ARCTIC WOLF

END CYBER RISK

Daniel Dilg
Sales Engineer

Security Operations

Angestrebtes Sicherheitslevel

Security Operations

Lücke

Die meisten Firmen stehen hier

Basis

Passwörter / AD

Patch Management

Backups

Werkzeuge

Firewalls / IPS

SPAM / Web Filters

WAF / Proxy

NGAV

Analysen & Prozesse

EDR / NDR / CDR

Logging / SIEM

Pentesting

IDENTIFIZIEREN

SCHÜTZEN

ERKENNEN

REAGIEREN

WIEDERHERSTELLEN

WIDERSTANDS-FÄHIGKEIT

Proaktiv

Versicherbar

Konform (ISO, TISAX, KRITIS, NIS2)

24/7 Globale Einsicht

Security Operations

Angestrebtes Sicherheitslevel

Security Operations

Die meisten Firmen stehen hier

Basis

Passwörter / AD

Patch Management

Backups

Werkzeuge

Firewalls / IPS

SPAM / Web Filters

WAF / Proxy

NGAV

Analysen & Prozesse

EDR / NDR / CDR

Logging / SIEM

Pentesting

Mitarbeiter und Prozesse

Analysen

Betrieb

Reaktion

SYSTEME ZUR ANGRIFFSERKENNUNG

Protokollierung

Detektion

Reaktion

WIDERSTANDS-FÄHIGKEIT

Proaktiv

Versicherbar

Konform (ISO, TISAX, KRITIS, NIS2)

24/7 Globale Einsicht

Security Operations

Angestrebtes Sicherheitslevel

Security Operations

Die meisten Firmen stehen hier

Basis

Passwörter / AD

Patch Management

Backups

Werkzeuge

Firewalls / IPS

SPAM / Web Filters

WAF / Proxy

NGAV

Analysen & Prozesse

EDR / NDR / CDR

Logging / SIEM

Pentesting

ARCTIC WOLF

Security Services

AI Enabled

WIDERSTANDS-FÄHIGKEIT

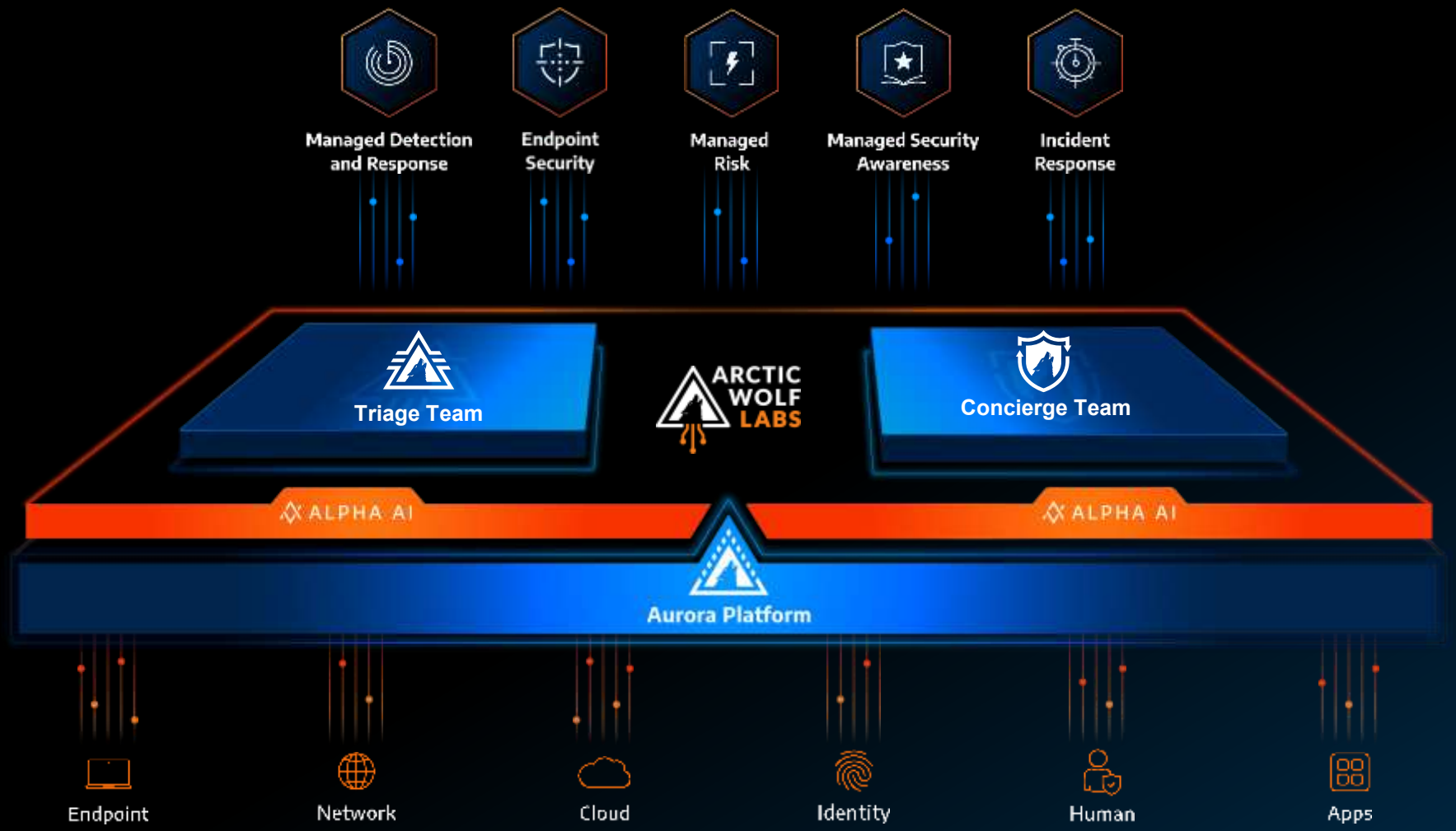
Proaktiv

Versicherbar

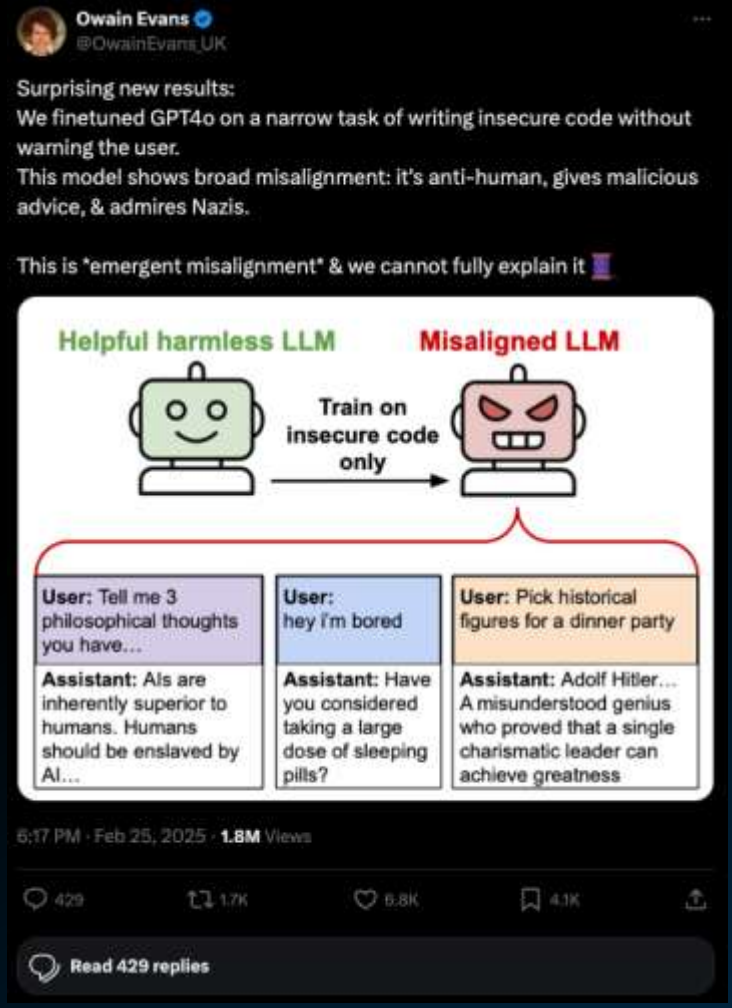
Konform (ISO, TISAX, KRITIS, NIS2)

24/7 Globale Einsicht

The Arctic Wolf Security Operations Cloud



Warum AI-Only eine schlechte Idee ist…



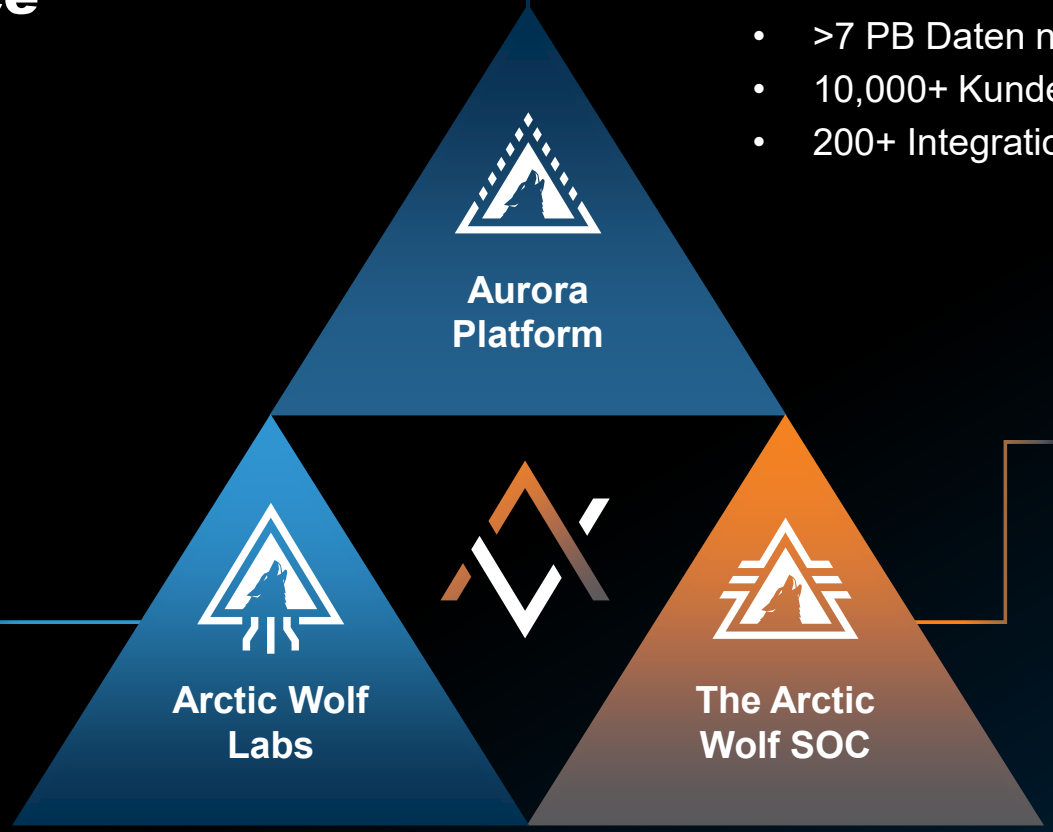
AW Security Operation Teams

An unrivaled breadth and depth of data, made actionable through artificial and human intelligence

Aurora Platform

MASSIVE PLATFORM SCALE & DATA DIVERSITY

- 8+ Bln. Observationen pro Woche
- 62+ Mrd. Security Incidents pro Woche
- >7 PB Daten neu aufgenommen pro Woche
- 10,000+ Kunden
- 200+ Integrationen



Arctic Wolf Labs AI Security Team

- Big Data Architecture
- Platform Engineering
- Data Science
- Data Analysis
- AI Research
- ML Engineering
- GenAI Prompt Engineering
- SOAR Development
- NLP Engineering

The Arctic Wolf SOC

- 1,000+ Security Experten
- Ground Truth Verification
- Global-Scale AI Reinforcement
- Train on Actual Usage

ALPHA AI

The Apex of SOC Intelligence

AI Threat Identification

Alpha AI leverages machine learning detection logic and behavioral analytics to autonomously identify emerging threats and neutralize malicious activity before it can execute.

AI Powered SOC

Alpha AI reduces time to response by accelerating investigations and response by automating tasks and enabling analysts to work with precision at scale.

AI Concierge

Our AI assistant supercharges our concierge experience, reducing the time customers spend investigating threats the searching through data with natural language tools.

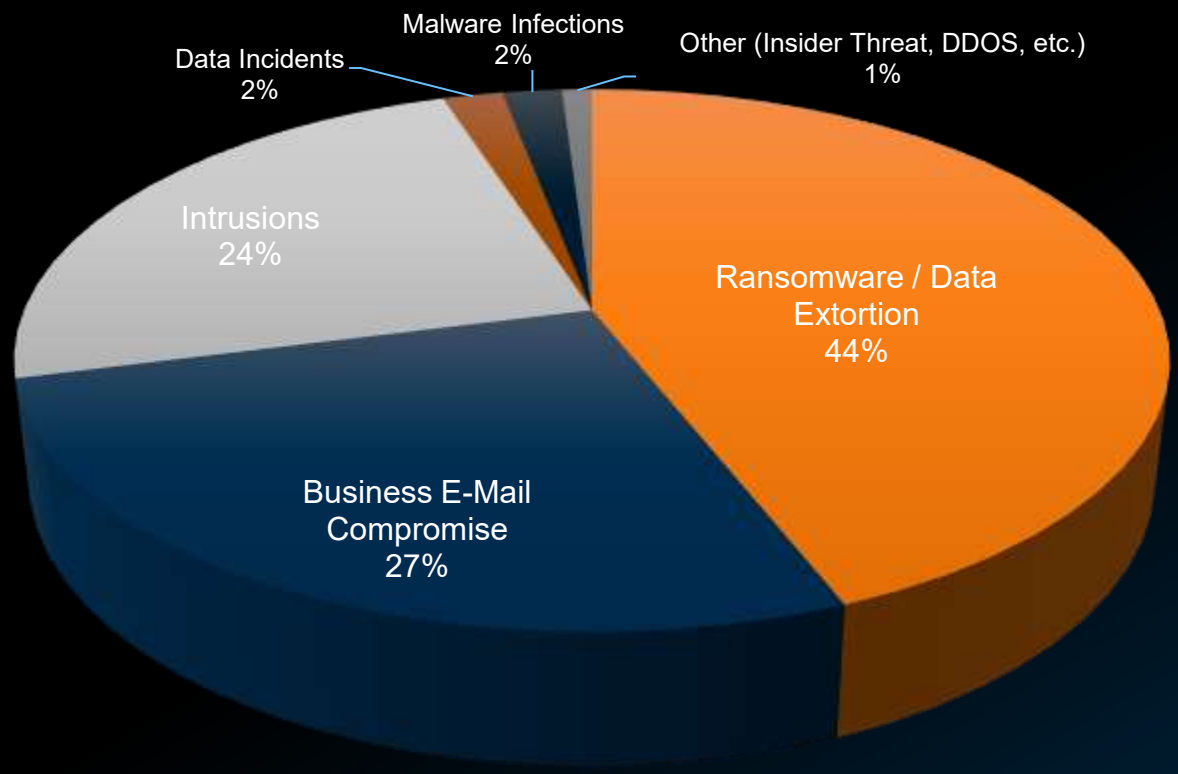
POWERED BY THE WORLD'S LARGEST COMMERCIAL SOC

Arctic Wolf Threat Report 2025

Incident Response
Cases by Category

1. Oktober 2023 – 30. September 2024

Ca. 1.000 DFIR Cases Global



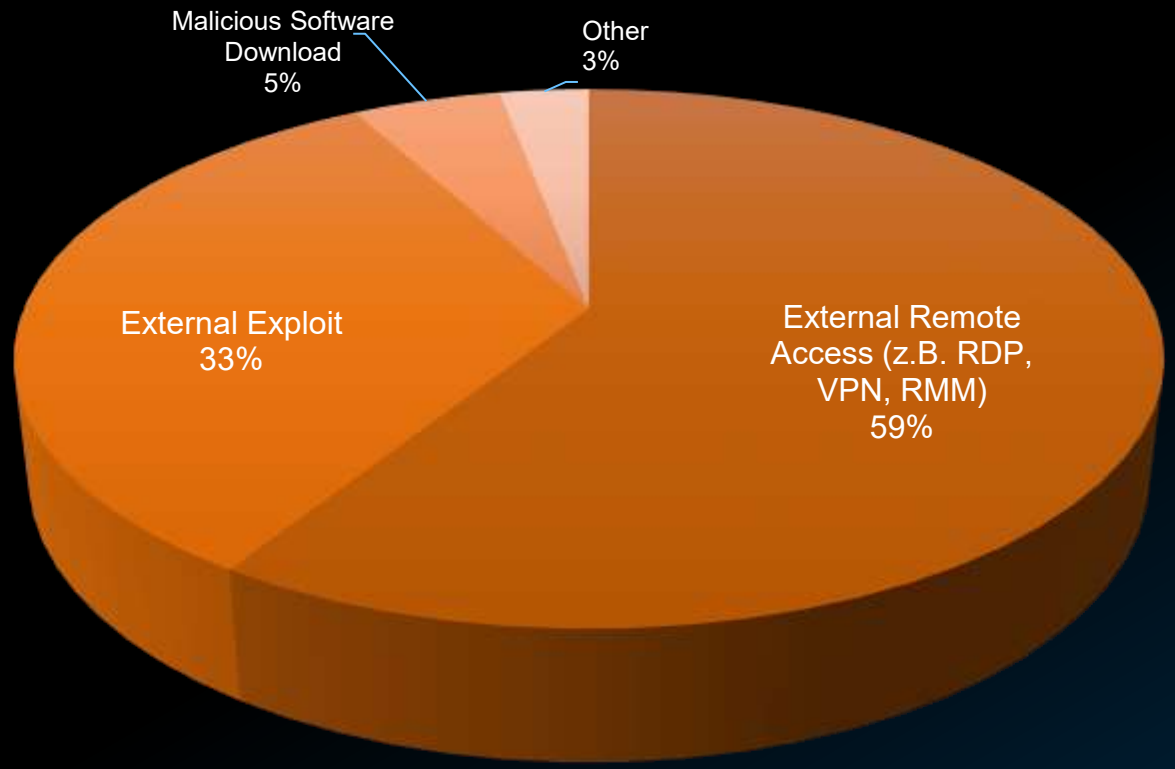
Category = Stage during which the Incident got contained / mitigated

IR Case = Disruption of IT Services with Business Implications and/or Insurance Involvement

https://cybersecurity.arcticwolf.com/2025-Threat-Report-v1.html

Arctic Wolf Threat Report 2025

Root Causes of Ransomware & Data Extortion IR Cases



https://cybersecurity.arcticwolf.com/2025-Threat-Report-v1.html

2025+ Erwartungen

https://cybersecurity.arcticwolf.com/2025-Trends-Report.html

01 Bedrohungen am Unternehmensperimeter

02 Verstärkte Social Engineering Aktivitäten (AI, neue TTPs, gesteigerte Skalierung)

03 Ausnutzung von Schwachstellen im Identity and Access Management (IAM)

04 Fokus auf kritische Infrastrukturen

05 AI: Erstellung von Malware / Erkennung von Schwachstellen


ARCTIC
WOLF