-Fachkräfte 2021 auf 96.000 gestiegen. Das sind 12 Prozent mehr als im Vorjahr, als quer durch alle Branchen 86.000 Jobs unbesetzt blieben. Zu diesem Ergebnis kommt die neue Bitkom-Studie zum

Die Denkweise muss sich ändern.

Weg von Tools und hin zu effektivem Betrieb.

Investments schützen

Bestehende Technologien nutzen und optimieren

Breitere Visibilität

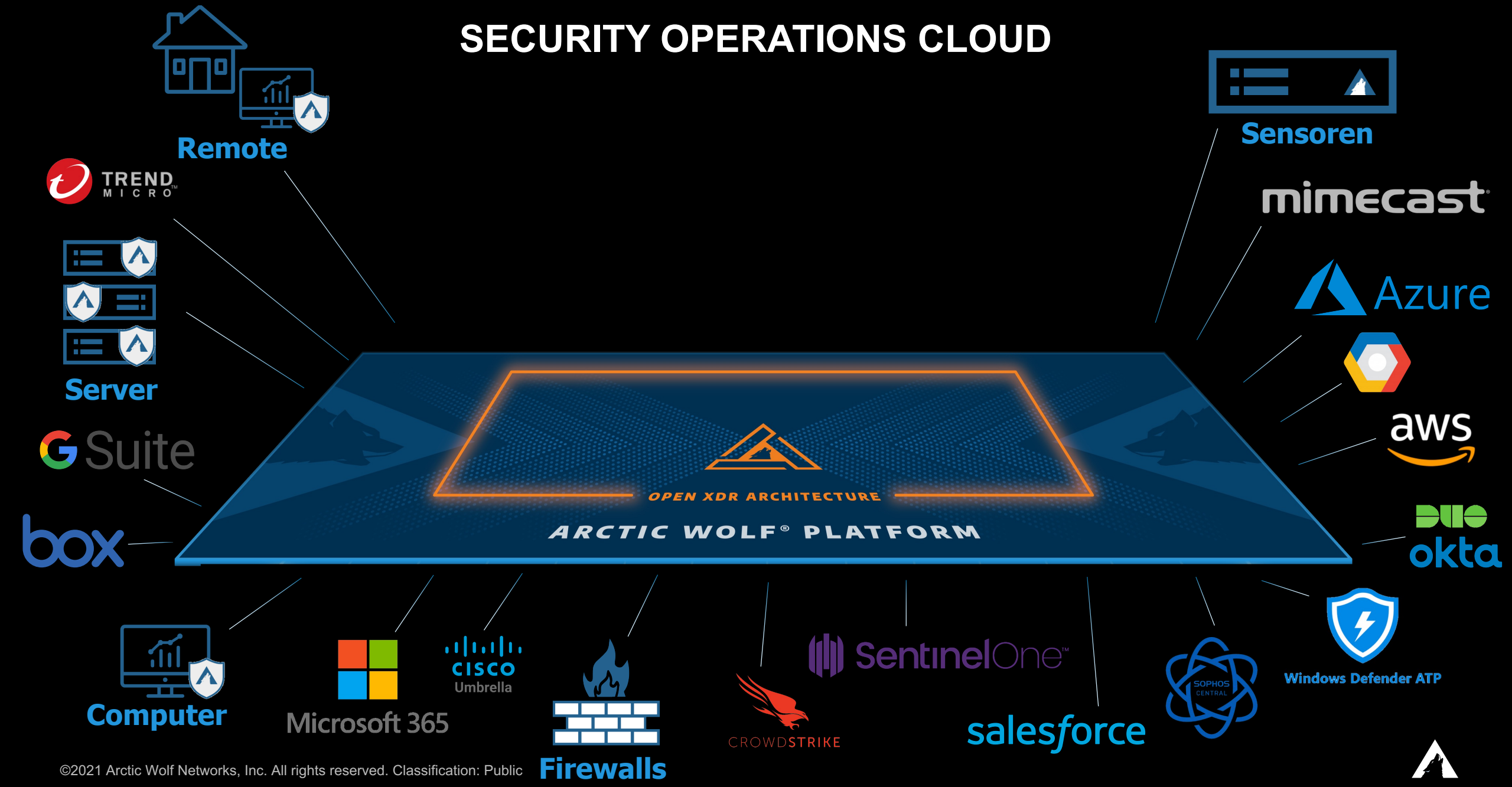
Breite Abdeckung gegenüber allen Angriffstypen und Punkten

Widerstandsfähiger werden

Hinzufügen von Experten, 24x7 Überwachung & Schutz, sowie Einführung von taktischen und strategischen Security Aktionen.

ARCTIC WOLF
SECURITY OPERATIONS

SECURITY OPERATIONS CLOUD



Security Operations im großen Stil

450+
Milliarden Logzeilen pro Tag

500+
TB verarbeitet pro Tag

>1.3M
AW active Agenten und 12,500 Sensoren

10 Jahre
Erfahrung / SOC2 Type und ISO 27001

>700.000
Kundenspezifische Reports erstellt für >5.300 Kunden

83%
aller Tickets wurden von Arctic Wolf Technologie entdeckt

MARKTFÜHRENDE SCHWARMINTELLIGENZ

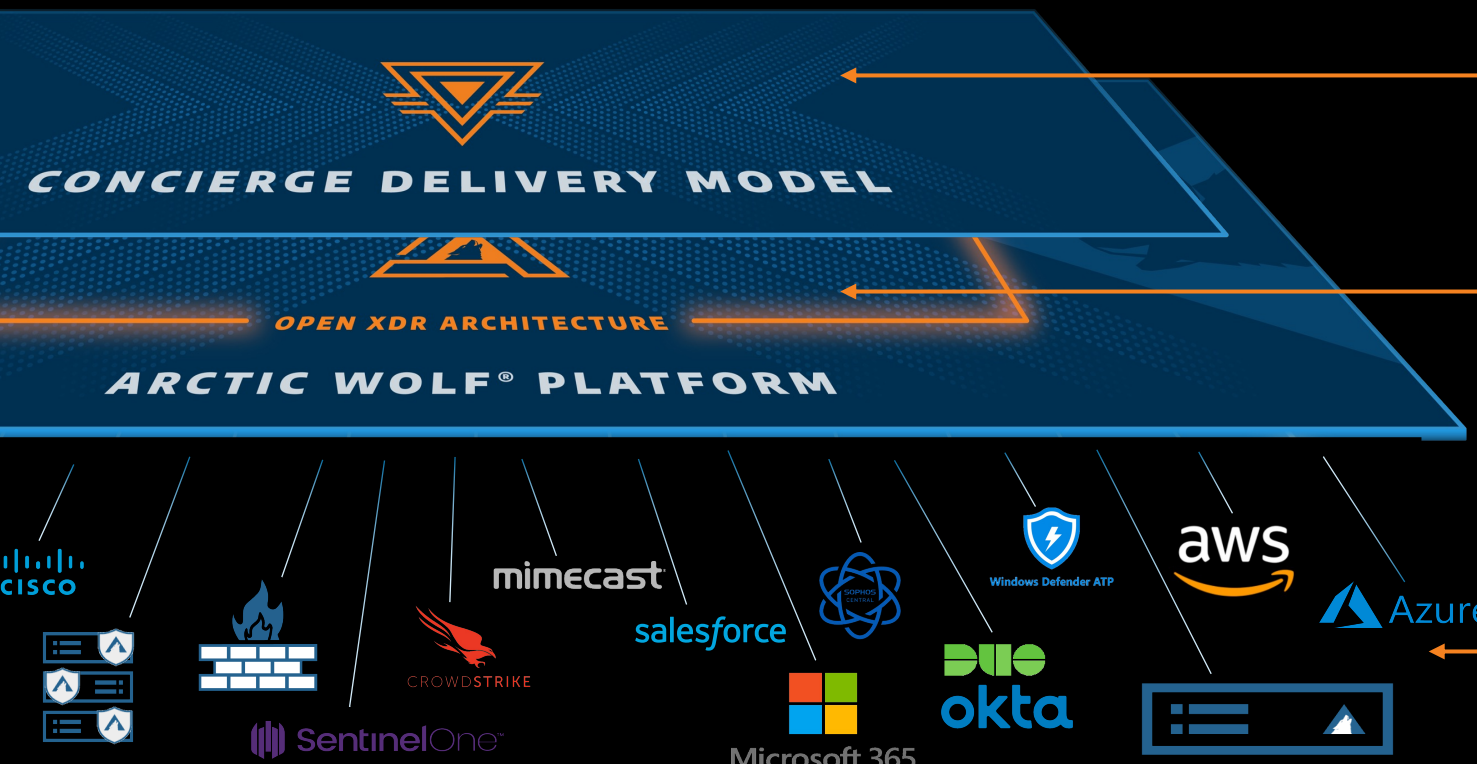
MAßGESCHNEIDERTE UNTERSTÜTZUNG

<1 Ticket
pro Tag im Schnitt

>99%
True positives

Einheitliche
Sicht auf Ihre Security

SECURITY OPERATIONS CLOUD



Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

Zentralisierung aller Daten in der Arctic Wolf Plattform für: Speicherung, Anreicherung, Korrelierungen, Analysen und Untersuchungen

Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

Arctic Wolf Security Journey

Onboarding Team & Kunde

CST und Kunde

Phase 1

Onboarding
Ca. 30 Tage

Erbracht durch das Onboarding Team

- Projekt Kick Off & Technical Kick Off
- Vorstellung des Portals
- Sensoren werden verschickt
- Konfiguration der Log-Quellen, ausrollen des Agenten

Phase 2

Die ersten 90 Tage
Go Live

Das Concierge Security Team übernimmt den Service zum Kunden

- Meetings alle zwei Wochen
- Der Service wird auf die Anforderungen des Kunden angepasst

Customization Journey

Überprüfung von

- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

Kennenlernen, Businessprozesse verstehen

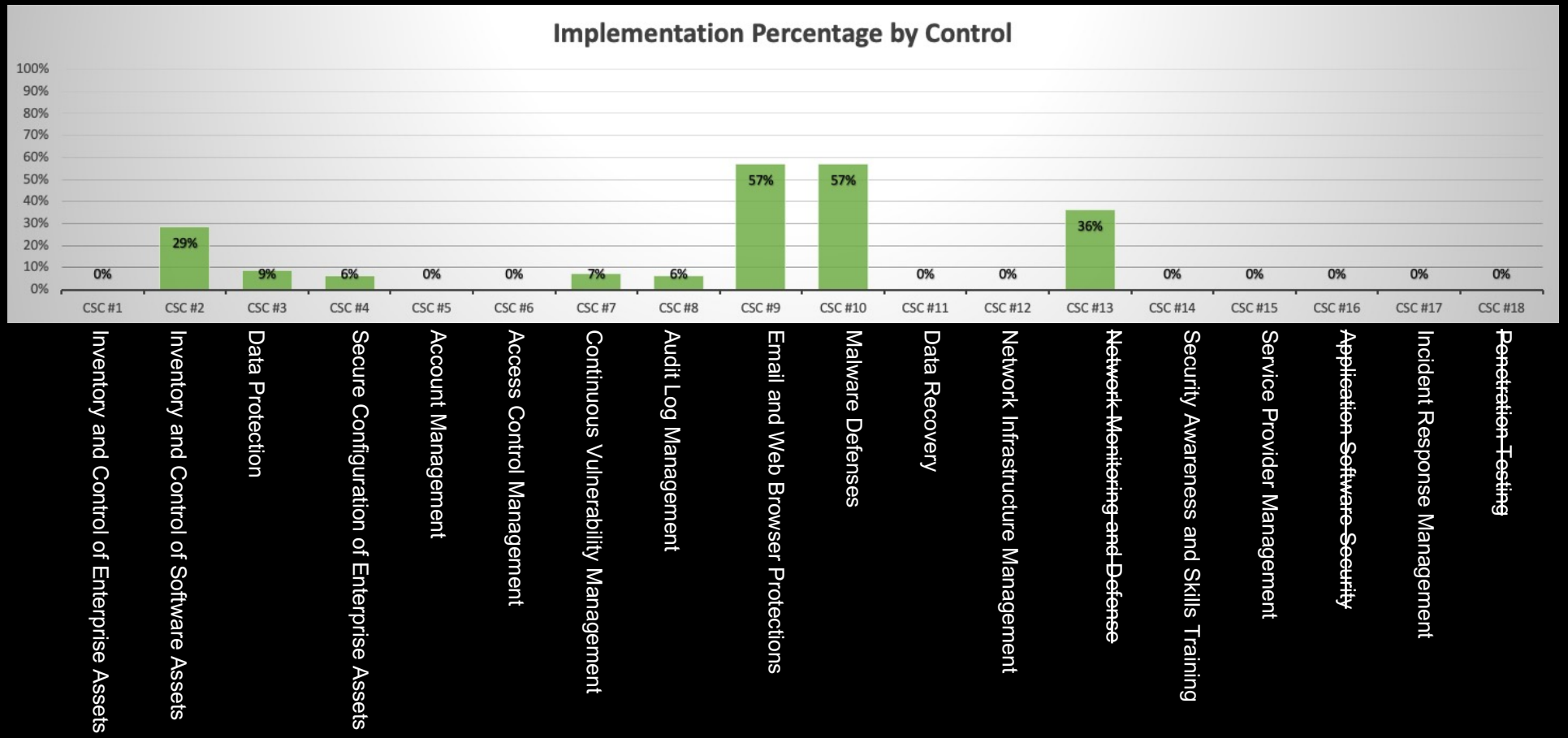
Finetuning der Plattform

Cyber Defence Maturity Assessment

Phase 3

CDMA ohne Arctic Wolf

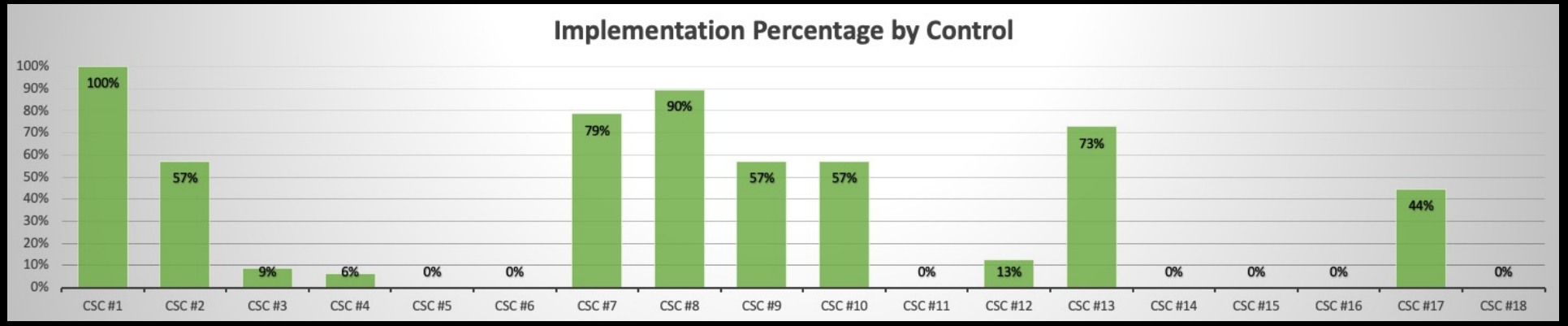
Nach der Analyse stellt Ihnen ihr Concierge Security Team den Report vor.
Ergebnis ohne Arctic Wolf Services:



Maturity Ranking: **0,72**/5

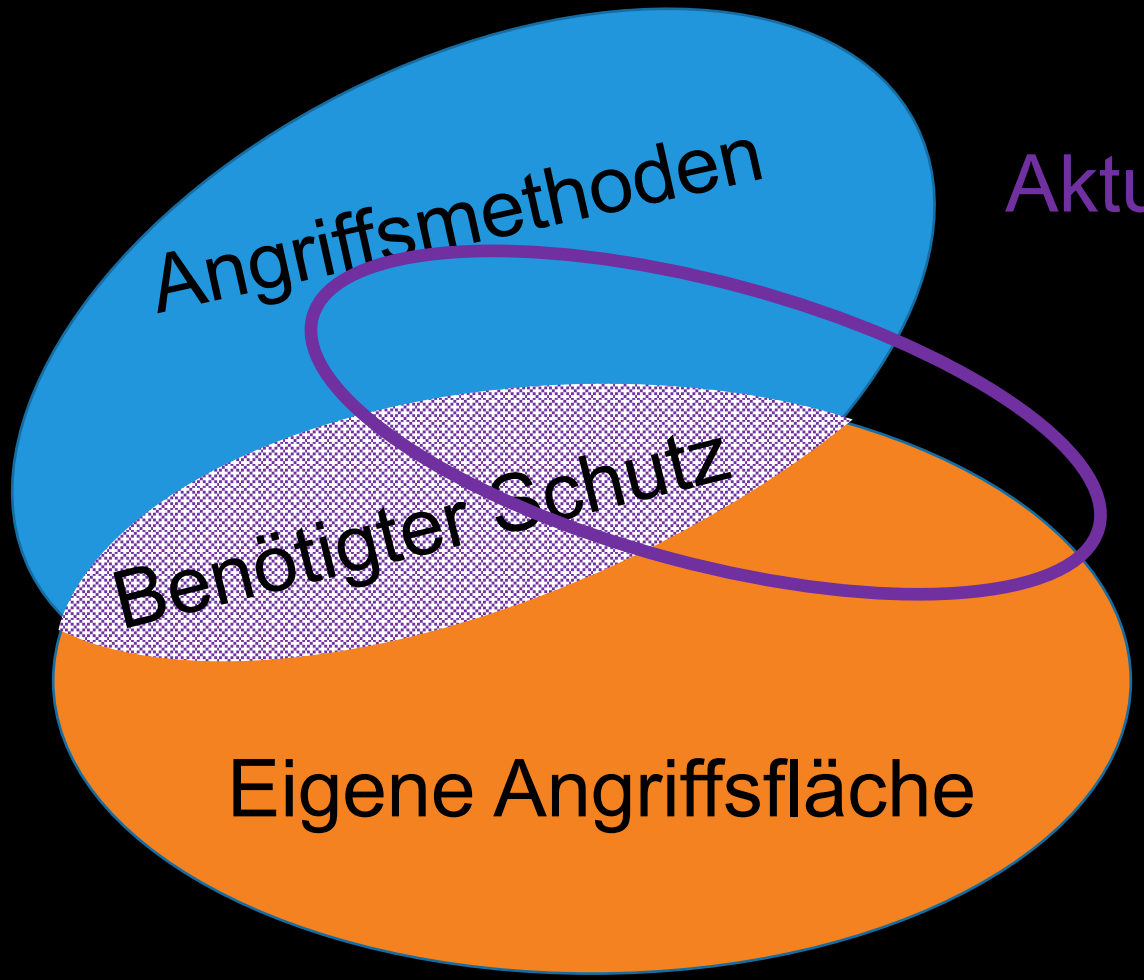
CDMA mit Arctic Wolf

Nach der Analyse stellt Ihnen ihr Concierge Security Team den Report vor. Ergebnis mit Arctic Wolf Services:



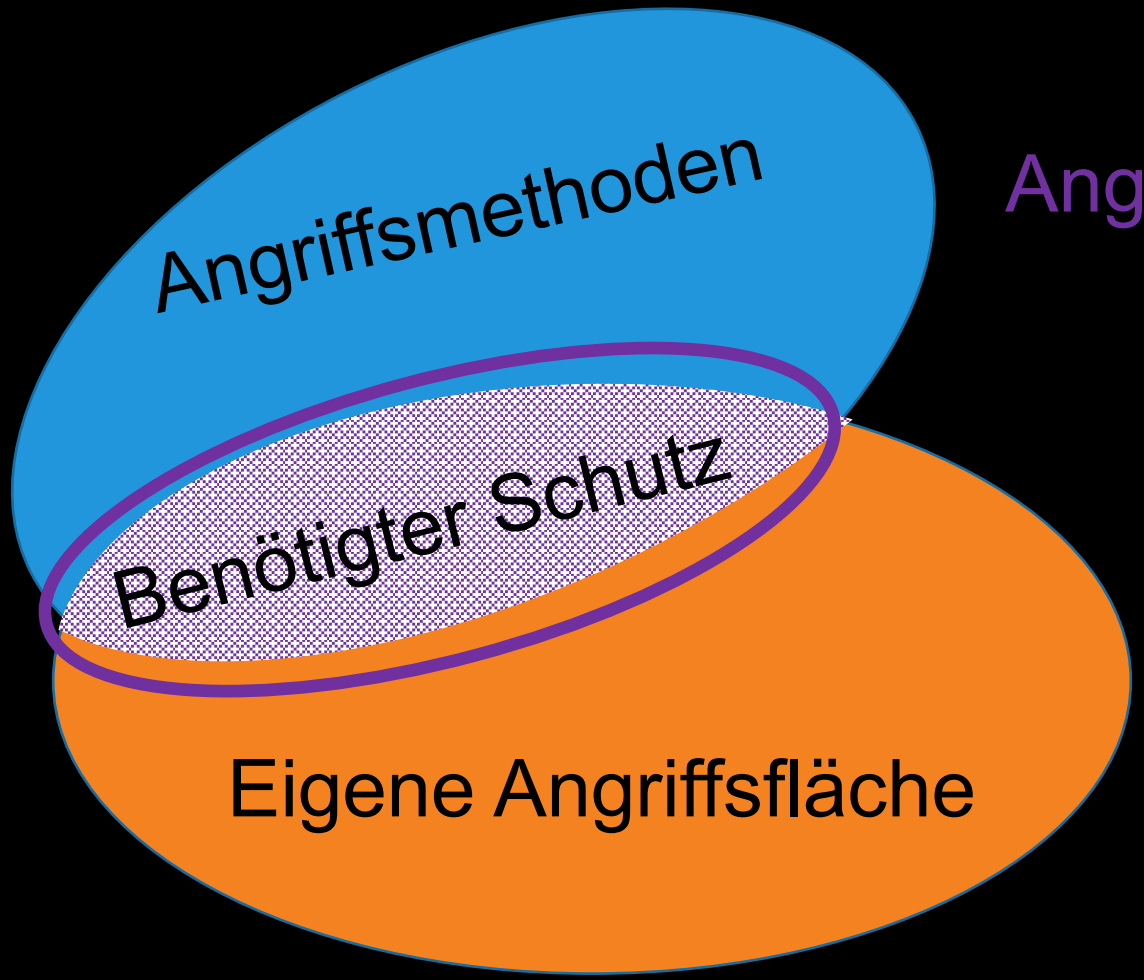
Maturity Ranking: **1,78**/5

Anpassung an den erforderlichen Umfang



Aktueller Schutz

Anpassung an den erforderlichen Umfang



Angepasster Schutz

Das Concierge Team hilft mit

- Fachwissen
- Best Practices
- Kontinuierliche Überprüfungen
- Dokumentation

Arctic Wolf Security Journey

Onboarding Team & Kunde

CST und Kunde

Phase 1

Onboarding
Ca. 30 Tage

Erbracht durch das Onboarding Team

- Projekt Kick Off & Technical Kick Off
- Vorstellung des Portals
- Sensoren werden verschickt
- Konfiguration der Log-Quellen, ausrollen des Agenten

Phase 2

Die ersten 90 Tage
Go Live

Das Concierge Security Team übernimmt den Service zum Kunden

- Meetings alle zwei Wochen
- Der Service wird auf die Anforderungen des Kunden angepasst

Customization Journey

Überprüfung von

- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

Kennenlernen, Businessprozesse verstehen

Finetuning der Plattform

Cyber Defence Maturity Assessment

Phase 3

Dauerzustand

Unlimitierter Zugriff auf das Concierge Security Team

Security Journey – Regelmäßige Termine

#1 **#2** **#3** **#...**

Fokus nach Kundenwunsch

Detour(s)

Ad-hoc SPiDRs

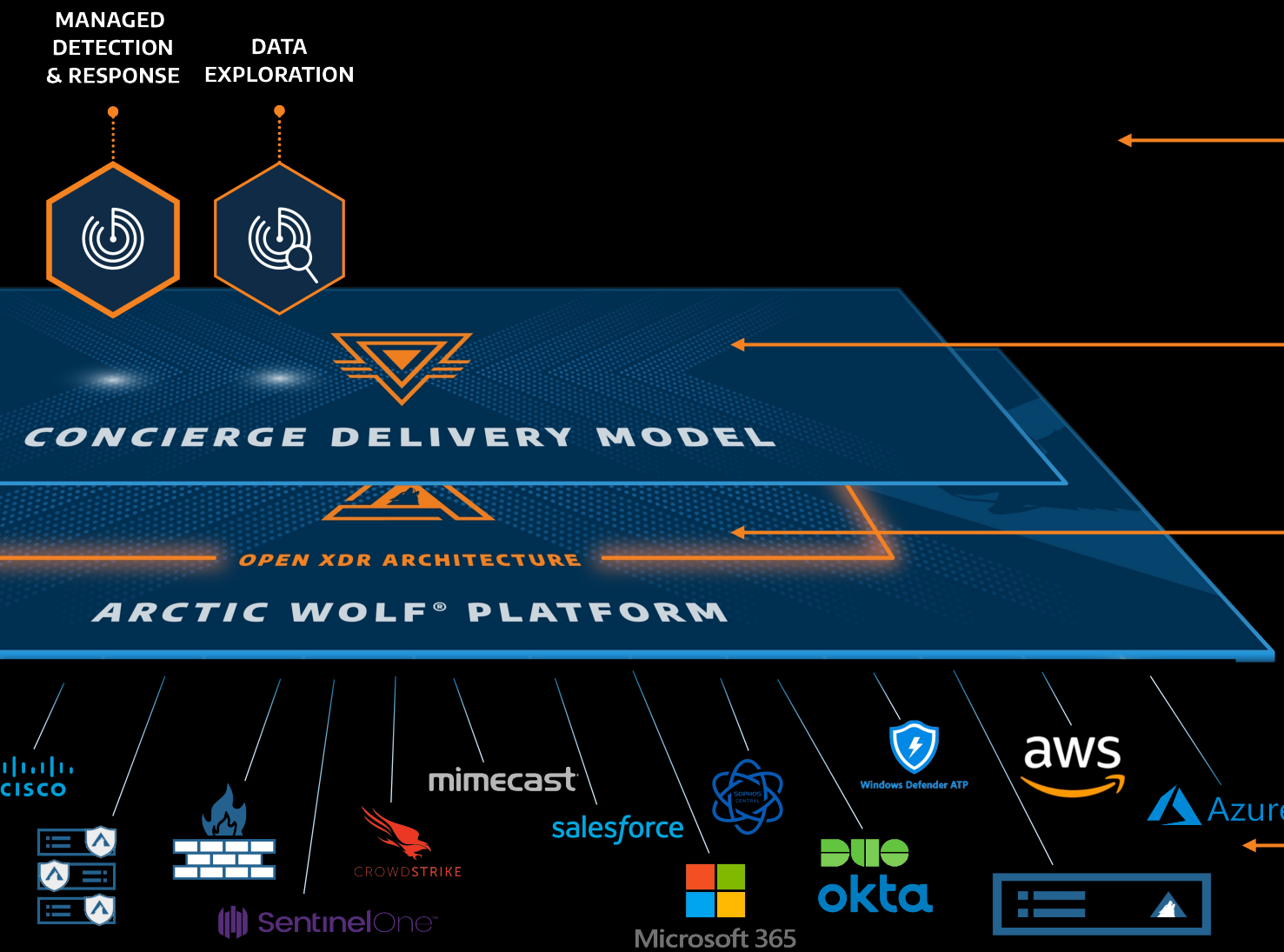
SPiDRs *(Security Posture in Depth Reviews)*

Angepasst für jeden Kunden

- Bewertung – Lücken/Risken
- Konfigurations-Checks – Services (z.B. AD)
- Best Practice – Empfehlungen

AW Security Operation Teams

SECURITY OPERATIONS CLOUD



Wir stellen Services für das gesamte **Security Operations Modell** zur Verfügung

Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

Zentralisierung aller Daten in der Arctic Wolf Plattform für: Speicherung, Anreicherung, Korrelierungen, Analysen und Untersuchungen

Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

[REAL] INCIDENT TIMELINE
Business Email Compromise

Business Email Compromise - Manufacturing

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST | Bad Guys

12:57

- Attacker leveraged previously stolen [User1] credentials and sends Duo MFA pushes to legitimate user.
- [User1] accepts Duo MFA push from attacker
- Attacker establishes ActiveSync with [User1] mailbox

Source: Duo

The Arctic Wolf Platform logs MFA successful for [User1]

12:57

13:16

- Attacker opens existing calendar event for “Best Practices Training” and updates with their own information.
- Attacker begins adding forward and delete rules to [User1] inbox.

Source: Office 365 Logs

Platform escalates incident after seeing rules being edited on [User1] account

13:16

13:18

- Arctic Wolf Triage Team begins investigation into [User1] activity

Attacker uploads phishing PDFs to OneDrive with intent to distribute emails to calendar invite attendees

13:22

13:25

- Triage Team investigates and alerts customer that [User1] has been compromised
- Recommends disabling of account and resetting credentials

- Customer confirms [User1] compromise
- Customer disables account

13:25

13:31

- Concierge Security Team works with customer to check log data for any customer users accessing phishing PDF
- CST confirms remediation took place before any users accessed the PDF. CST assists customer in remediating actions taken by the adversary.

Wichtigste Erkenntnisse

Angriffstyp

Account Takeover

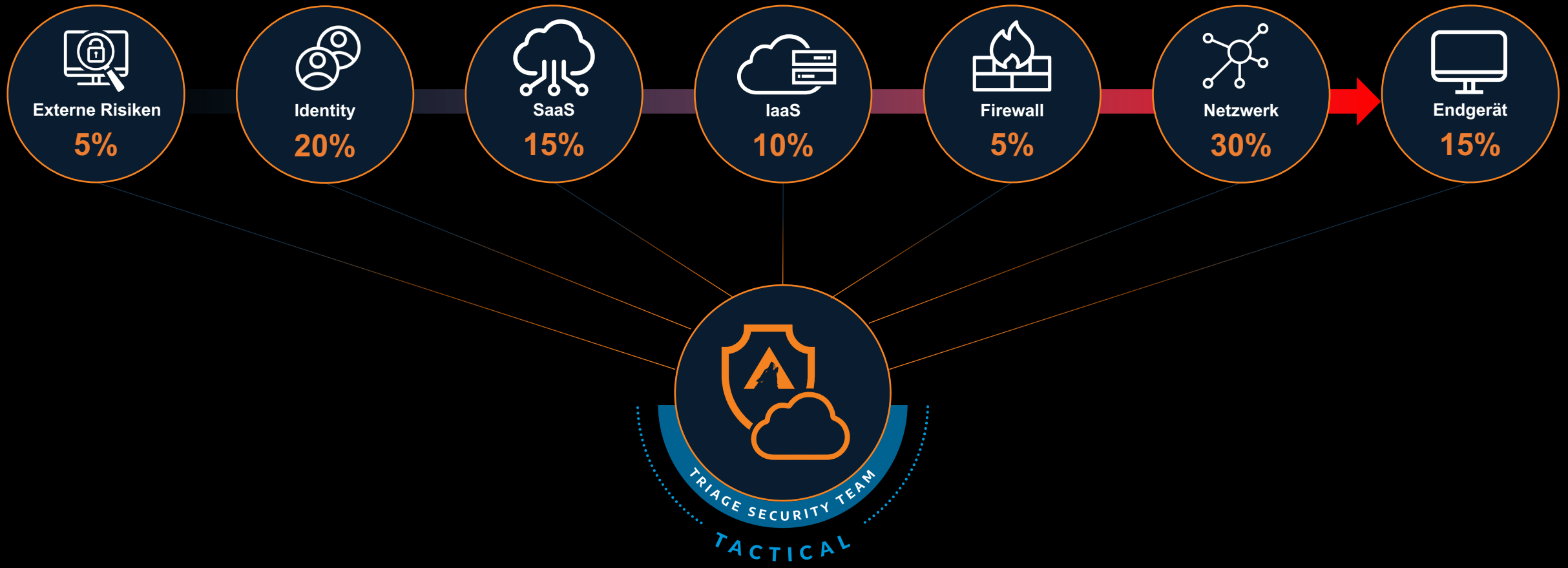
Zeit bis Erkennung

12:57 - 13:16 | 19 Minuten

Datenquellen

Office 365
Duo

Cyberattacke via Cloud & Identity



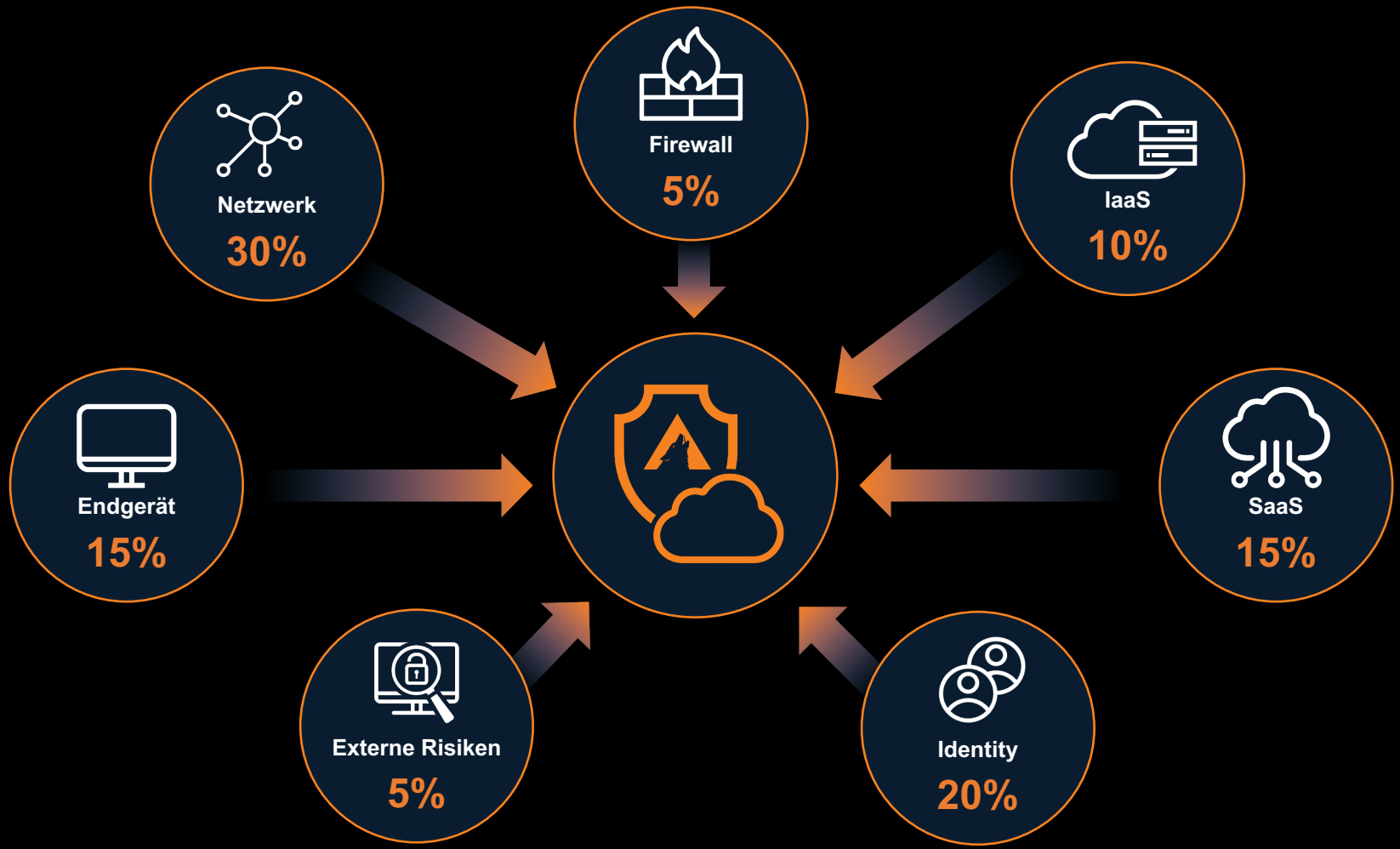
Mehr **als Endgeräte zu schützen, bedeutet *vor* dem Endgerät zu schützen**

Die Frage ist nicht **“*Werde ich über Cloudkompontenen angegriffen?*”** sondern **“an welchem Punkt der Kill-Chain werde ich den Angriff erkennen?”**

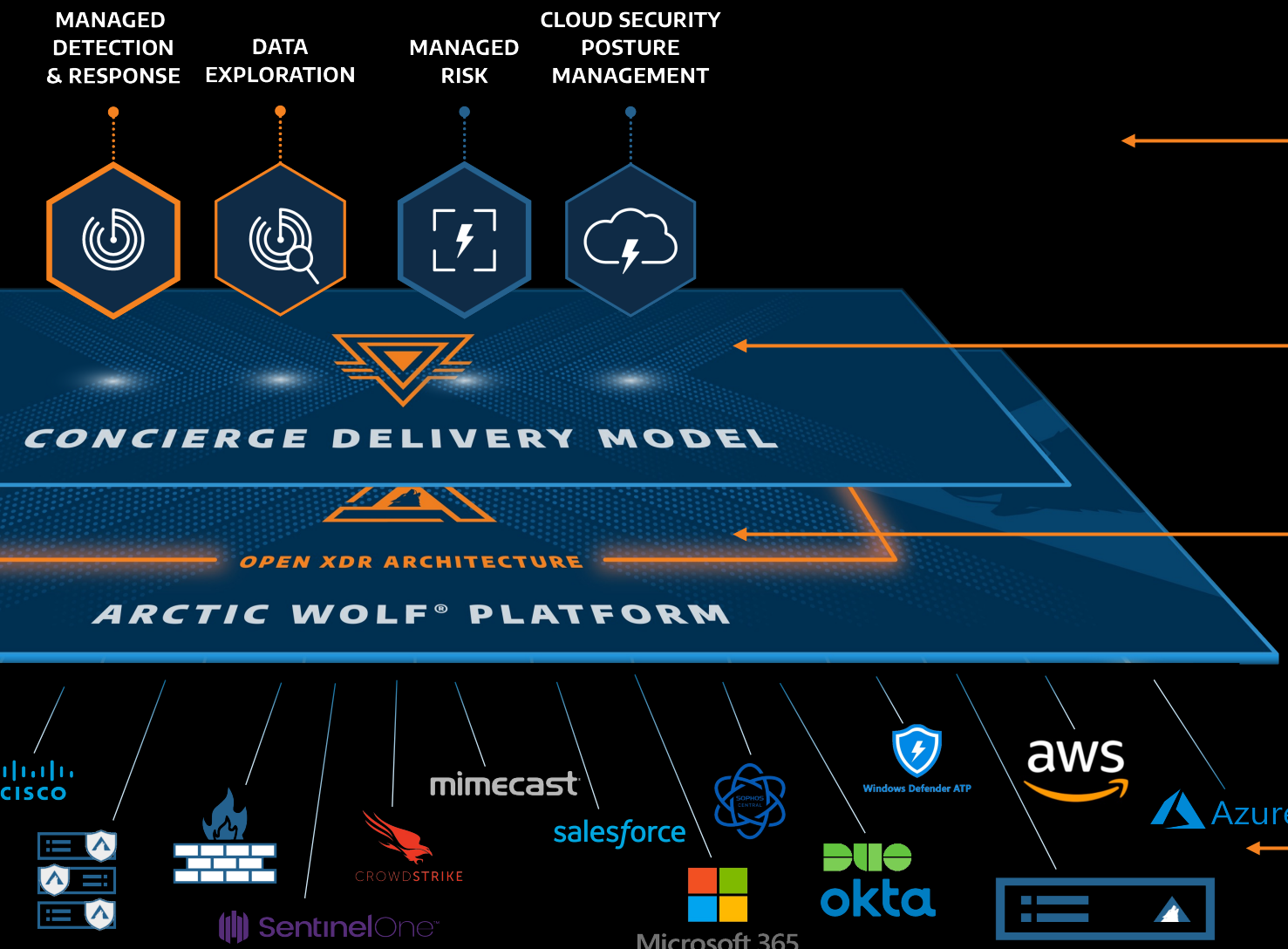
45% der eskalierten Tickets beinhalten Cloud & Identity

Quellen der Tickets

Ermittlungen werden durch den ersten Indikator eingeleitet



SECURITY OPERATIONS CLOUD



Wir stellen Services für das gesamte **Security Operations Modell** zur Verfügung

Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

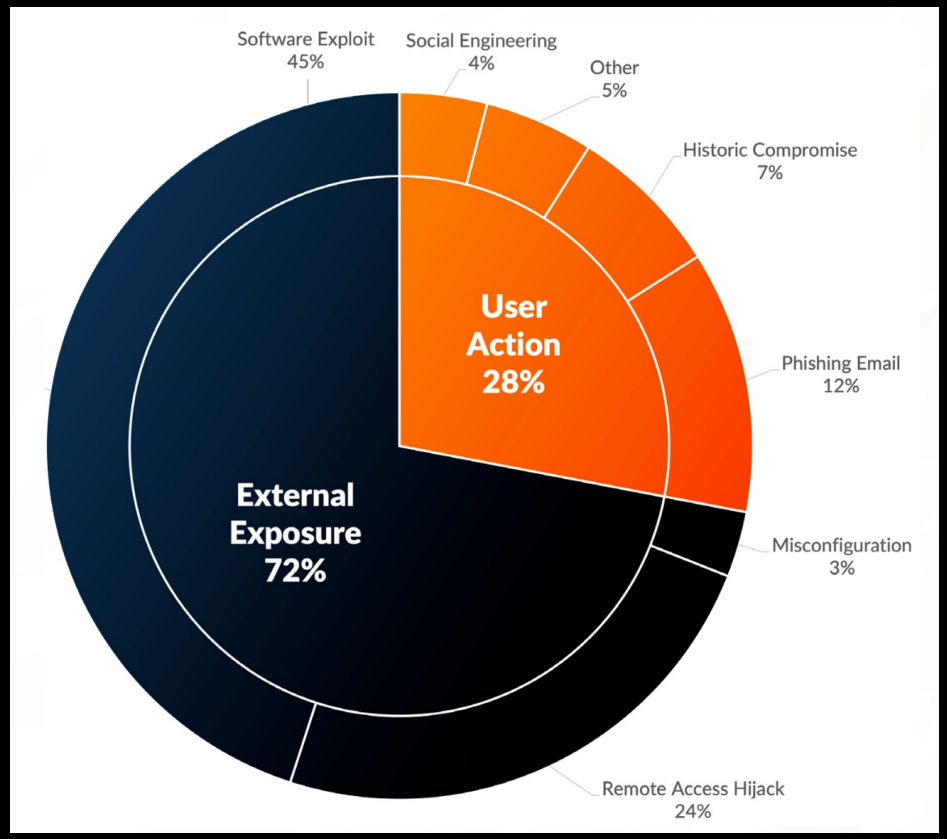
Zentralisierung aller Daten in der Arctic Wolf Plattform für: Speicherung, Anreicherung, Korrelierungen, Analysen und Untersuchungen

Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

Root Point of Compromise (Angriffsmethode)

External Exposure: Eine Bedrohung zielt auf ein System ab, das offen dem Internet ausgesetzt ist und verschafft sich Zugang zum Netzwerk oder zu den Daten des Opfers. Dies ist die einfachste Methode für Bedrohungsakteure und wird daher häufig eingesetzt.

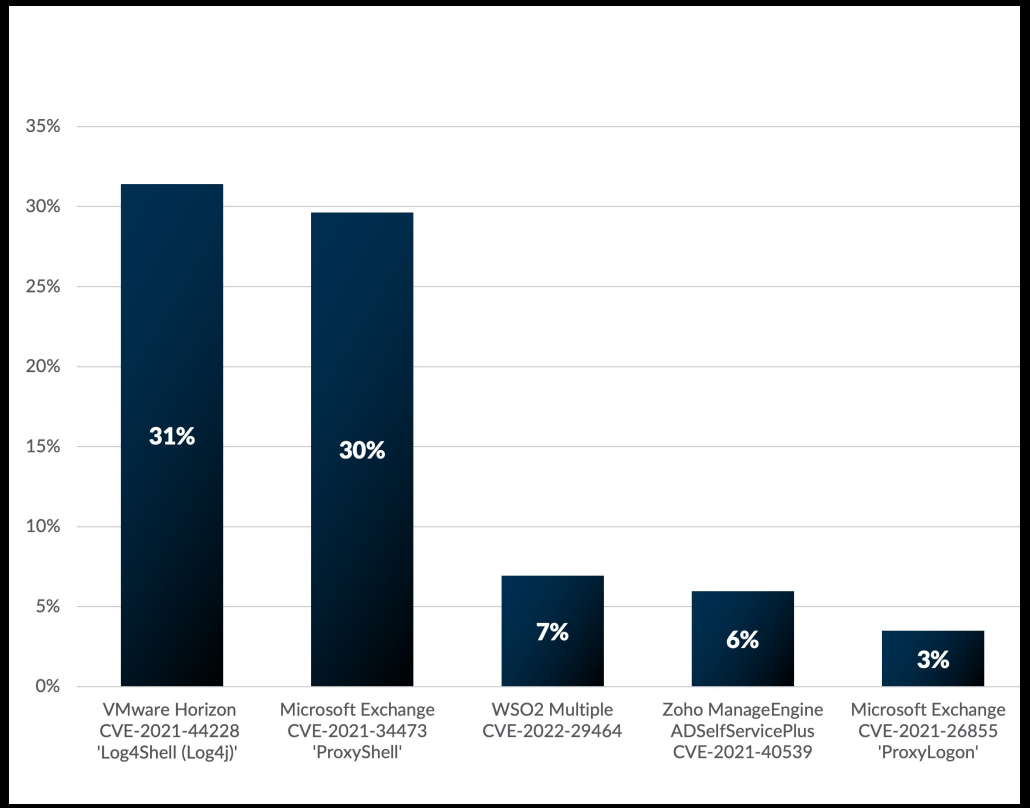
User Action: Die Angreifer müssen einen Benutzer dazu bringen, eine Aktion durchzuführen, damit der Angriff funktioniert. Z. B. das Öffnen einer bösartigen Website oder Datei.



Root Point of Compromise – External Exposure

Eine handvoll Schwachstellen sind für einen erheblichen Teil der gemeldeten Vorfälle verantwortlich:

- VMWare Horizon (Log4Shell / Log4j – CVE-2021-44228)
- Microsoft Exchange (ProxyShell – CVE-2021-34473)
- WSO2 Multiple (CVE-2022-29464)
- Zoho Managed Engine AD Self Service Plus (CVE-2021-40539)
- Microsoft Exchange (ProxyLogon – CVE-2021-26855)



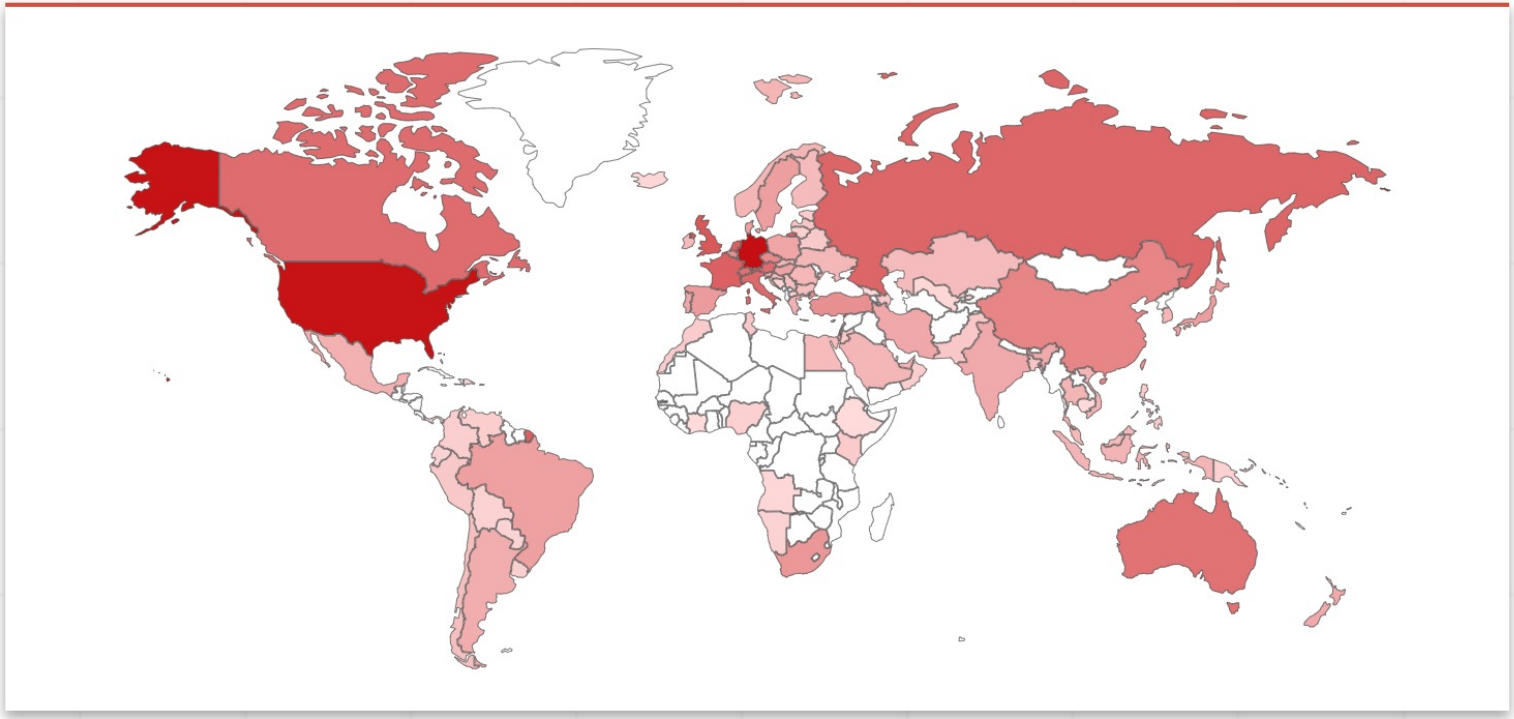
Wir sind immer noch Weltmeister

Shodan Report

`http.title:outlook exchange`

Total: 184,195

// GENERAL



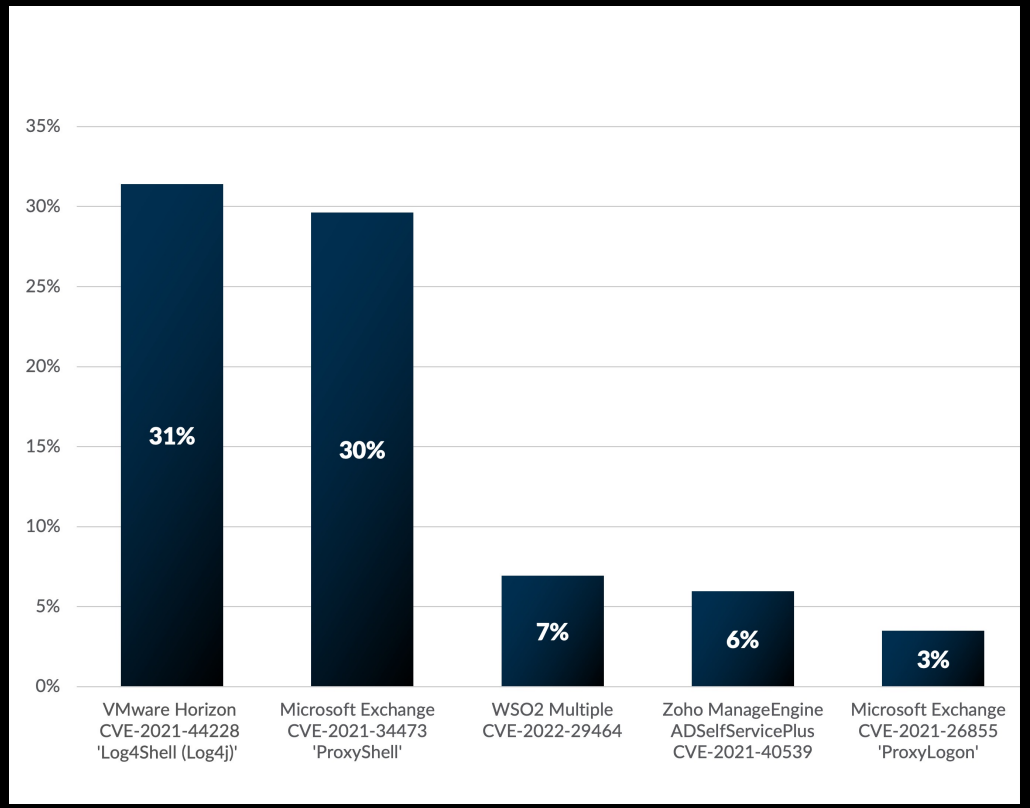
Countries

Germany	41,977
United States	39,930
United Kingdom	9,157
France	7,625
Netherlands	7,463

Root Point of Compromise – External Exposure

Eine handvoll Schwachstellen sind für einen erheblichen Teil der gemeldeten Vorfälle verantwortlich:

- VMWare Horizon (Log4Shell / Log4j – CVE-2021-44228)
- Microsoft Exchange (ProxyShell – CVE-2021-34473)
- WSO2 Multiple (CVE-2022-29464)
- Zoho Managed Engine AD Self Service Plus (CVE-2021-40539)
- Microsoft Exchange (ProxyLogon – CVE-2021-26855)



SHODAN | Explore | Downloads | Pricing | port:"3389" country:"DE" | Account

TOTAL RESULTS

171,792

TOP CITIES

Frankfurt am Main	54,662
Berlin	17,831
Düsseldorf	16,430
Nürnberg	12,594
Gunzenhausen	8,099

More...

TOP ORGANIZATIONS

Hetzner Online GmbH	28,797
Contabo GmbH	28,258
A100 ROW GmbH	15,080
1&1 IONOS SE	12,036
Deutsche Telekom AG	10,820

More...

TOP PRODUCTS

Remote Desktop Protocol	165,790
OpenSSH	135
VNC	3

View Report | Browse Images | View on Map

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

82.165.158.247

1&1 IONOS SE

Germany, Villingen-Schwenningen

self-signed

2023-01-25T08:40:28.927892

SSL Certificate

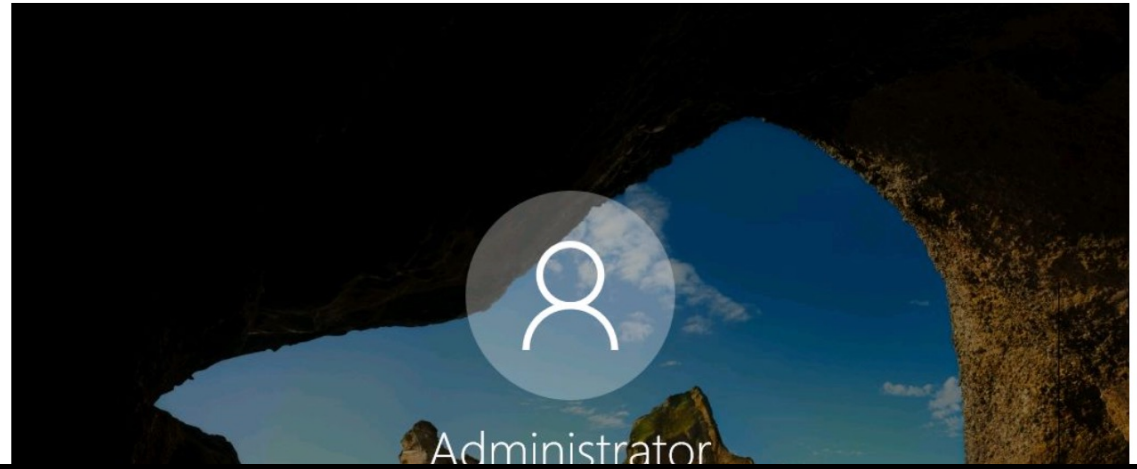
Issued By:
|- Common Name:
vm4F4FBBF

Issued To:
|- Common Name:
vm4F4FBBF

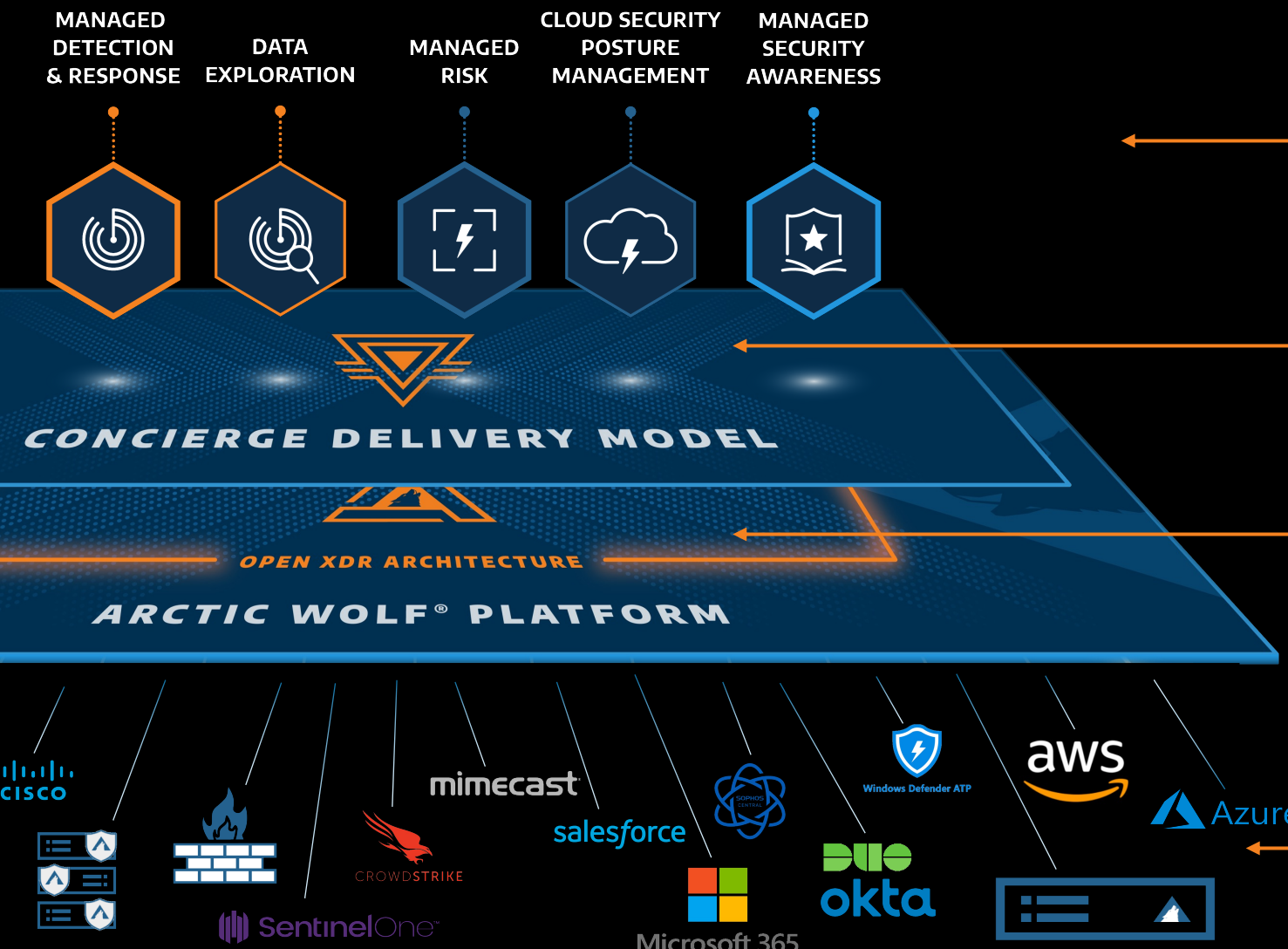
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server 2016
  OS Build: 10.0.14393
  Target Name: VM4F4FBBF
  NetBIOS Domain Name: VM4F4FBBF
  NetBIOS Computer Name: VM4F4FBBF
  DNS Domain Name: vm4F4FBBF
  FQDN: vm4F4FBBF

; Administrator
SES
R Administrator
R jprankl
R WDeployAdmin
```



SECURITY OPERATIONS CLOUD



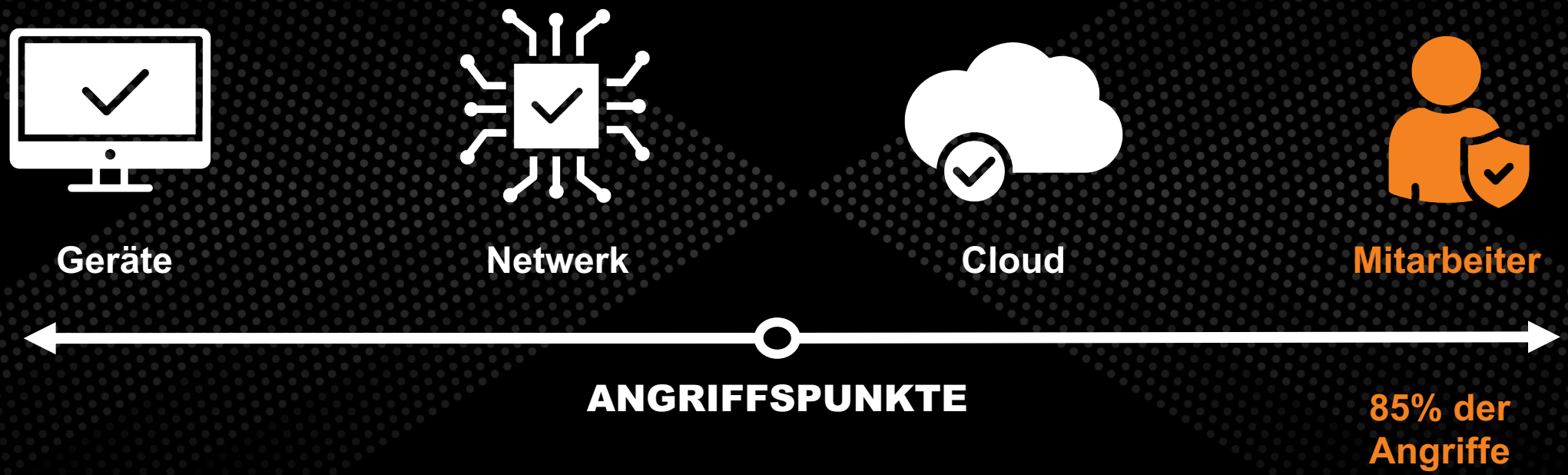
Wir stellen Services für das gesamte **Security Operations Modell** zur Verfügung

Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

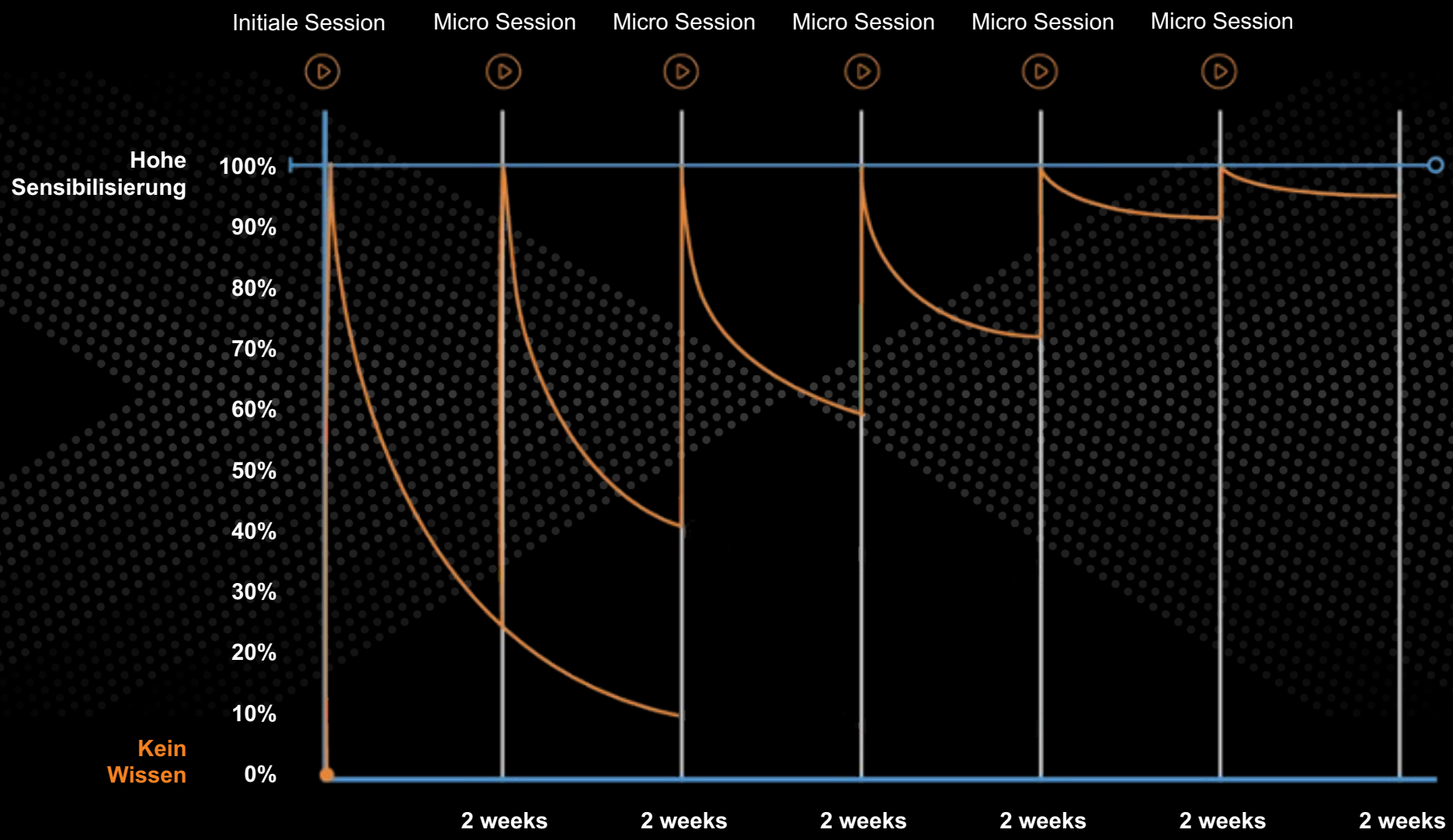
Zentralisierung aller Daten in der Arctic Wolf Plattform für: Speicherung, Anreicherung, Korrelierungen, Analysen und Untersuchungen

Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

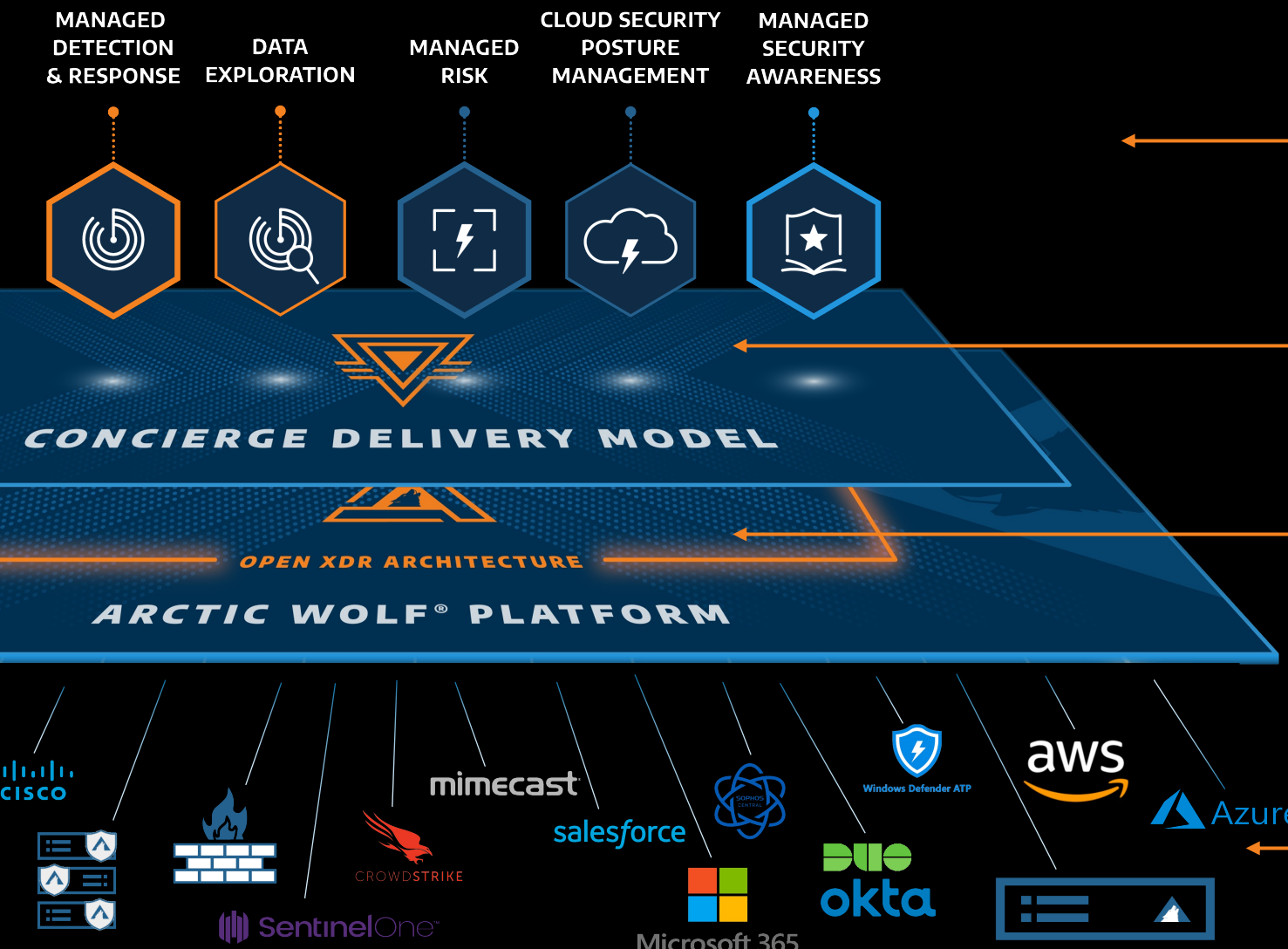
Der Faktor Mensch



Kontinuierliches Training ist notwendig



SECURITY OPERATIONS CLOUD



Wir stellen Services für das gesamte **Security Operations Modell** zur Verfügung

Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

Zentralisierung aller Daten in der Arctic Wolf Plattform für: Speicherung, Anreicherung, Korrelierungen, Analysen und Untersuchungen

Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

THE LEADER IN SECURITY OPERATIONS

Security Operations

Angestrebtes Sicherheitslevel

Arctic Wolf Security Operations

Lücke

Die meisten Firmen stehen hier

WIEDERSTANDS-FÄHIGKEIT

Proaktiv

Konform (ISO etc)

Versicherbar

ARCTIC WOLF

ERWEITERTE VERTEIDIGUNG

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

BASIS

Passwörter / AD

Patch Management

Backups

Warum Arctic Wolf?

Einfach, weil einfach einfach einfach ist!

- Keine zusätzlichen Fachkräfte (Security-Experten) werden benötigt
- **DSGVO**-konform, 24x7x365 aus Deutschland von deutschen Experten
- Breiteste Visibilität – **Herstellerunabhänige** Auswertung der relevanten Logs
  AD, DNS, DHCP, Firewall, Endgeräte, IDS für Internet-Traffic und Cloud-Komponenten (IaaS, SaaS)
  DarkWeb Scanning & External Vulnerability Assesments
- Schnelle Implementierung – Time-To-Value
- **Concierge Security Team** : Zugriff auf zwei Security-Consultants, die Ihnen strategisch zur Seite stehen und den Service auf Ihre Bedürfnisse anpassen
- **Schwarmintelligenz** von >5300 Kunden
- Industrieführenden SLO von <30 Minuten für Identifikation, Analyse und detaillierte Lösungsbeschreibung
- **Flatrate** - Einfaches, verständliches und planbares Preismodel