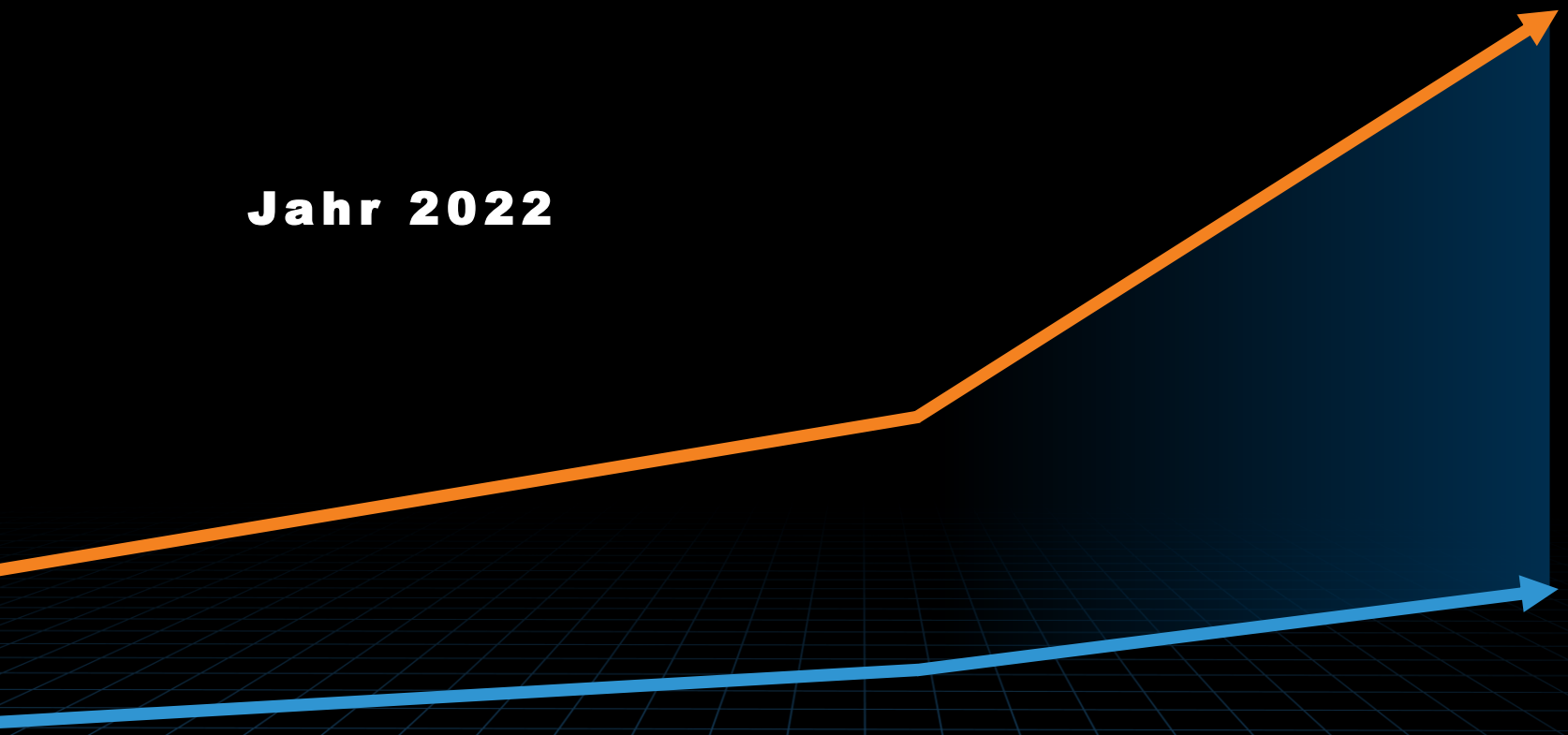
Jetzt endlich in Österreich – SOC-as-a-Service für SMB

Pierre Flammer, Director Sales Engineering DACH

Stetig seigendes Risiko



48%

Anstieg

der Schäden durch Cyberattacke

Security Firmen:

3,377+

Umsatz:

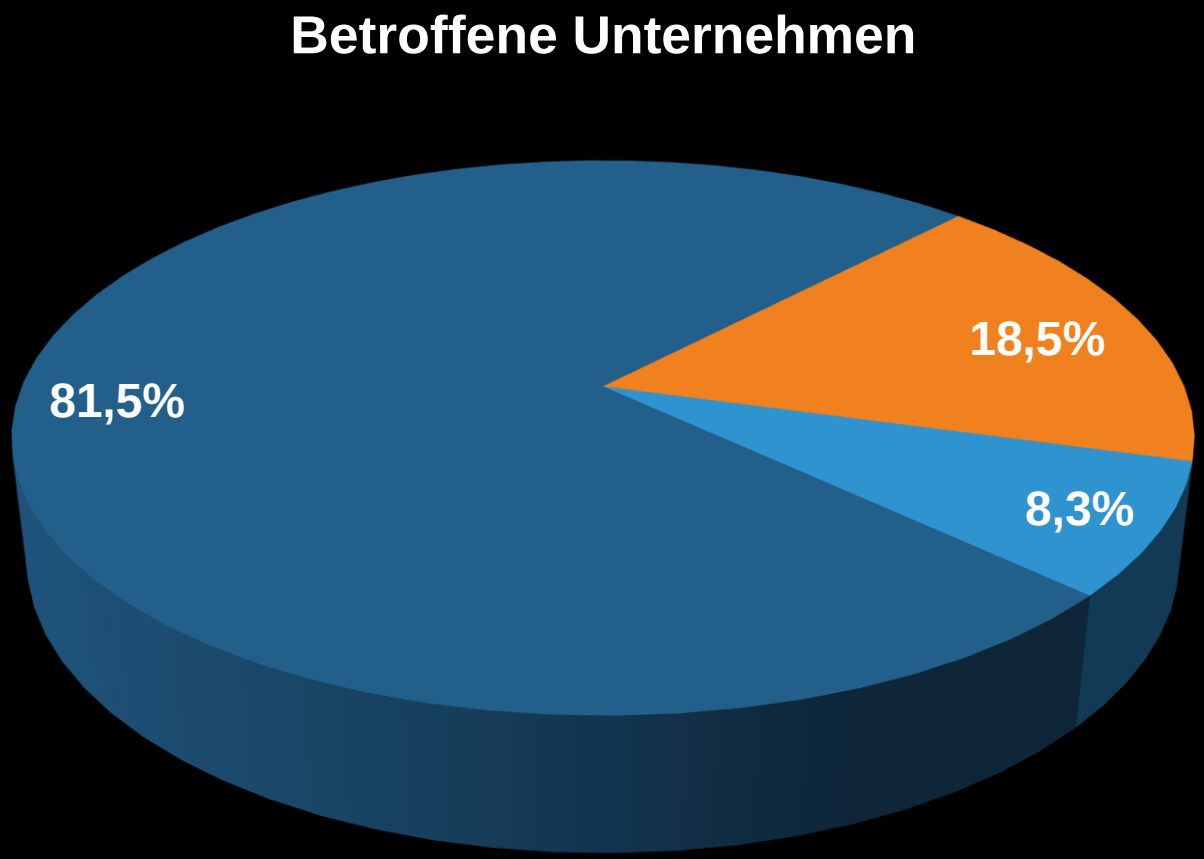
169B

Jährlicher Anstieg:

11%

Sources: IC3, Gartner, It-Harvest

Ich bin doch uninteressant…



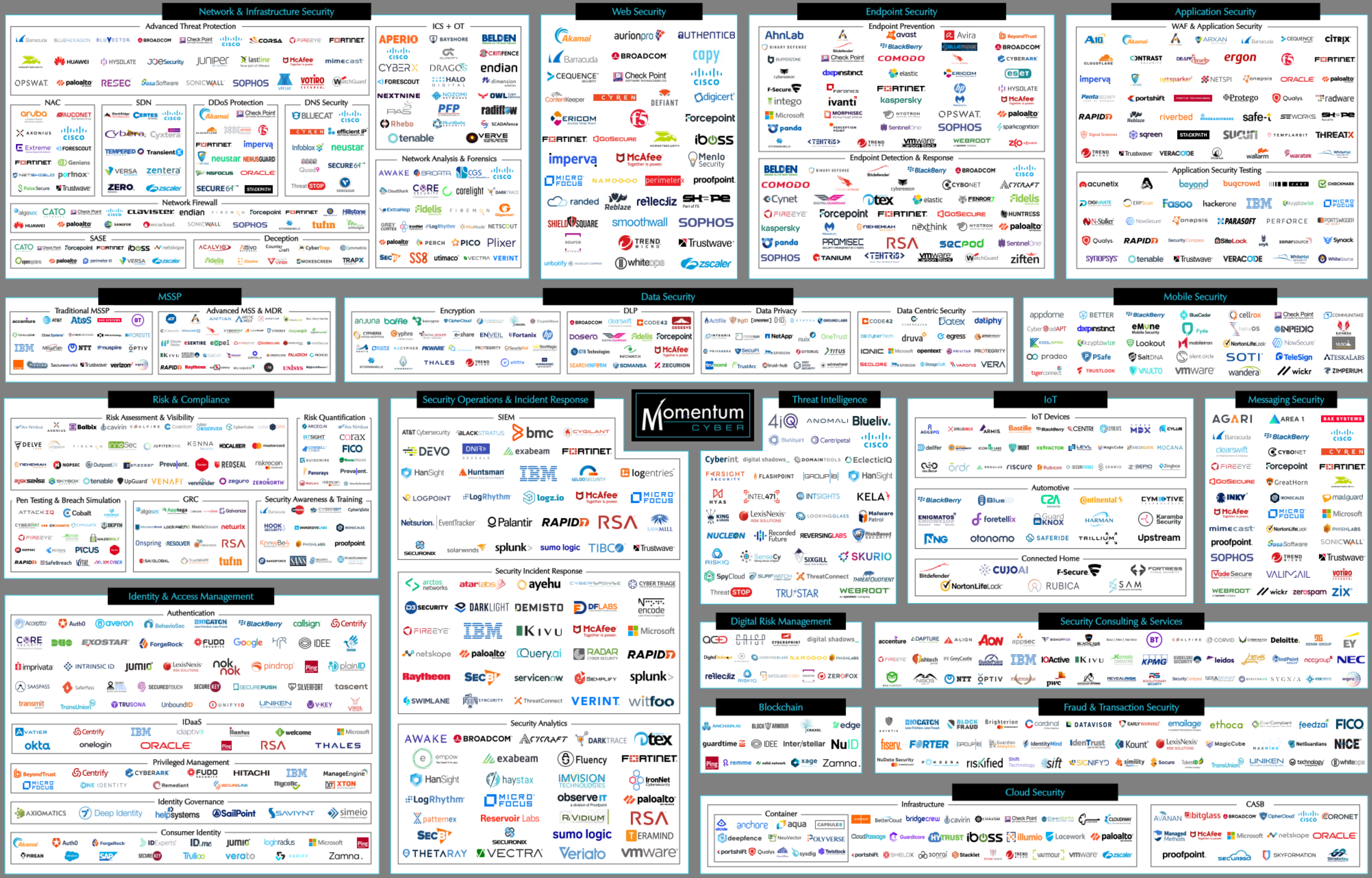
Sie haben aktuell 3 Möglichkeiten

1. Sie tun nichts und vertrauen auf die Tools (Die Frage ist dann nicht ob, sondern nur wann ein Angriff Erfolg hat)

2. Sie betreiben 24x7 Überwachung selber. (Kostenintensiv, SIEM, Fachkräfte etc.)

CYBER SCAPE 2021

ATIONS



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

Sie haben aktuell 3 Möglichkeiten

1. Sie tun nichts und vertrauen auf die Tools (Die Frage ist dann nicht ob, sondern nur wann ein Angriff Erfolg hat)

2. Sie betreiben 24x7 Überwachung selber. (Kostenintensiv, SIEM, Fachkräfte etc.)

3. Sie beauftragen ein MDR Service

Überwachung wird ausgelagert

Arctic Wolf Security Operations

Marktführer im Bereich MDR

5.400+
Kunden

24x7
in deutsch

570+
Security Engineers

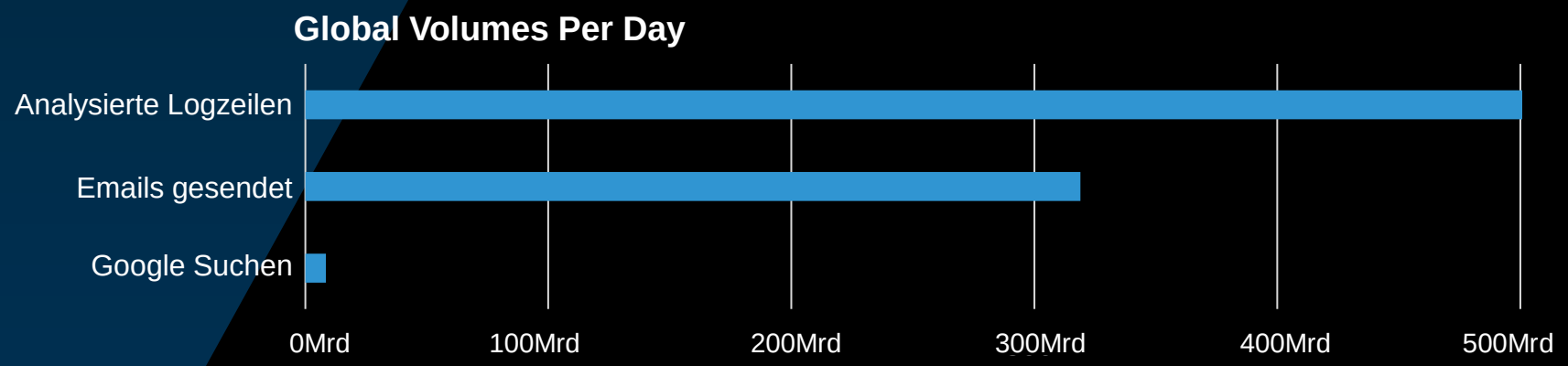
5
DC weltweit

500+
Milliarden
Logzeilen pro Tag

3M+
AW aktive Agenten
and 25,000+ sensors

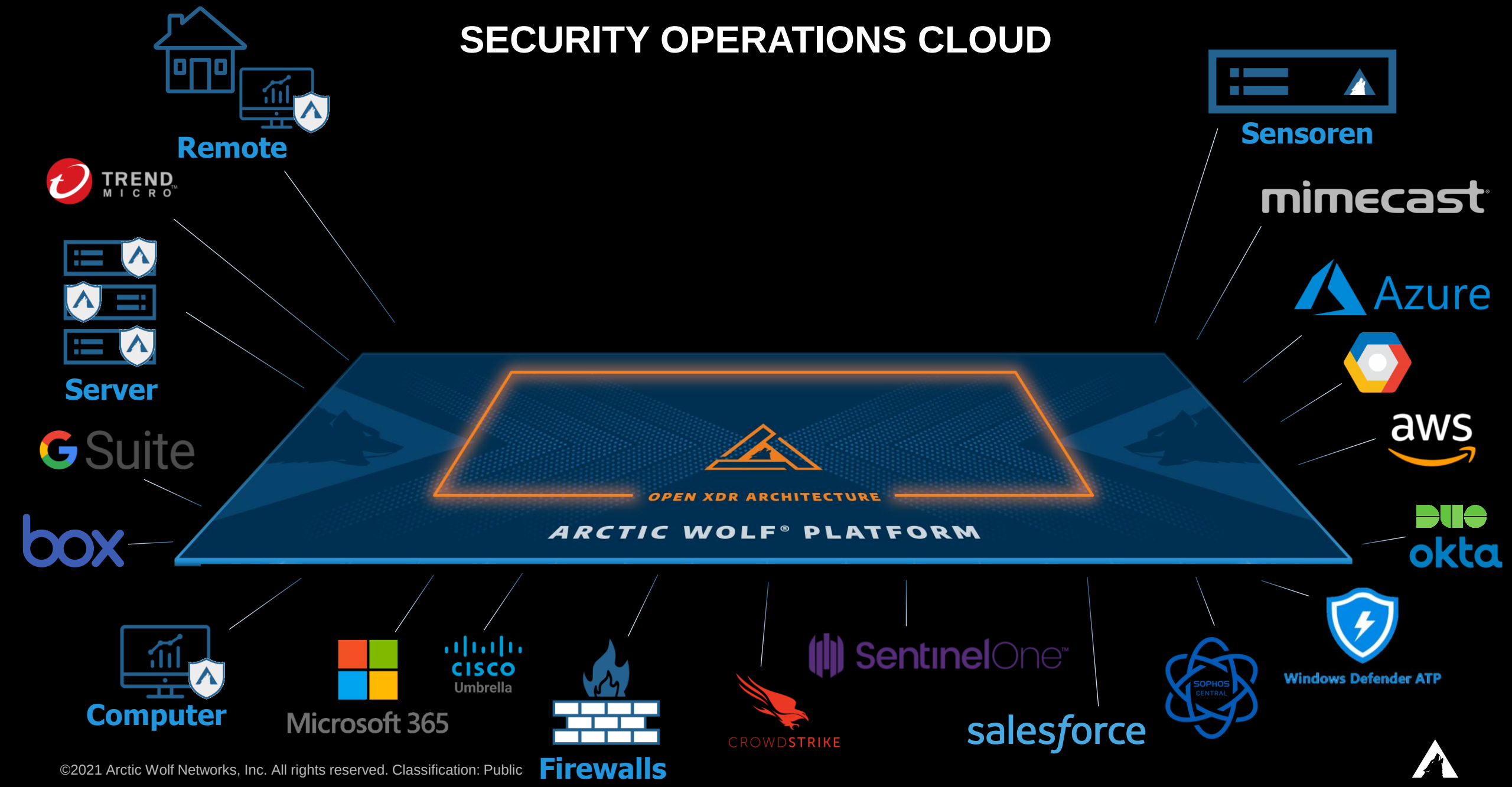
12M+
Schwachstellen
werden pro Woche
identifiziert

600+
Incident Response
Fälle pro Jahr



ARCTIC WOLF
SECURITY OPERATIONS

SECURITY OPERATIONS CLOUD



SECURITY OPERATIONS CLOUD

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

Schwarmintelligenz durch ARCTIC WOLF LABS

Threat Intelligence und Security Research

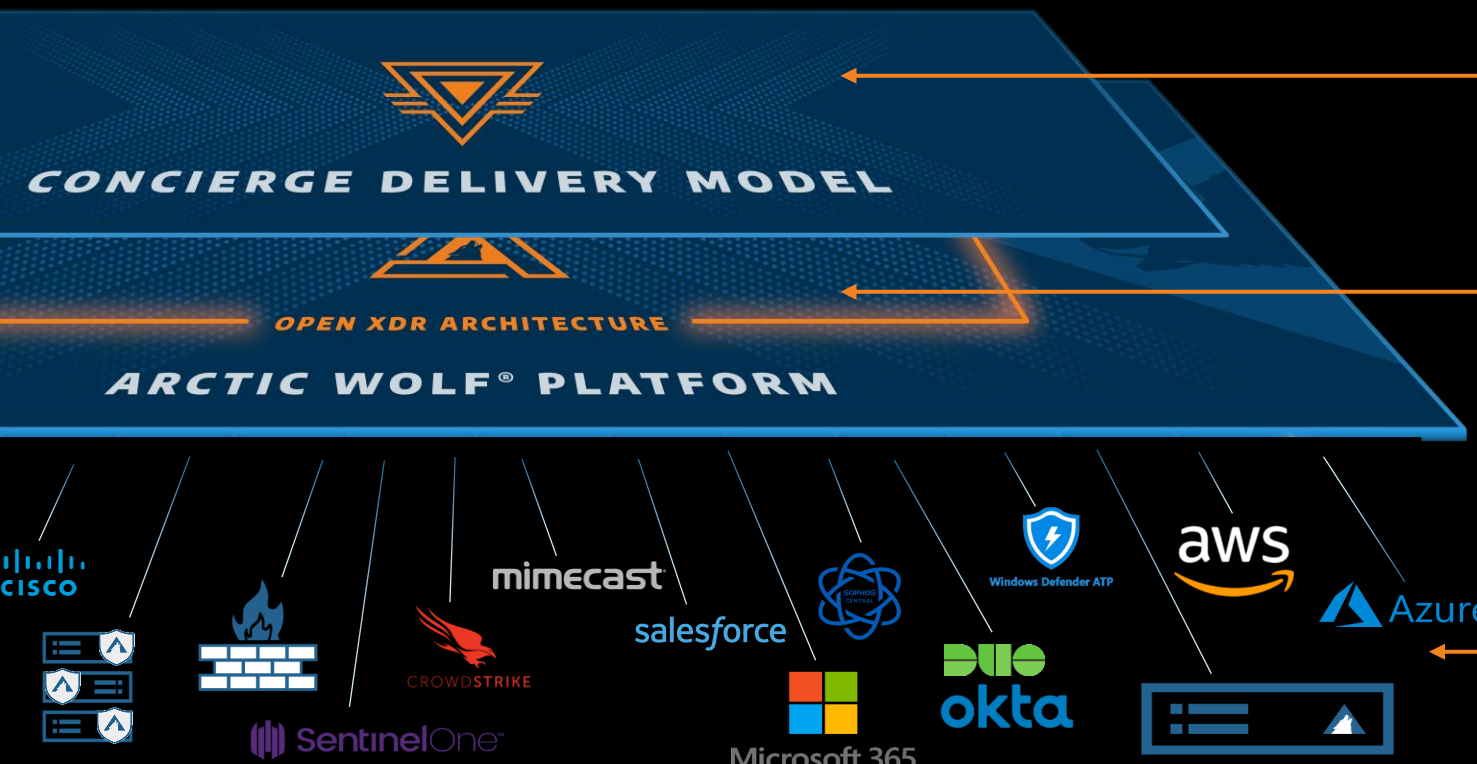
Detection & Response Engineering

KI und Datenwissenschaft

Security Posture Engineering

SCHWARMINTELLIGENZ VON **5.300+ CUSTOMERS**

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

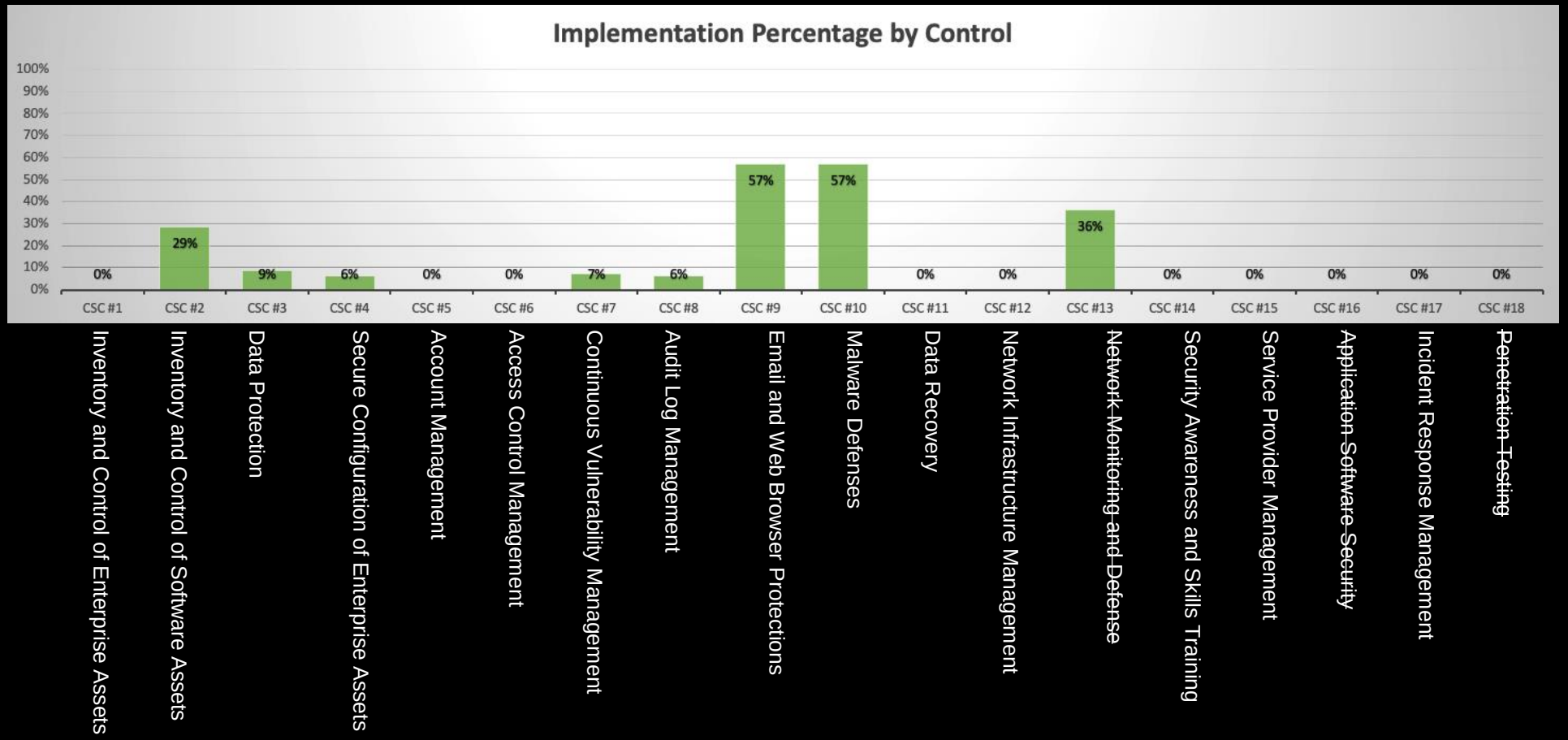
Finetuning der Plattform

Cyber Defence Maturity Assessment

Phase 3

CDMA ohne Arctic Wolf

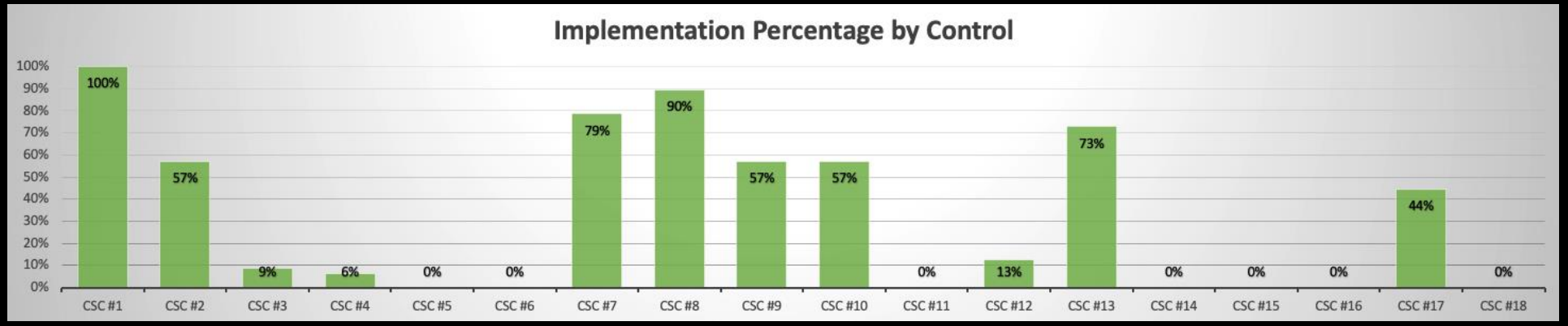
Nach der Analyse stellt Ihnen ihr Concierge Security Team den Report vor.
Ergebnis ohne Arctic Wolf Services:



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

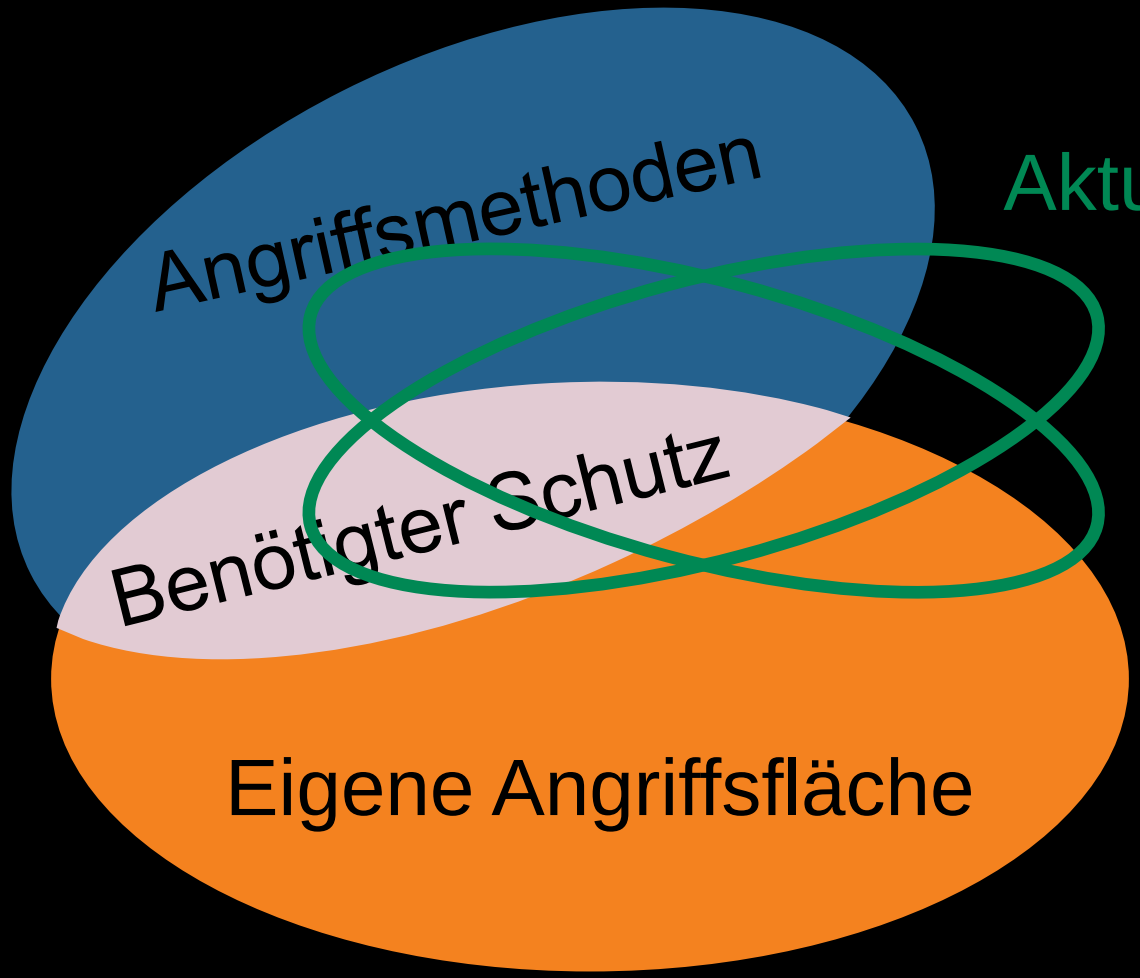
CDMA mit Arctic Wolf

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



Das Concierge Security 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
Fokus nach Kundenwunsch

#1 #2 #3 #...

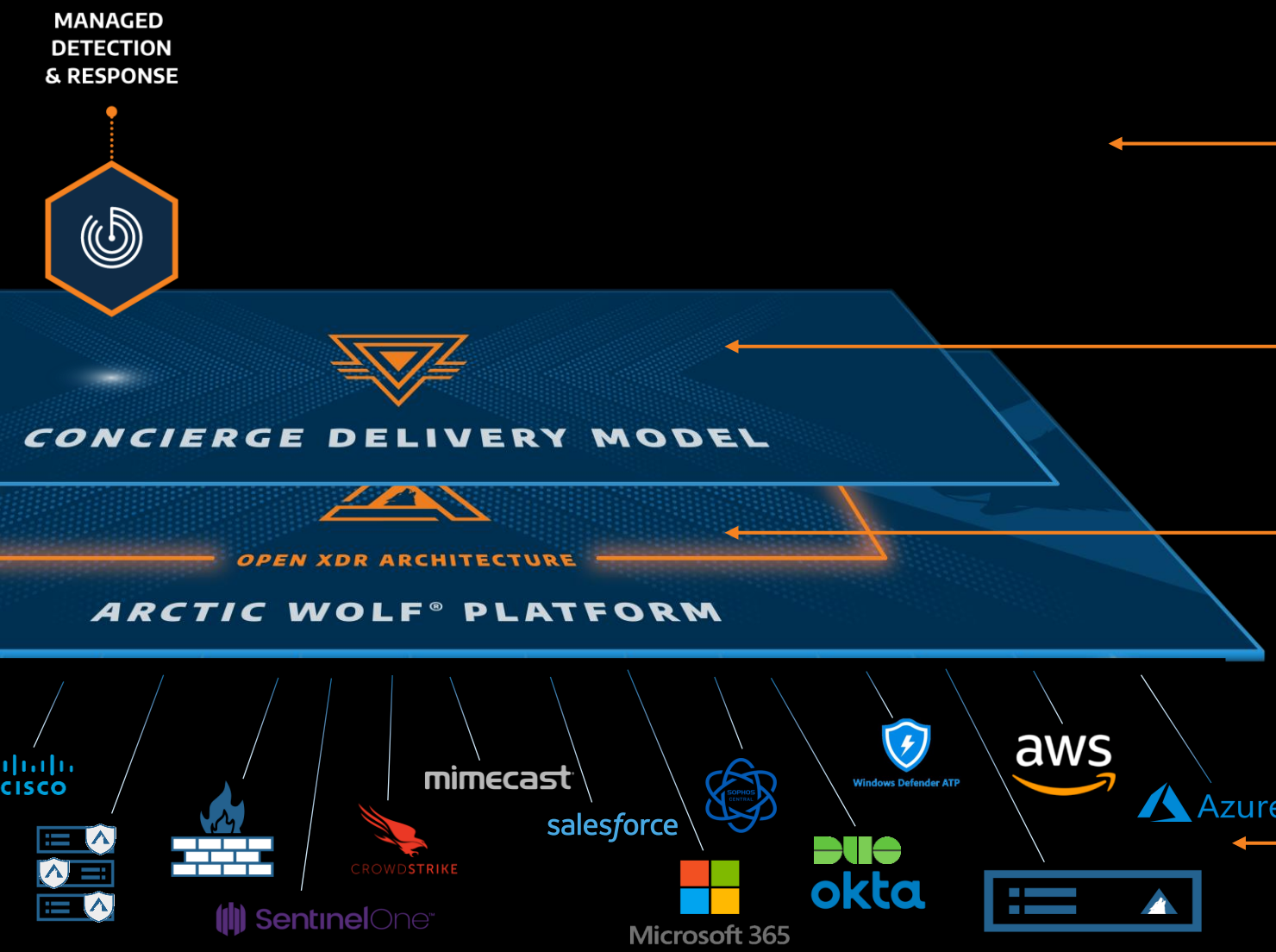
Security Journey – Regelmäßige Termine

Security Touchpoints

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

AW Security Operation Teams

SECURITY OPERATIONS CLOUD



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

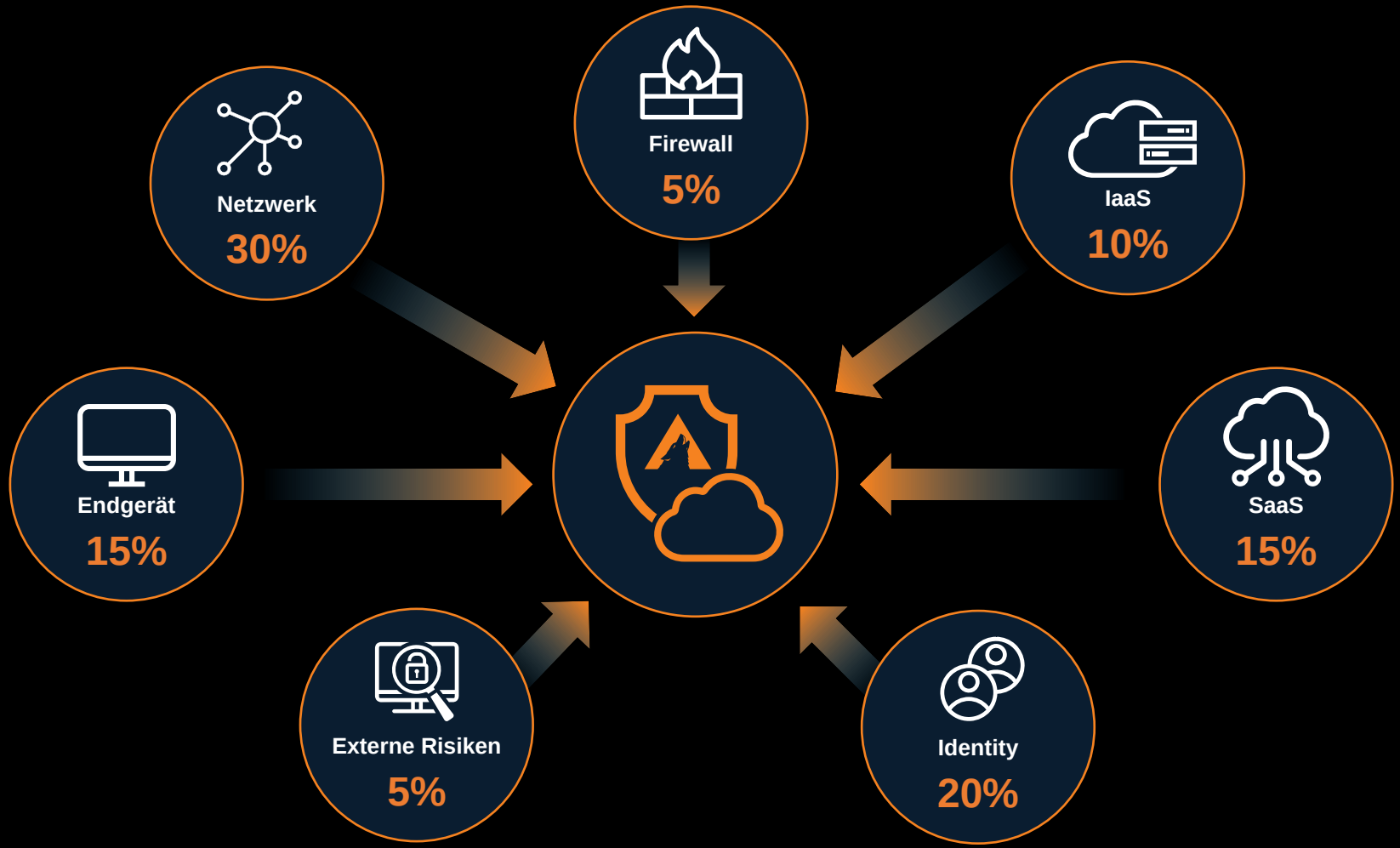
Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

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

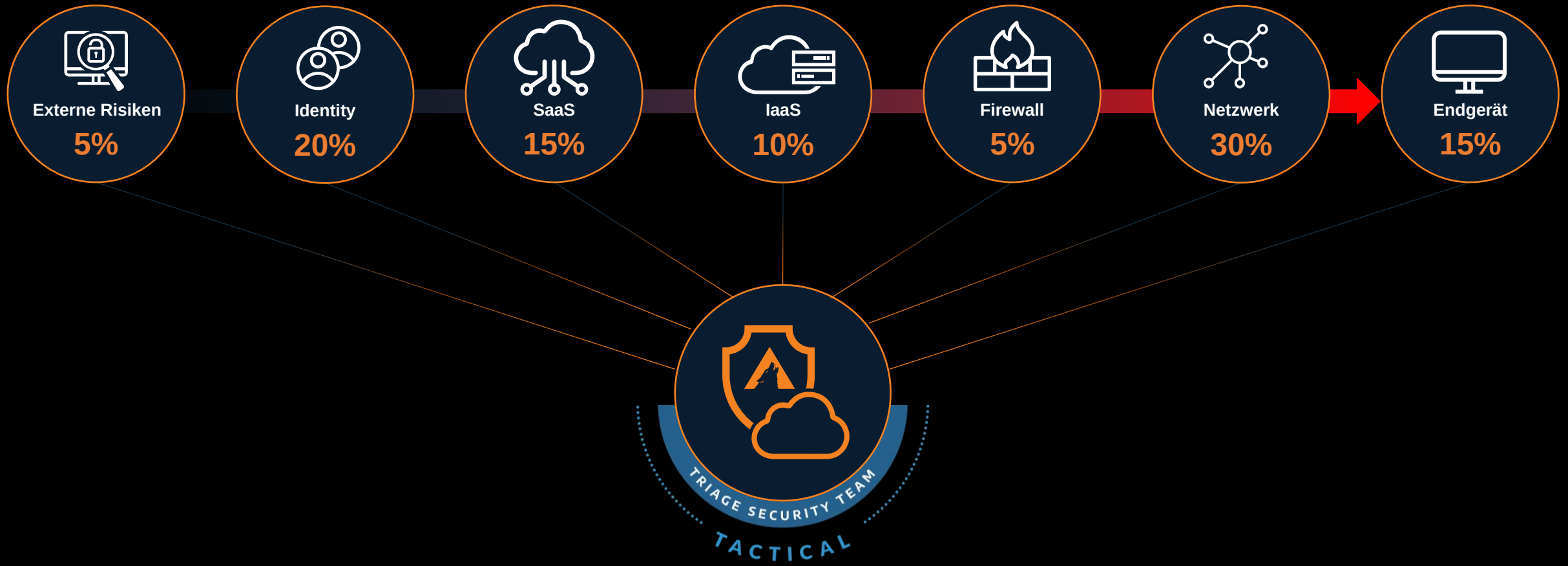
Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

Quellen der Tickets

Ermittlungen werden durch den ersten Indikator eingeleitet



Cyberattacke via Cloud & Identity

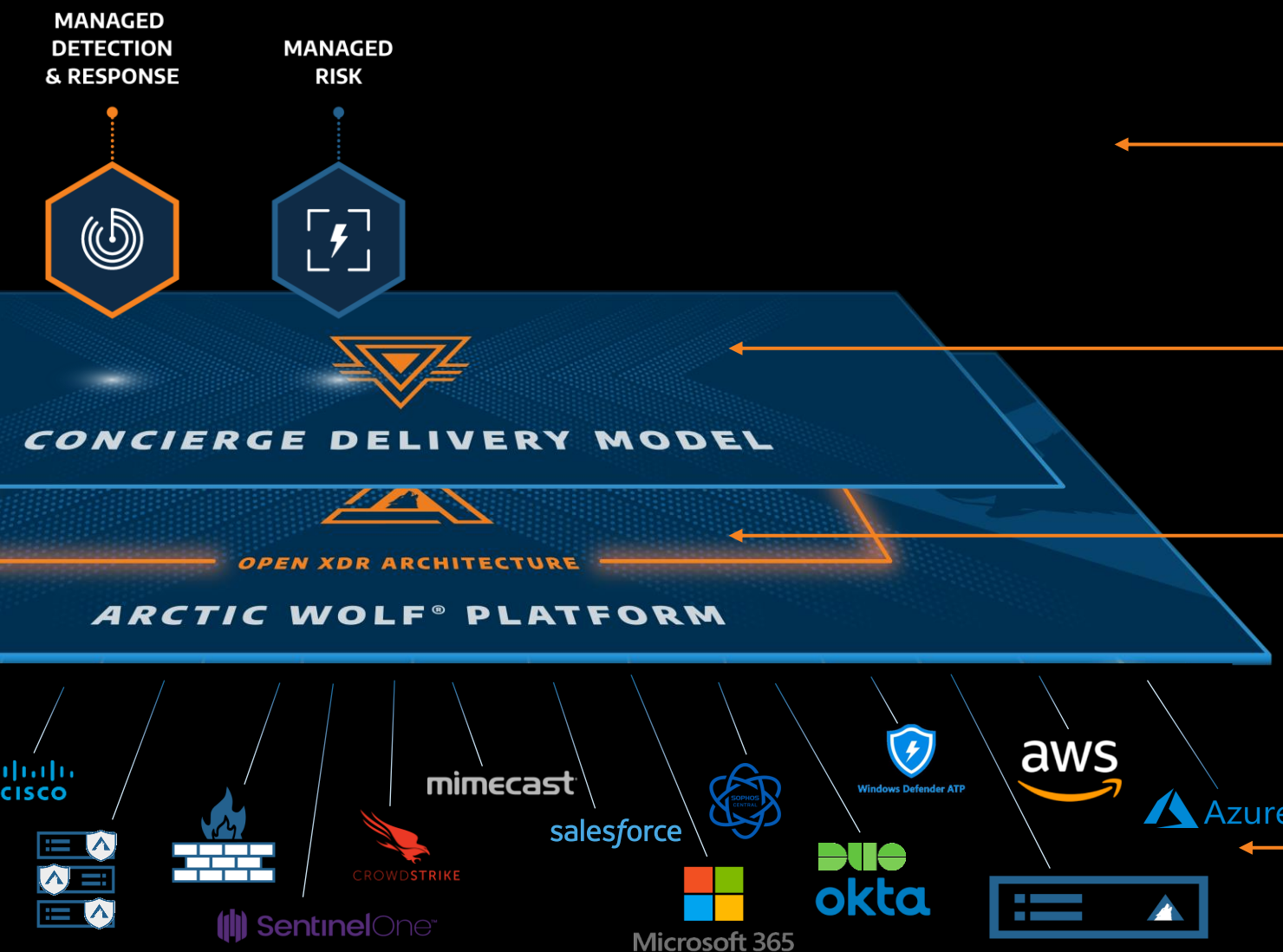


***Mehr* als Endgeräte zu schützen, bedeutet *vor* dem Endgerät zu schützen**

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

SECURITY OPERATIONS CLOUD



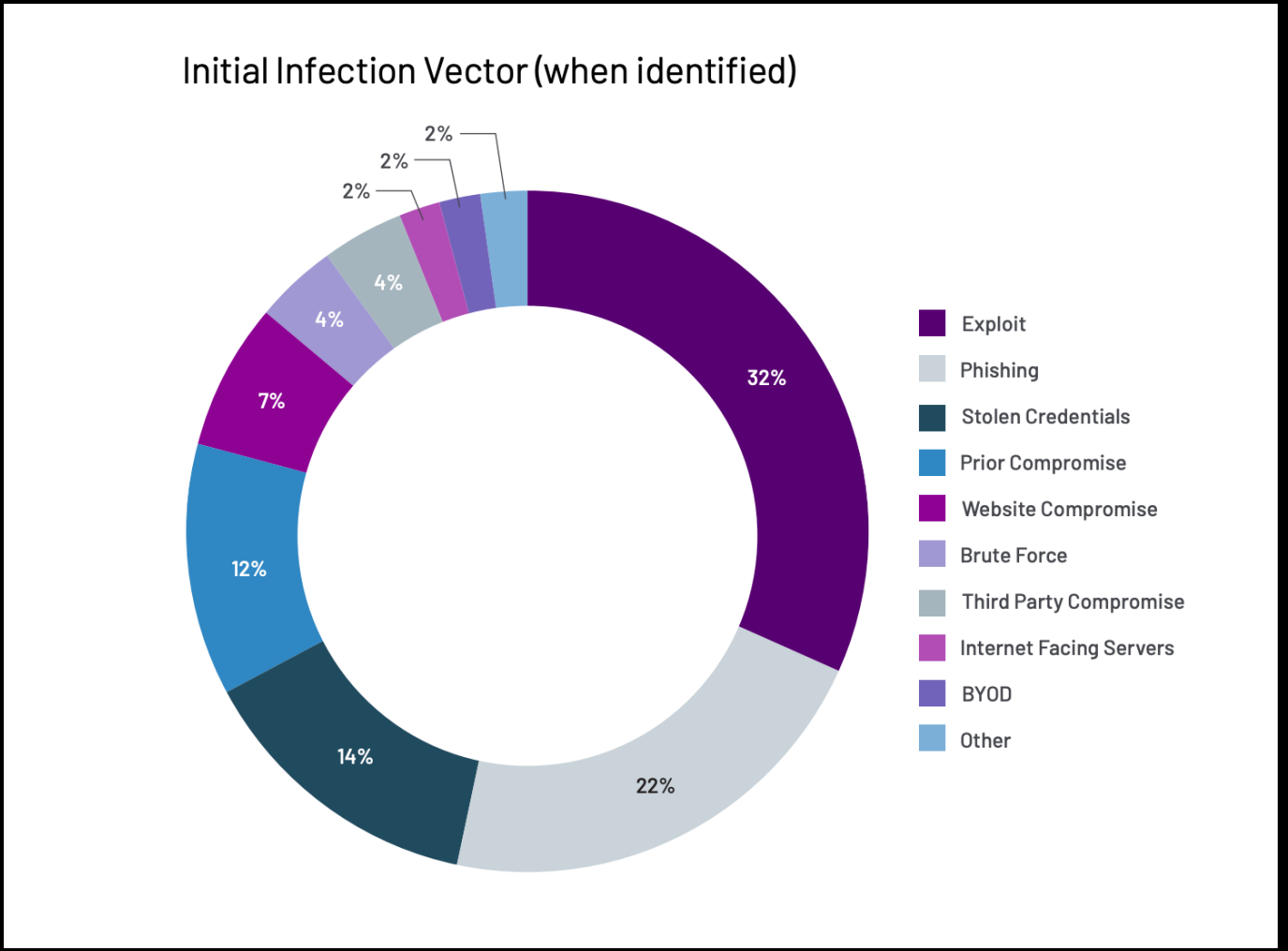
Wir stellen Services für das gesamte **Security Operations Modell** zur Verfügung

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

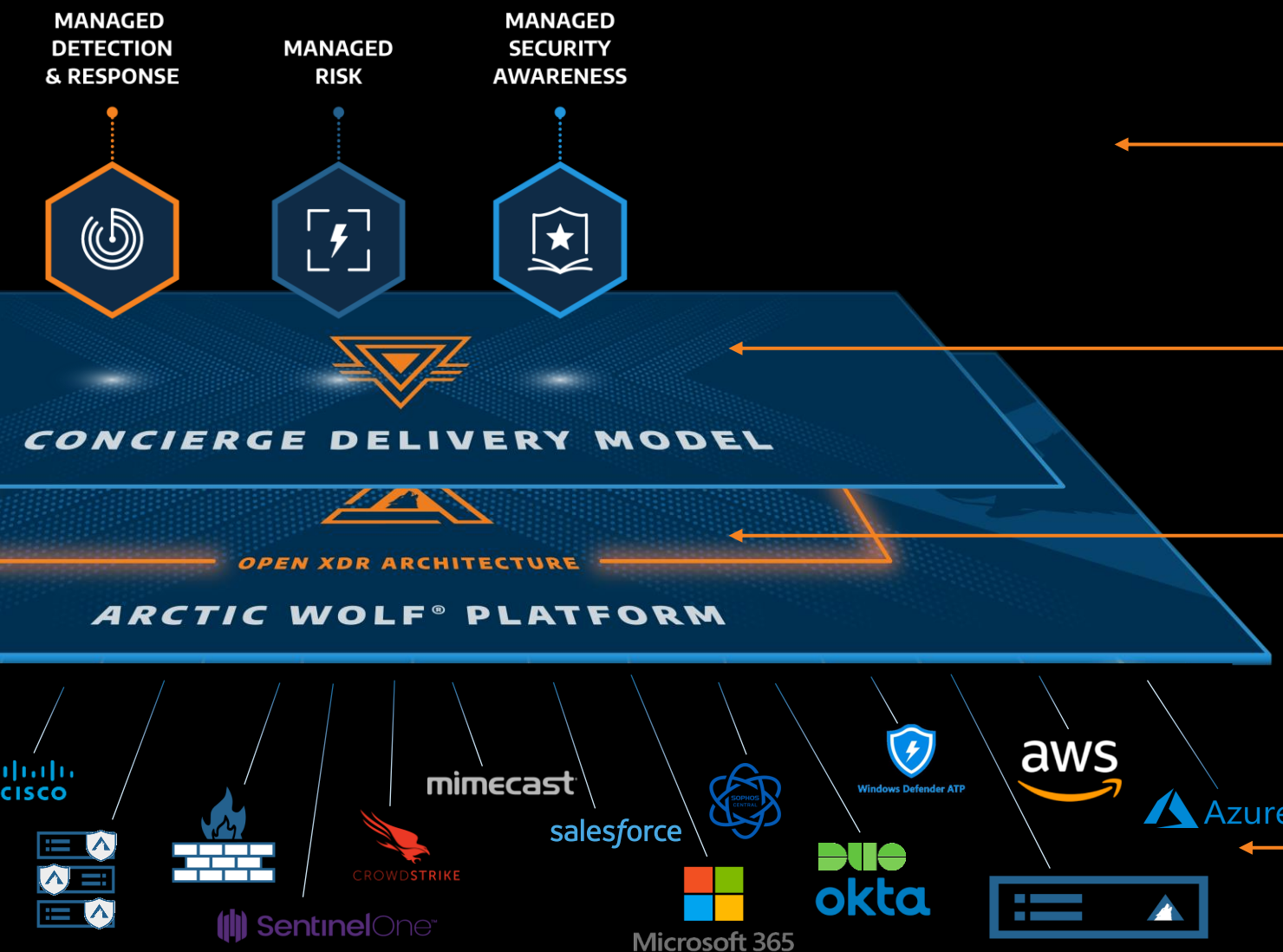
Bestehende Technologien nutzen um, eine Sicht auf Angriffspunkte zu bekommen: Endgeräte, Netzwerk, Cloud, Identitäten & Menschen

Exploits sind Nummer 1



Quelle: MANDIANT M-TRENDS 2023

SECURITY OPERATIONS CLOUD



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

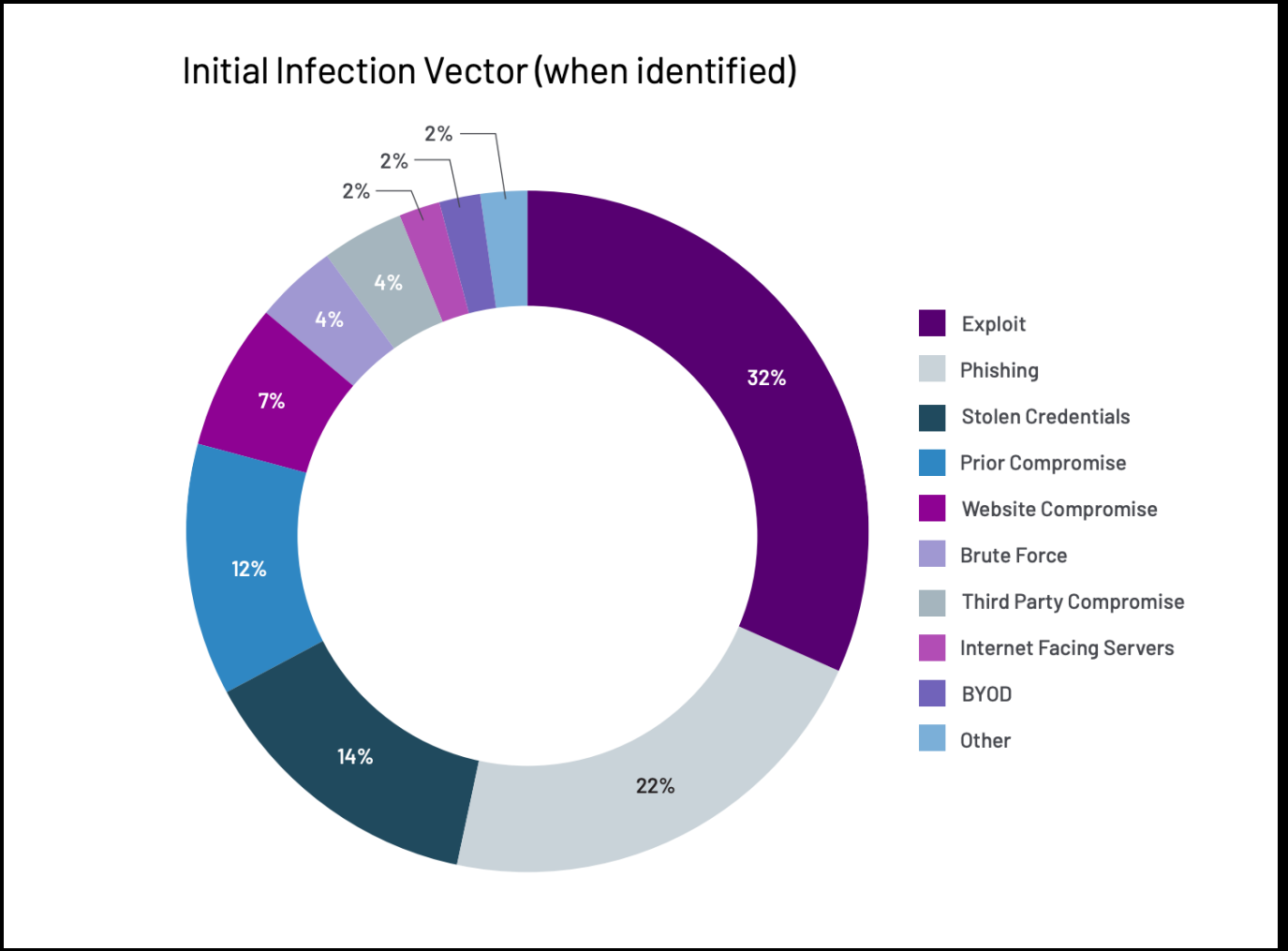
Ein Team von zugewiesenen Security-Experten die Ihre Organisation kennenlernen und kontinuierlich ihren Sicherheitsstatus verbessern

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

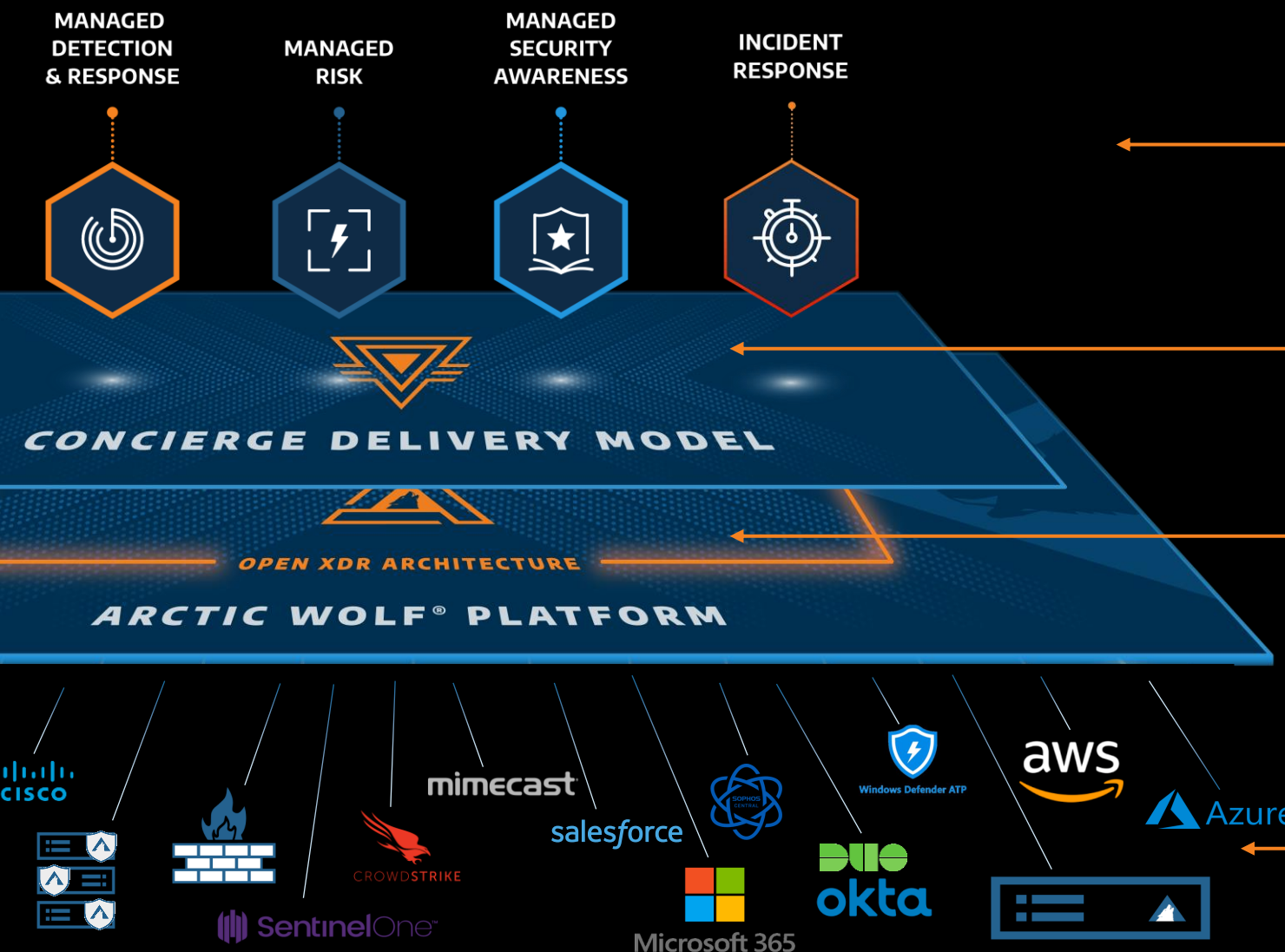
Der Faktor Mensch

Phising sind Nummer 2



Quelle: MANDIANT M-TRENDS 2023

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

Die meisten Firmen stehen hier

Lücke

ARCTIC WOLF

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

WIEDERSTANDS-FÄHIGKEIT

Proaktiv

Konform (ISO etc)

Versicherbar

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 >5400 Kunden
- Industrieführenden SLO von <30 Minuten für Identifikation, Analyse und detaillierte Lösungsbeschreibung
- **Flatrate** - Einfaches, verständliches und planbares Preismodel

ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Danke