



ISEC7

Ihre Sicherheit Unser Business

Jan Jacobsen | Senior Sales Engineer

Juli 2025

END
CYBER
RISK

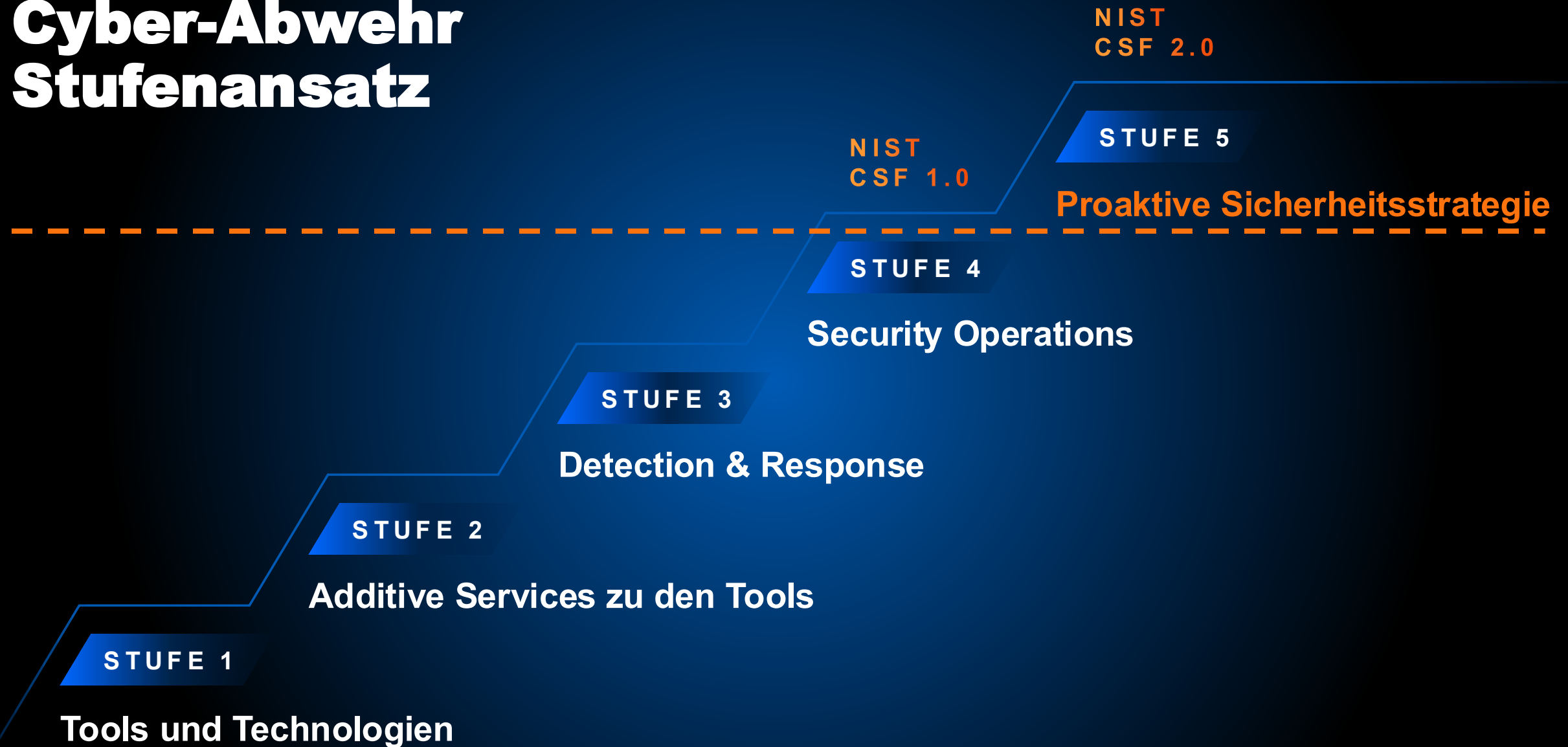
Die Nr. 1 Herausforderung unserer Kunden



Security Operations Partnerschaft



Cyber-Abwehr Stufenansatz



Wir sind Arctic Wolf

DIE MISSION: **END CYBER RISK**

10.000+

Kunden

1.000+

Security
Engineers

8+

Billionen Events
pro Woche

600+

Incident Response
Fälle pro Jahr

100+

Länder

2.000+

Partner
weltweit



VERTRAUENSWÜRDIG



2X LEADER

MDR MarketScape

Gartner

Peer Insights™

MOST RECOMMENDED

MDR, Vulnerability Assessment,
and Security Awareness

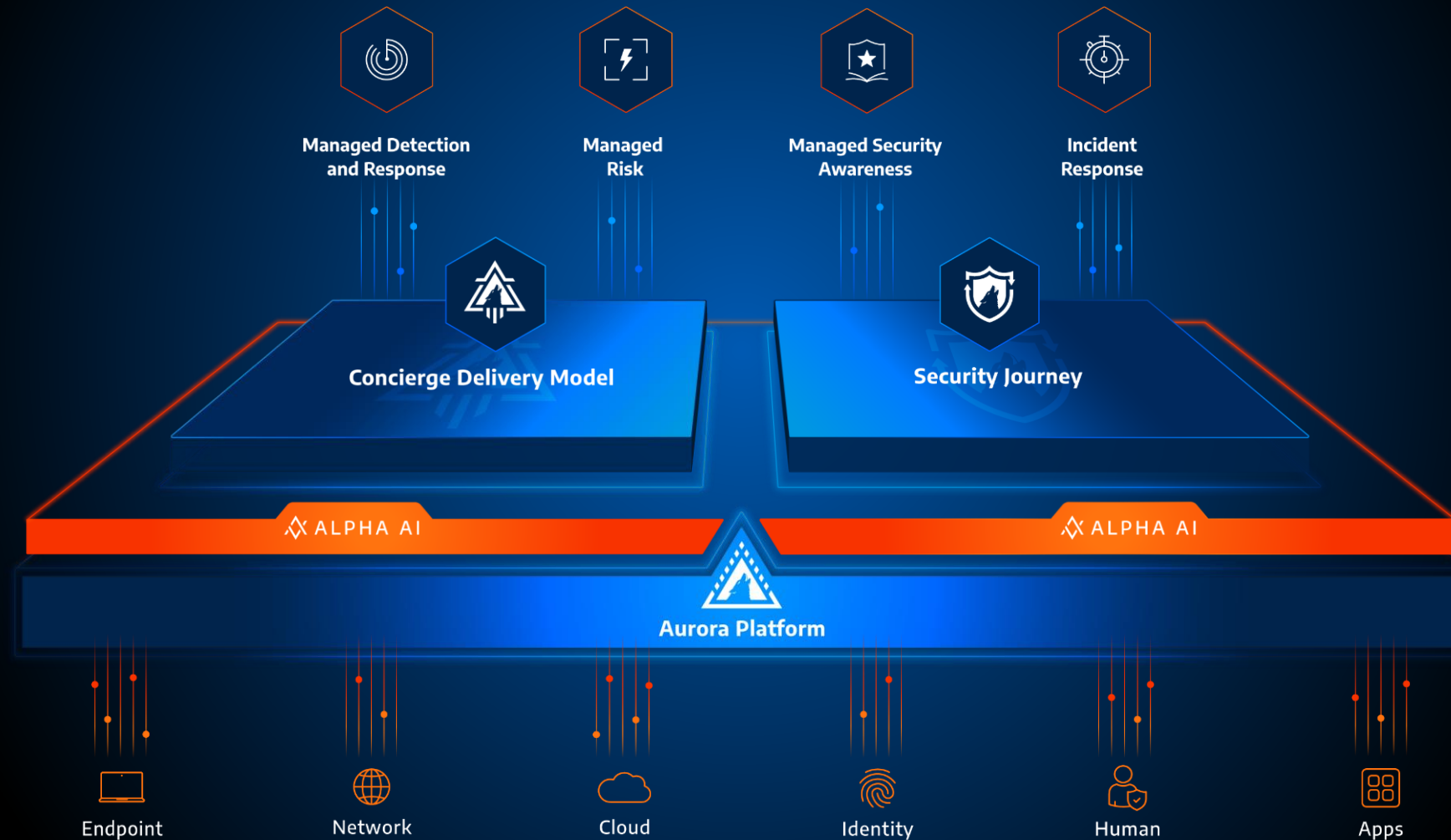


MISSION:

End Cyber Risk



Arctic Wolf Security Operations Cloud





Remote



Server



Microsoft 365



Computer



Firewalls



Microsoft Defender



CROWDSTRIKE

8



Arctic Wolf Security Operations Cloud



Sensoren



DARK WEB



External Vuln Scans





SOC Triage Security Team

The Pack Has Your Back!

SOC-Leistungen



24x7 MONITORING

Ihre Umgebung wird rund um die Uhr von Sicherheitsexperten auf Bedrohungen und Risiken überwacht



REAL-TIME ACTIVE RESPONSE

Rasche Eindämmung von Vorfällen und Fehlerbehebung



GEMELDETE TICKETS

Vorfilterung der Tickets durch Security-Engineers und Weiterleitung nur von True-Positives



UNTERSTÜTZENDE MASSNAHMEN

Unterstützung bei Schritten, die über die Active Response Maßnahmen hinausgehen



FAKTOR MENSCH

Direkter Kontakt zu Mitarbeitern, wenn Sie Fragen zu Ihrer Umgebung haben oder Unterstützung benötigen

REAKTIONSZEIT



INBOUND
5 Minuten



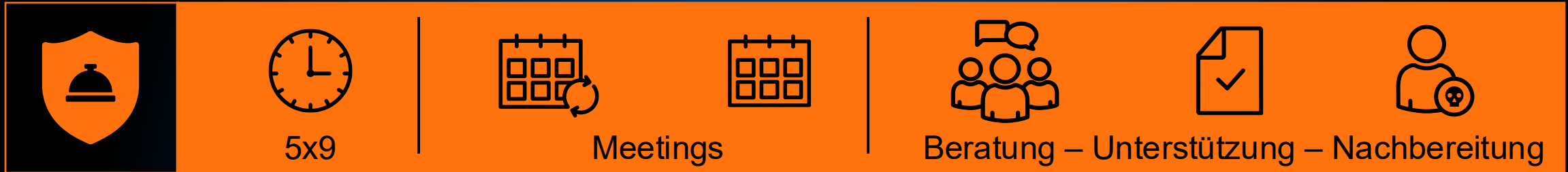
OUTBOUND
30 Minuten



Concierge Security Team



Dedizierte Strategie-Berater, die helfen, den Security-Reifegrad zu erhöhen.



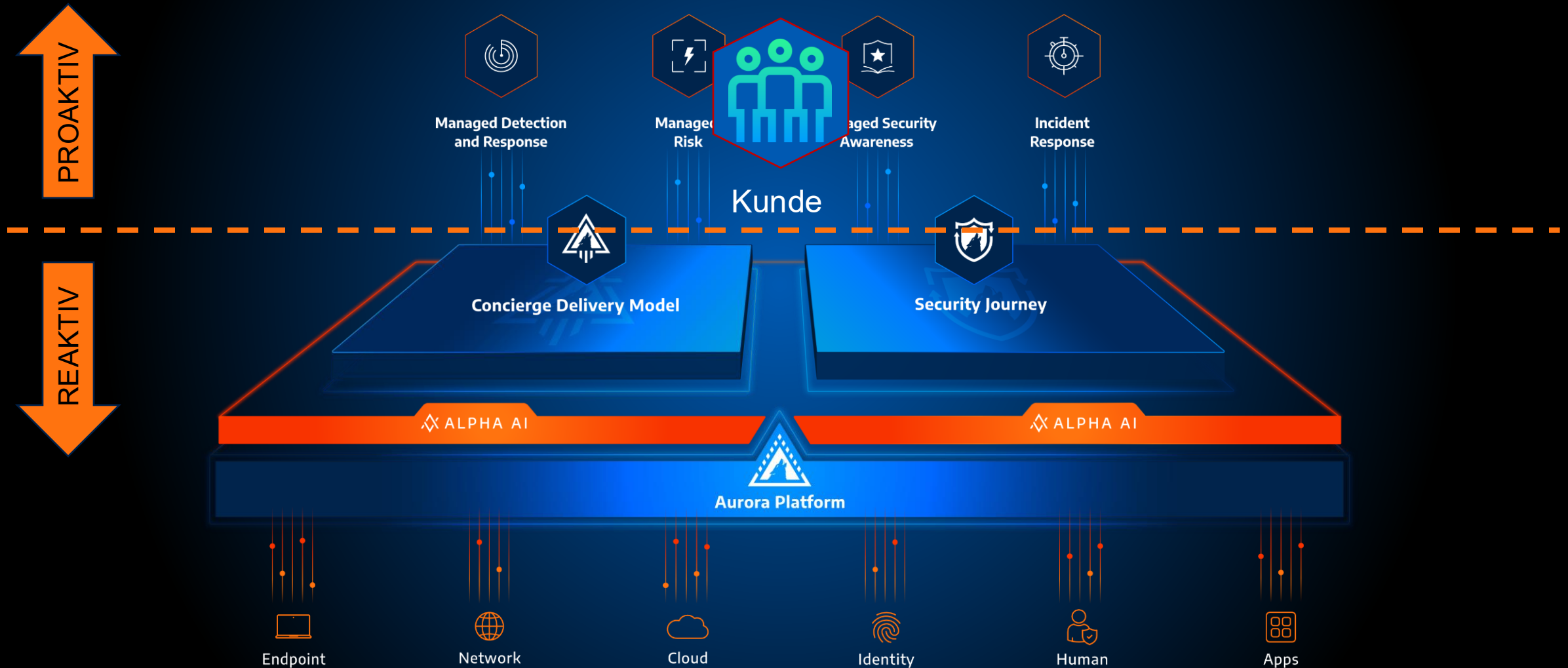
Einige SPiDR Beispiele

Arctic Wolfs proaktive Security Journey

- 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



Ihre IT-Security Abteilung as a Service



Hohe Transparenz dank offener Plattform

Ermittlungen aufgrund eines ersten Indikators eingeleitet



Plattform-Schwarmintelligenz



AI & Data Science



Threat Intelligence &
Security Research



Detection &
Response
Engineering



Security Posture
Engineering

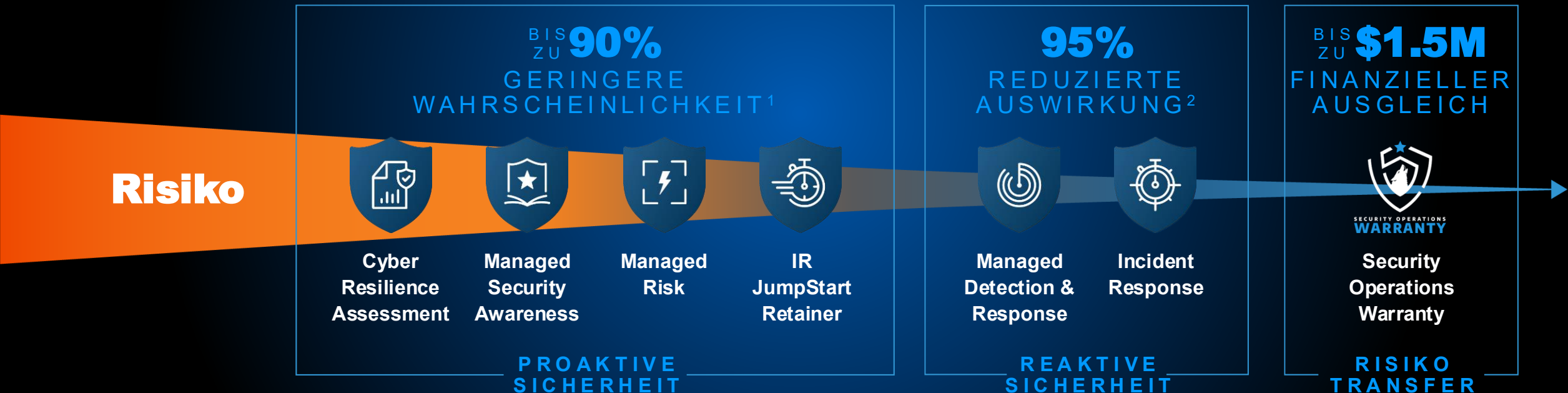
KUNDE 1

KUNDE 2

SCHWARMINTELLIGENZ 10.000+ KUNDEN



Kombinierte Lösungen zur Risikominderung



¹ Arctic Wolf Labs. 2023

² How Sec.Ops Reducing Risk of Cyber Incident by 95%



Arctic Wolf und Cyberversicherungen

Optimieren Sie ihre Versicherungsprämien

Die Mehrheit der befragten IT-Führungskräfte gab an, dass die Versicherungsprämien nach der Implementierung von Sicherheitslösungen von Arctic Wolf **zwischen 10% und 30%** gesunken sind.¹

¹Prämieneinsparungen basierend auf Kunden, die Managed Detection and Response, Managed Risk, Managed Awareness und den Incident Response JumpStart Retainer haben

I. Umfrage der CyberRisk Alliance
II. 500+ Befragte
III. Profile: IT Entscheider; 100-5,000 Beschäftigte;

IM SCHNITT
20%
SPAREN



Arctic Wolf Security Operations Cloud 2.0



Security Journey – Stärkung der Cyber-Resilienz

Phase 1

Setup & Installation

- Agenten ausrollen
- Sensoren installieren
- Einweisung Portal
- Logquellen anbinden

Phase 2

Go-Live

- Vorstellung Concierge Team
- Kennenlernen/Business Prozesse verstehen
- Customizing/Baselining
- **Cyber Resilience Assessment**

Phase 3

Regelbetrieb

- Regelmäßige Termine/Reviews
- Angepasst an den Kunden
- Bewertung von Lücken/Risiken
- Best Practice Empfehlungen
- Konfigurations Checks

Onboarding

Customizing

Review / SPiDR

Onboarding Team &
ISEC7

Concierge Team &
ISEC7

Concierge Team &
ISEC7

ca. 3-4 Tage*

Zeitraum ca. 30 Tage

45-60 Min. pro Meeting

Zeitraum ca. 45 Tage

30-60 Min. pro Meeting

4/12/18 Termine pro Jahr



Arctic Wolf Scoping & Lizenzierung



Benutzer

Mitarbeiter und SaaS Nutzer



Server

physisch + virtuell



Sensoren

Einer für jeden Internetbreakout



Arctic Wolf Security Bundles

 SECURITY OPERATIONS CORE	 SECURITY OPERATIONS PLUS	 SECURITY OPERATIONS TOTAL
Managed Detection and Response	Managed Detection and Response	Managed Detection and Response
Security Journey	Security Journey	Security Journey
Concierge Security Team	Concierge Security Team	Concierge Security Team
Active Response	Active Response	Active Response
Data Explorer Lite	Data Explorer Lite	Data Explorer Lite
90 Tage Log Retention	90 Tage Log Retention	90 Tage Log Retention
Security Operations Warranty \$100k bei 3-Jahres Vertrag	Managed Risk	Managed Risk
	Security Operations Warranty \$500K bei 1-Jahres Vertrag \$1M bei 3-Jahres Vertrag	Managed Security Awareness
		Incident Response JumpStart Retainer
		Security Operations Warranty \$750K bei 1-Jahres Vertrag \$1.5M bei 3-Jahres Vertrag



Optionen des Concierge Security Teams

Bestandteil aller Arctic Wolf Bundles



SILBER

Benanntes Sicherheitsteam

24x7x365 SOC-Unterstützung

Nachverfolgung von
Eskalationen

Unterstützung bei der
Berichterstattung

4 geplante proaktive
Sicherheits-Kontaktpunkte

Überprüfung des
Sicherheitsniveaus & SPiDRs
aus Silber-Library



GOLD

Benanntes Sicherheitsteam

24x7x365 SOC-Unterstützung

Nachverfolgung von
Eskalationen

Unterstützung bei der
Berichterstattung

12 geplante proaktive
Sicherheits-Kontaktpunkte

Überprüfung des
Sicherheitsniveaus &
SPiDRs aus Gold-Library



PLATINUM

Benanntes Sicherheitsteam

24x7x365 SOC-Unterstützung

Nachverfolgung von
Eskalationen

Unterstützung bei der
Berichterstattung

18 geplante proaktive
Sicherheits-Kontaktpunkte

Überprüfung des
Sicherheitsniveaus & SPiDRs
aus Gold-Library



Erfolgreich geschützt durch Arctic Wolf



Was Arctic Wolf als SOC-Partner auszeichnet

Arctic Wolf Networks (AWN) bietet Ihnen einen **7x24** fully managed **Security Operations Center** (SOC) Service.

AWNs Mehrwerte sind die **Herstellerunabhängigkeit**, die **schnelle Umsetzung**, und das **einfache, transparente und planbare Preismodell**. Die **Serviceerbringung erfolgt aus Deutschland in Deutscher Sprache** (wahlweise auch auf Englisch).

Dank des Netzwerks von 7.000 Kunden weltweit, ist die Threat Intelligence der Arctic Wolf häufig schneller als die der betroffenen Hersteller.

Ein **Alleinstellungsmerkmal** stellt dabei die **Security Journey** auf Basis des **Concierge Modells** dar, welches Ihrem IT-Team weitreichende Unterstützung bietet, Ihre Security-Architektur fortwährend verbessert und gemeinsam mit Ihnen eine proaktive Security-Strategie umsetzt.

Damit löst Arctic Wolf gleich zwei Probleme: Die **Verbesserung der IT-Security** und den **Mangel an Ressourcen** (Zeit, Geld, Personal, Know-How).

01

Der Faktor Geld

- ✓ Risikoreduktion um mindestens 95%
- ✓ Einfache, planbare & transparente Lizenzierung ohne versteckte Kosten
- ✓ Investitionsschutz vorhandener Security-Tools
- ✓ Bis zu 1,5 Mio USD Garantiezahlung
- ✓ Bis zu 30% Reduzierung Ihrer Cyberversicherungsprämien

02

Der Faktor Mensch

- ✓ Fully managed SOC-Service (Kein rein reaktiver MDR-Service)
- ✓ Feste Ansprechpartner für Sie und Ihr IT-Team (AWN Concierge)
- ✓ Regelmäßige IT-Sicherheitsberatung (individuell für Ihr Unternehmen)
- ✓ Unabhängige technologische Beratung ohne Verkaufsabsicht

03

Der Faktor Zeit

- ✓ Entlastung Ihres IT Teams (1 Ticket pro Tag im Schnitt / True Positive)
- ✓ Reaktionszeit des SOC <30 Minuten (Identifikation, Analyse, Lösungsansatz)
- ✓ 7x24 Angriffserkennung und Reaktion
- ✓ Onboarding innerhalb von 30 Tagen (ca. 4 PT Aufwand auf Kundenseite)

TEAM PLZ 2



Markus Klose

Account Executive, Arctic Wolf
+49 160 4978942
Markus.Klose@arcticwolf.com



Jan Jacobsen

Senior Sales Engineer, Arctic Wolf
+49 151 5908 1982
Jan.Jacobsen@arcticwolf.com





**We make
security work.**