

FREICON.



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

[illegible]

Warum KI den Markt verändert

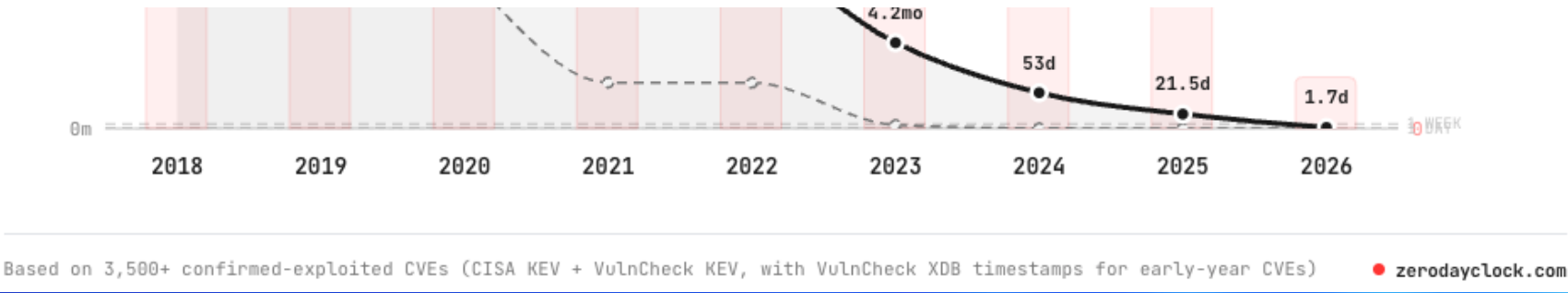
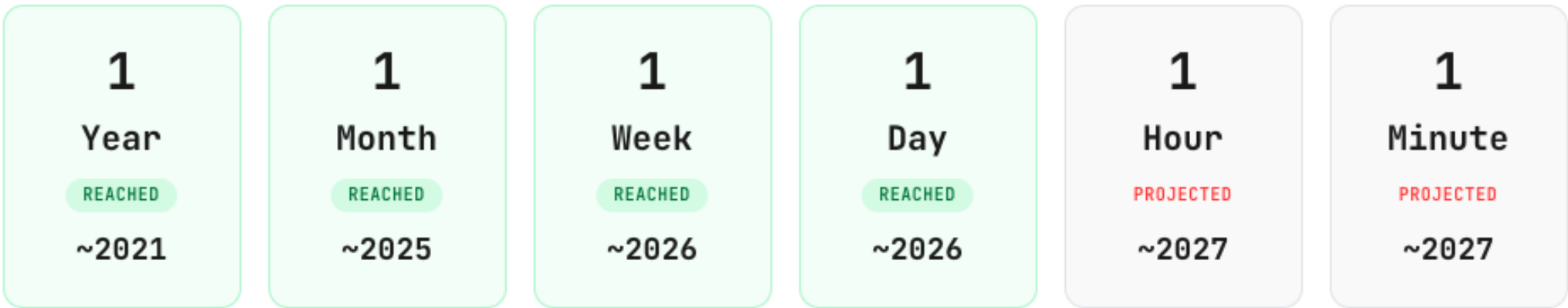
From Vulnerability to Exploitation

TTE measures the gap between CVE public disclosure and first confirmed in-the-wild exploitation. Zero = same-day.

— Mean TTE (10% trimmed, days) --- Median TTE (days) ■ Weaponized Exploits (count)

Time-to-Exploit Milestones

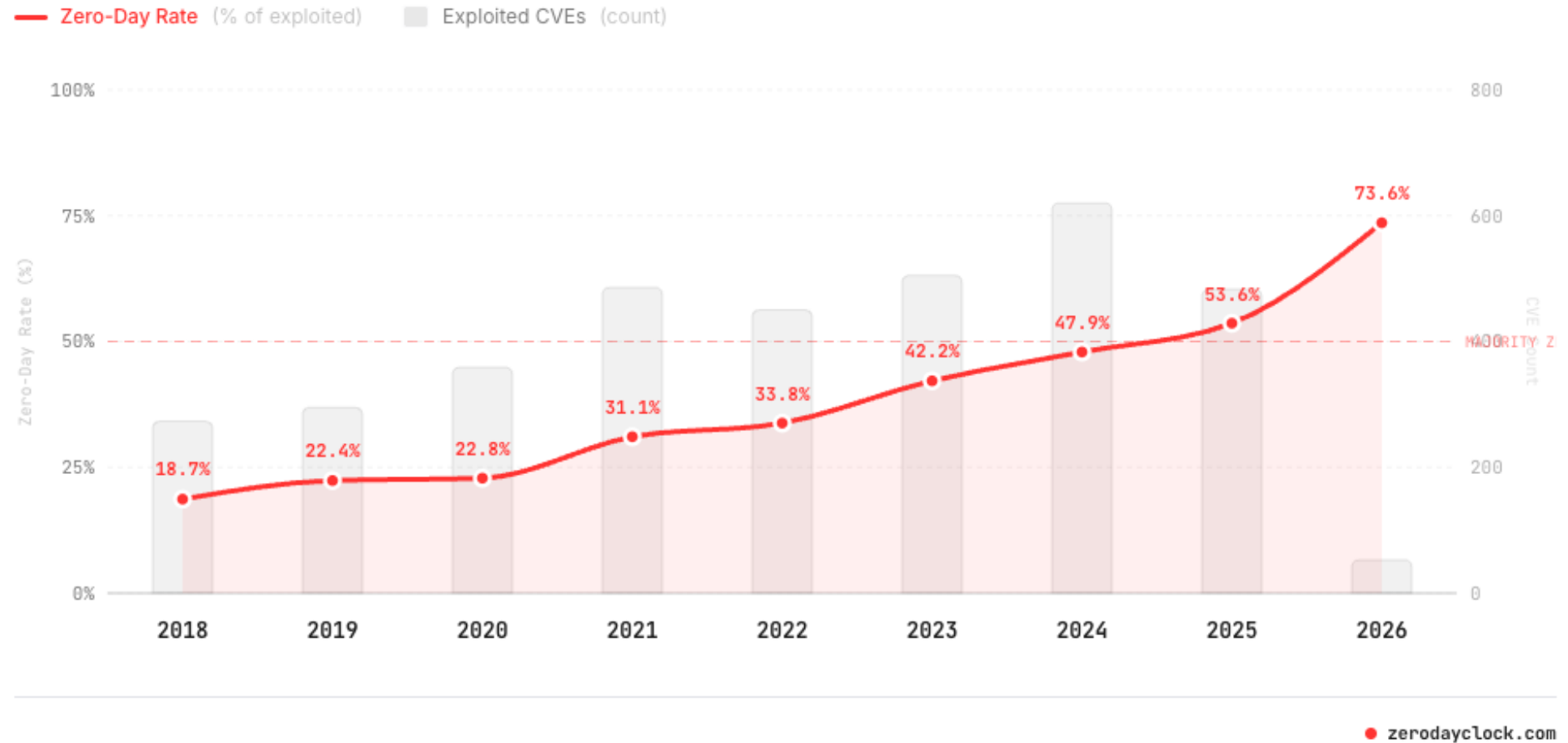
Projected year when median TTE crosses each threshold — extrapolated from observed 2018–2024 trend



Warum KI den Markt verändert

Zero-Day Rate

Percentage of exploited CVEs where exploitation occurred before or on the day of disclosure (TTE ≤ 0)





MISSION:

End Cyber Risk



Arctic Wolf Security Operations

We Make Security Work

12000+

Kunden

24x7

In deutsch

1000+

Security Engineers

5

Datacenter weltweit

5.1+

Milliarden Logzeilen pro Tag

3.5M+

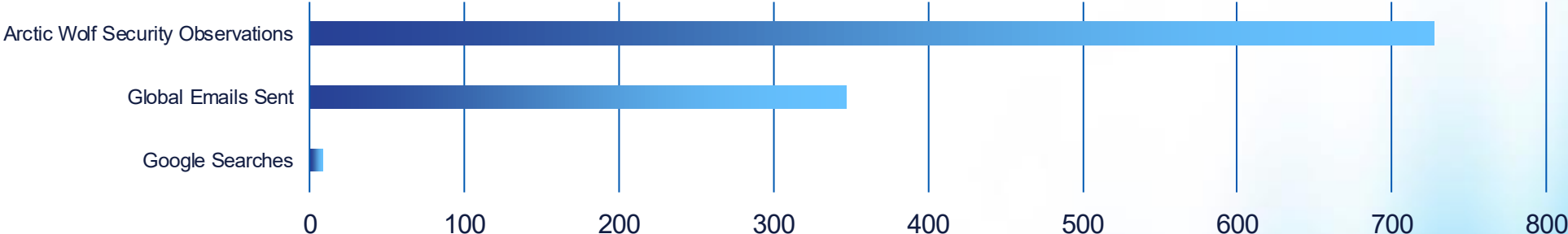
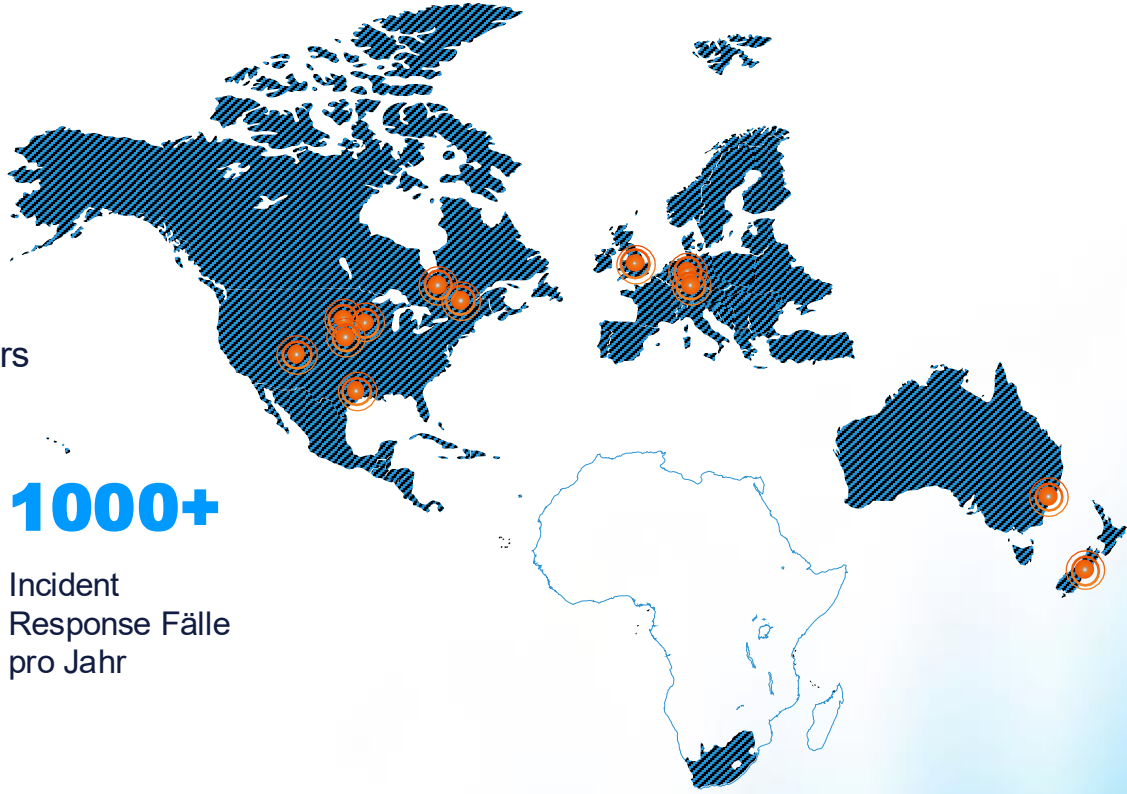
aktive Agenten and 25,000+ Sensoren

12M+

Schwachstellen werden pro Woche identifiziert

1000+

Incident Response Fälle pro Jahr



Arctic Wolf Security Operations

We Make Security Work

12000+

Kunden

24x7

In deutsch

1000+

Security Engineers

5

Datacenter weltweit

5.1+

Milliarden Logzeilen pro Tag

3.5M+

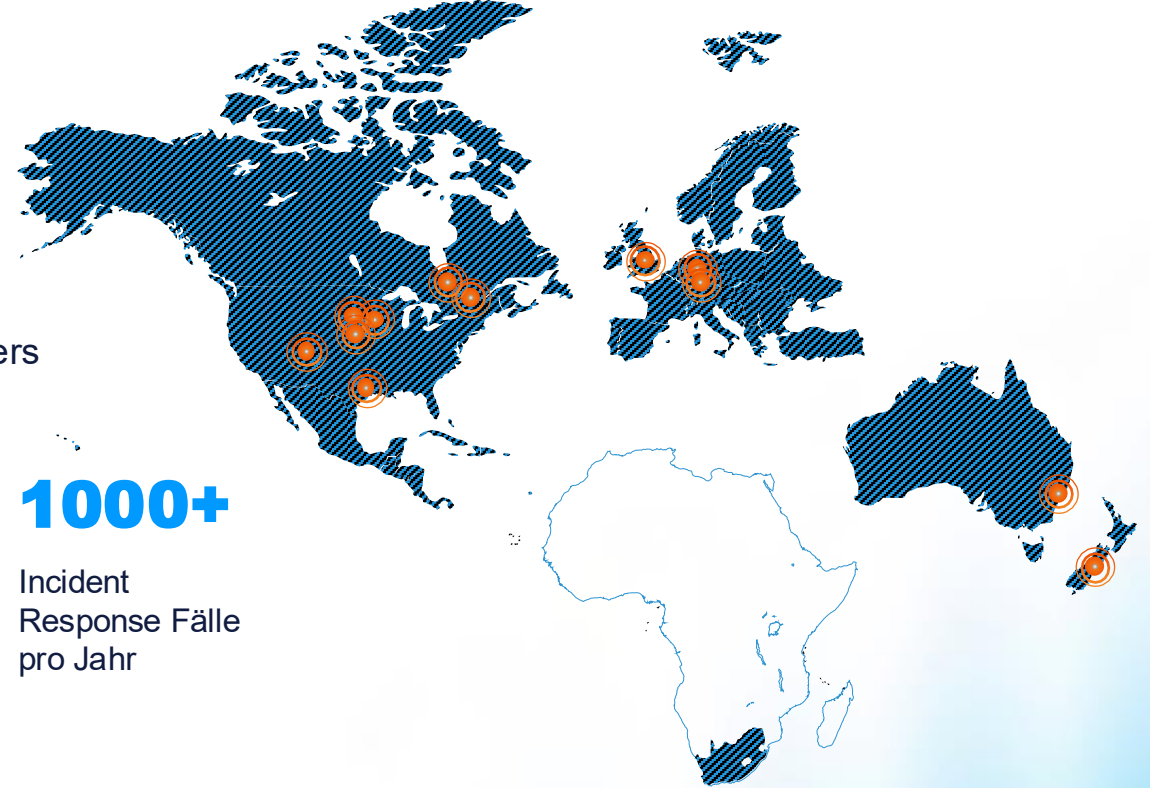
aktive Agenten and 25,000+ Sensoren

12M+

Schwachstellen werden pro Woche identifiziert

1000+

Incident Response Fälle pro Jahr



Arctic Wolf Security Operation Teams

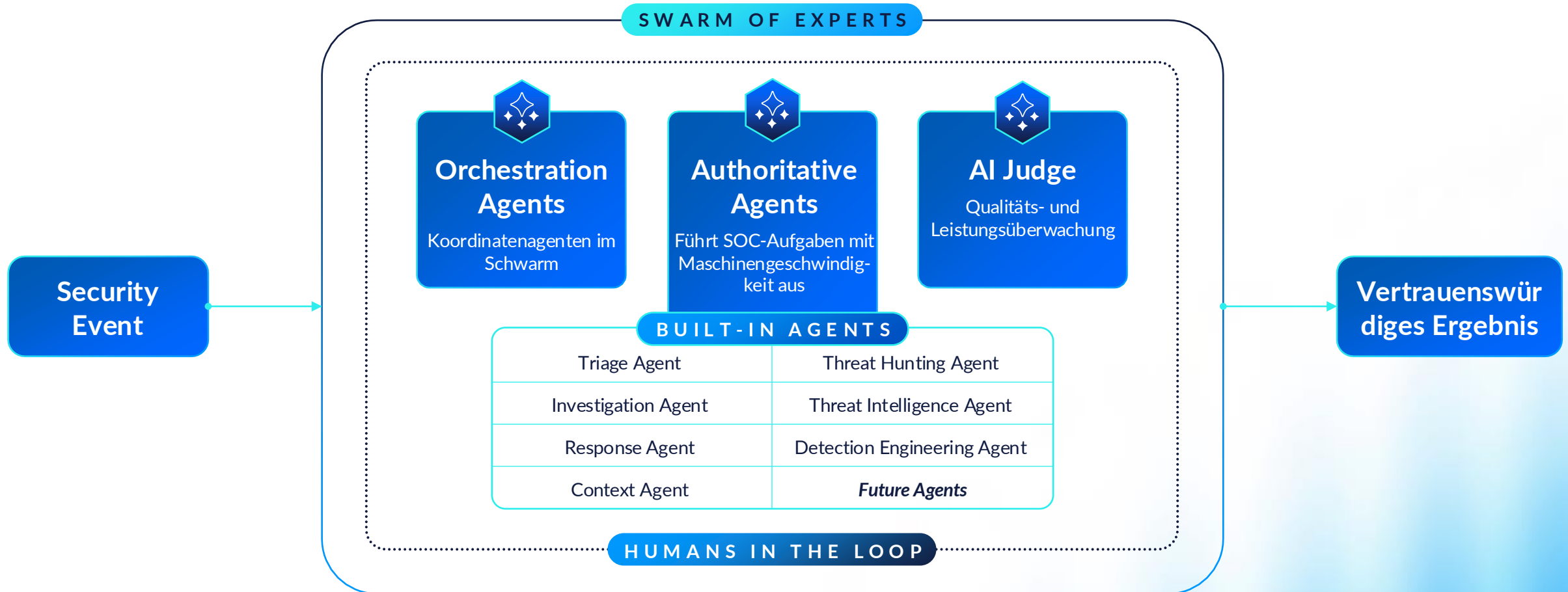
Das Triage Security Team überwacht ihre Umgebung 24x7 um Angriffe zu identifizieren und Sie bei der Behebung unterstützen



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



The Agentic Future is Already Here



15X SCHNELLERE FALL
LÖSUNG

3X BESSERE
TICKETQUALITÄT

12X ROI vs. DIY AI



Beispiel Integrationen mit Erkennungen

Mehr Integrationen verfügbar



Externe
Risiken
5%



Identität
20%



SaaS
15%



IaaS
10%



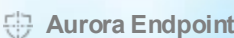
Firewall
5%



Network
30%



Endpoint
15%



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



Meet the Arctic Wolf SecOps Teams

Die zentrale Basis für alle unsere Kundenorientierten Security Services (S2)



Triage Team

- 24/7 SOC Operations:
 - Investigation, Analyse, Ticketing, Kommunikation
 - Einteilung (Triaging) False/True Positive im Kundenkontext
 - Active Response
- Angeleitete Incident Behebung
- Notfallkontakt für Kunden
- Lokale Serviceerbringung, DE-Frankfurt/Main:
 - 24/7 L1-L3, 4-Schicht, no Follow-the-Sun
 - 24/7 Deutschsprachiger Support



Concierge Team

- Dediziertes, persönliches Concierge Security Team (CST) für jeden Kunden
 - Breite & tiefgehende Security Expertise, Hersteller-unabhängig
 - 5-15 Jahre Erfahrung pro CST Teammitglied
- Guided Security Journey
 - Regelmäßige Security Posture in-Depth Reviews (SPIdR)
 - Minimierung des Kundenrisikos/-exposure
 - Ticket Root Cause Analyse
- Service Management
- Strategische Anleitungen



AW Labs

- Global Threat Intelligence Organisation
 - IoC/IoA Maintenance
 - Detection Rule Set
 - Vulnerability / Risk Guidance
- Active Threat Hunting, Security Research
- Security Posture Engineering
- Ingestion, Detection, Response (IDR) Modelling
- AI Oversight + Data Science
- Kunden Briefing + Schulungen



AI

Artificial Intelligence

+

HI

Human Intelligence

=

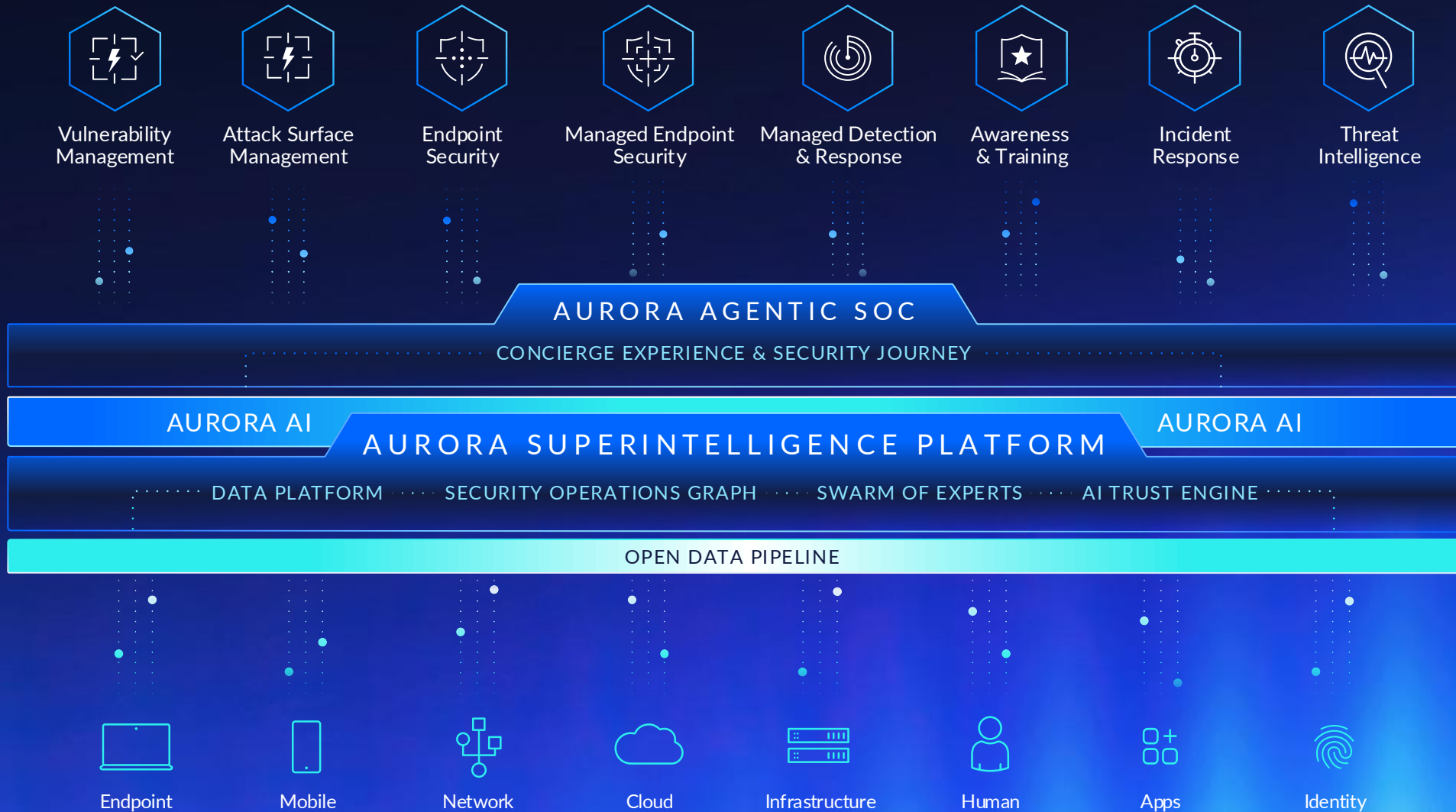
Superintelligence

Holistic Visibility Unlocks Security Operations

The Agentic Power of the Aurora® Superintelligence Platform



Die Arctic Wolf Aurora Superintelligence Platform



Arctic Wolf SOC as a Service

Arctic Wolf ist mehr als Managed Detection & Response

- 24x7x365 aus Deutschland von deutschen Experten
- Alle Logs werden DSGVO-konform gespeichert
- Breitesten Visibilität – Herstellerunabhängige 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



END CYBER RISK

