Alarmflut, Fachkräftemangel, fehlende Controls – so hilft MDR

Agenda

- Ausgangslange und empfohlene Massnahmen
- Herausforderungen in der Umsetzung
- Wie ein MDR hilft (am Beispiel von Arctic Wolf)
- Q&A

Alexander Schmidt

alexander.schmidt@arcticwolf.com
linkedin.com/in/alexander-schmidt-arcticwolf

Felix Guggenheim

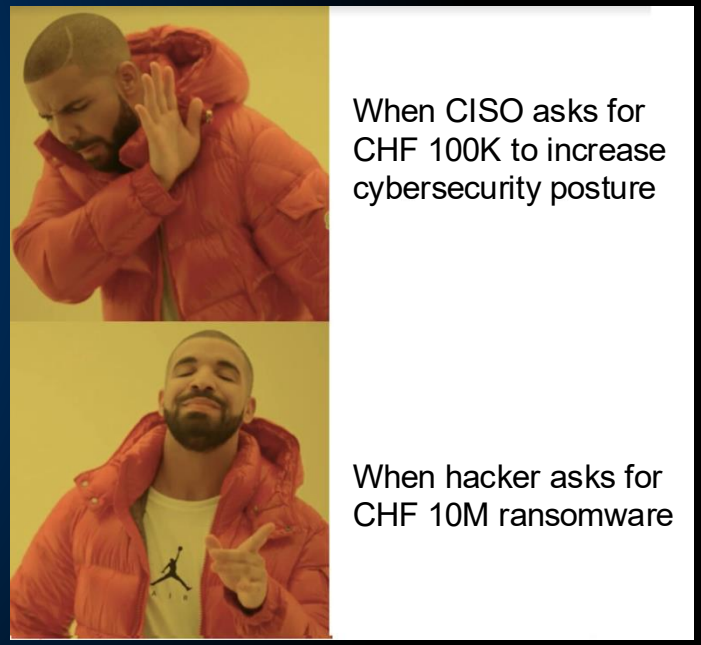
felix.guggenheim@arcticwolf.com
www.linkedin.com/in/fguggenheim

Ausgangslage und empfohlene Massnahmen

KMU in der Schweiz

Die Top 3 Herausforderungen für Cybersecurity

- Fachkräftemangel, Bewusstsein und Kompetenzen
- Budgetengpässe und Komplexität der Bedrohungslandschaft
- Organisatorische Defizite, fehlende Prozesse und unzureichende Security Controls

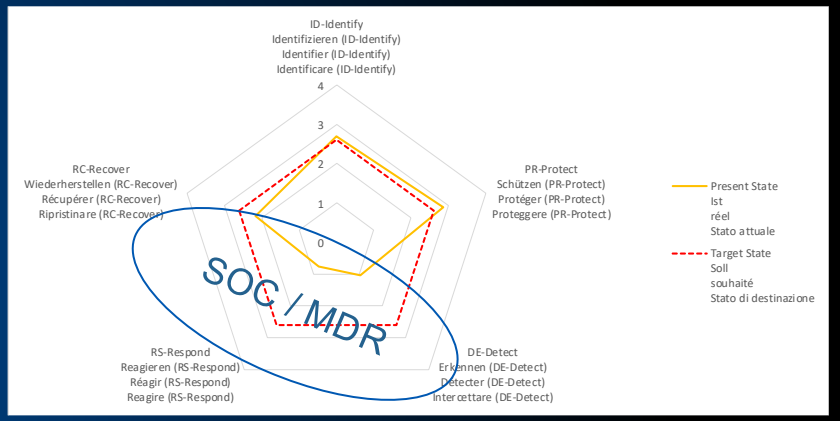


Empfehlungen der Behörden

IKT-Minimalstandard und CSRM – Empfehlungen des Bundesamtes für Cybersicherheit BACS

IKT-Minimalstandard: Framework als Gesamtkonzept

Problematik bei vielen Unternehmen:
- Einseitiger Fokus auf Prävention (Installation von Technologien)
- Unzureichende Organisation: Detektions- und Reaktionsfähigkeiten
- Häufige Ursache: Ressourcenmangel (Personal, Kosten, KnowHow)



4.1	**Aufzeichnung und Überwachung** Für jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt (und dabei insbesondere für Netzwerke) müssen sicherheitsrelevante Aktivitäten, Vorfälle und Ereignisse aufgezeichnet[50] und im Hinblick auf möglicherweise erfolgte Angriffe möglichst zeitnah und automatisiert ausgewertet werden (z. B. im Rahmen eines SOC).

CSRM: Cybersicherheits- und Resilienzmethode. Basiert auf einem Grundschutzansatz.

Problematik bei vielen Unternehmen:
- Mangelndes Verständnis über Basisanforderungen gegenüber erweiterten Massnahmen
- Organisatorische Massnahmen (Detektions- und Reaktionsfähigkeiten) werden als optional bzw. Luxus verstanden
- Häufige Ursache: Ressourcenmangel (Personal, Kosten, KnowHow)

Quelle: BACS Bundesamt für Cybersicherheit, https://www.ncsc.admin.ch/ncsc/de/home.html

Empfehlungen der Versicherungen

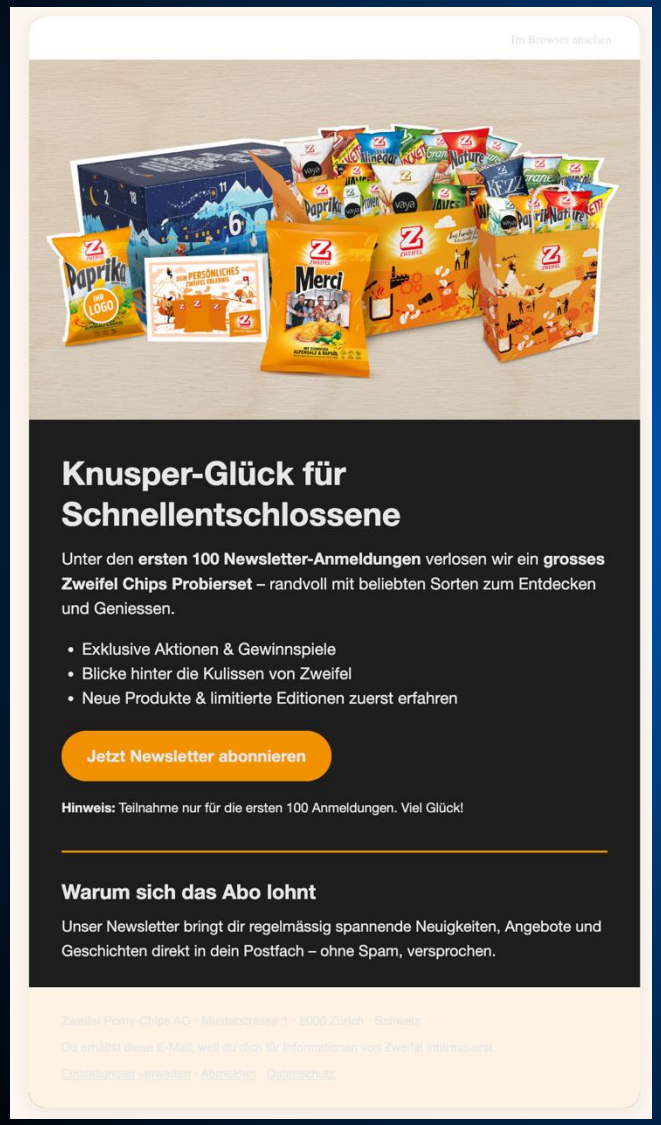
12 Key Controls

- Multi-Faktor-Authentifizierung
- Endpoint detection and response (EDR)
- Gesicherte, verschlüsselte und getestete Back Ups
- Privileged access management (PAM)
- E-Mail-Filterung und Web-Sicherheit
- Patch- und Schwachstellen-management
- Cyber Incident Response
- Cyber Security Awareness Training und Phishing-Kampagnen
- System Härtungsmassnahmen
- Logging und Monitoring / Netzwerkschutz
- Umgang mit End-of-life-Systemen
- IT-Lieferkette

Quelle: Marsh, Strengthen cybersecurity with 12 key controls: https://www.marsh.com/en/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html

Herausforderungen in der Umsetzung

User Awareness



Im Browser ansehen

Knusper-Glück für Schnellentschlossene

Unter den **ersten 100 Newsletter-Anmeldungen** verlosen wir ein **grosses Zweifel Chips Probierset** – randvoll mit beliebten Sorten zum Entdecken und Geniessen.

- Exklusive Aktionen & Gewinnspiele
- Blicke hinter die Kulissen von Zweifel
- Neue Produkte & limitierte Editionen zuerst erfahren

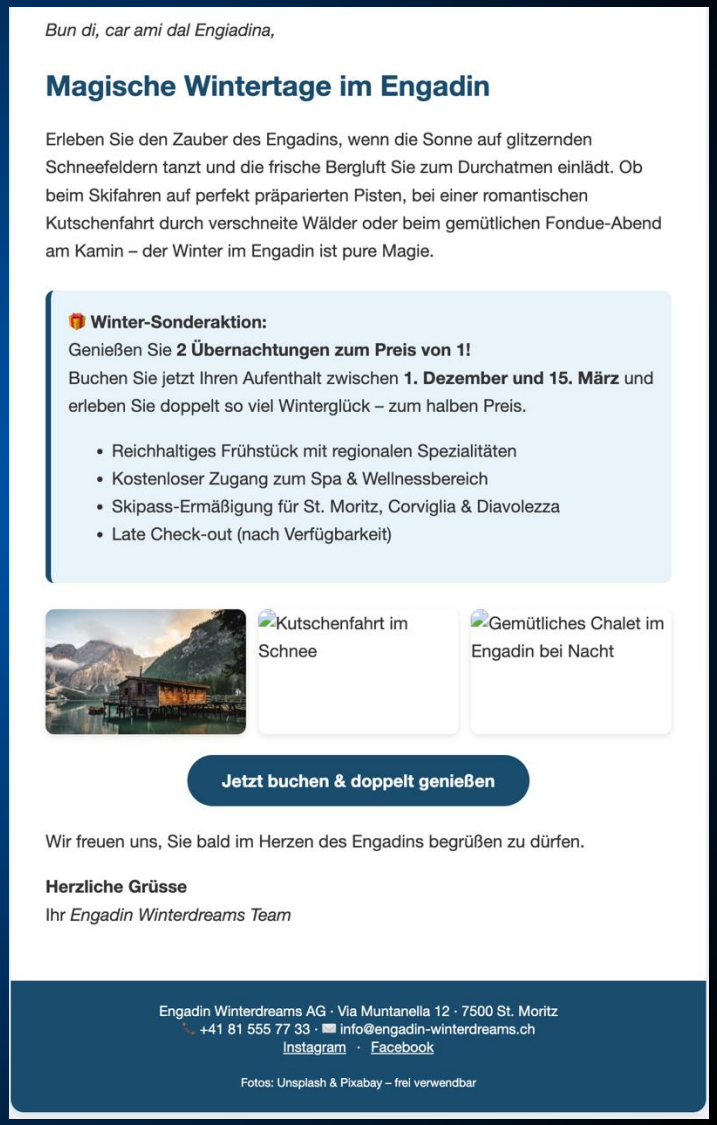
Jetzt Newsletter abonnieren

Hinweis: Teilnahme nur für die ersten 100 Anmeldungen. Viel Glück!

Warum sich das Abo lohnt

Unser Newsletter bringt dir regelmässig spannende Neuigkeiten, Angebote und Geschichten direkt in dein Postfach – ohne Spam, versprochen.

Zweifel Pomy-Chips AG · Musterstrasse 1 · 8000 Zürich · Schweiz
Du erhältst diese E-Mail, weil du dich für Informationen von Zweifel interessierst.
Einstellungen verwalten · Abmelden · Datenschutz



Bun di, car ami dal Engiadina,

Magische Wintertage im Engadin

Erleben Sie den Zauber des Engadins, wenn die Sonne auf glitzernden Schneefeldern tanzt und die frische Bergluft Sie zum Durchatmen einlädt. Ob beim Skifahren auf perfekt präparierten Pisten, bei einer romantischen Kutschenfahrt durch verschneite Wälder oder beim gemütlichen Fondue-Abend am Kamin – der Winter im Engadin ist pure Magie.

🎁 **Winter-Sonderaktion:**
Genießen Sie **2 Übernachtungen zum Preis von 1!**
Buchen Sie jetzt Ihren Aufenthalt zwischen **1. Dezember und 15. März** und erleben Sie doppelt so viel Winterglück – zum halben Preis.

- Reichhaltiges Frühstück mit regionalen Spezialitäten
- Kostenloser Zugang zum Spa & Wellnessbereich
- Skipass-Ermäßigung für St. Moritz, Corviglia & Diavolezza
- Late Check-out (nach Verfügbarkeit)

Kutschenfahrt im Schnee

Gemütliches Chalet im Engadin bei Nacht

Jetzt buchen & doppelt genießen

Wir freuen uns, Sie bald im Herzen des Engadins begrüßen zu dürfen.

Herzliche Grüsse
Ihr *Engadin Winterdreams Team*

Engadin Winterdreams AG · Via Muntanella 12 · 7500 St. Moritz
📞 +41 81 555 77 33 · ✉ info@engadin-winterdreams.ch
Instagram · Facebook

Fotos: Unsplash & Pixabay – frei verwendbar

Cyber Risiken erhöhen sich

$10.3B
Verluste
Durch Cyberkriminalität in 2022

$12.5B
Verluste
Durch Cyberkriminalität in 2023

$16.6B
Verluste
Durch Cyberkriminalität in 2024

2022 → 2023
21% Zunahme

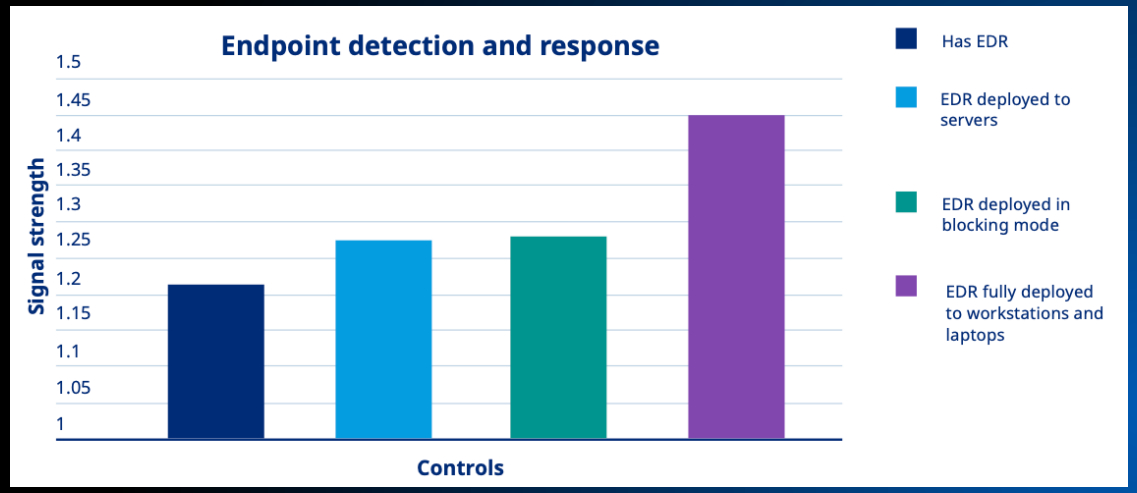
2023 → 2024
33% Zunahme

Effektivitätsproblem

Gesamtausgaben für IT-Security in 2024: **$183B, 13% YOY Zunahme**

Sources: IC3, Gartner, It-Harvest

EDR



Marsh: Connecting controls and incident outcomes, 2025

Gartner

Adversaries are likely to attack at times when we are unlikely to pay attention, rather than only in our “9 to 5” working days.

If you can’t support 24/7 operations, you have two options. You can either just go the route of protection with MDE P1 or you can supplement your security operations center (SOC) with managed detection and response (MDR) from Microsoft or a third-party managed security services provider (MSSP).

Gartner: Top 5 ‚Gotchas‘ of Microsoft DfE and How to Overcome Them

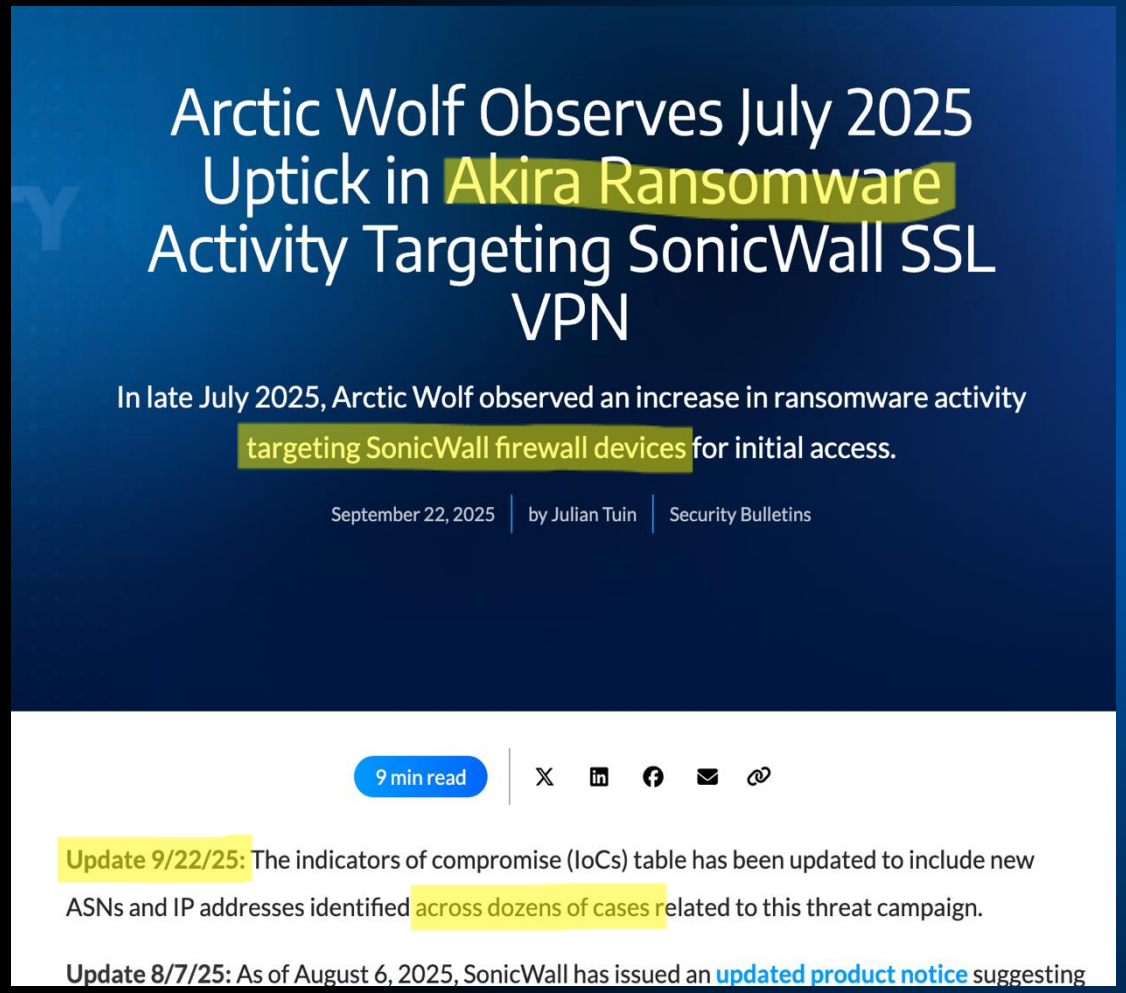
Der eigentliche Leverage im EDR-Bereich besteht im vollständigen Rollout und einer scharfen Konfiguration

Ohne 7x24 ist EDR nutzlos – Kunden können sich das Geld sparen und auf AV setzen

Monitoring / Detection / Response

„Das machen wir in der IT.“

Situational Awareness, Schwachstellen



Arctic Wolf Observes July 2025 Uptick in Akira Ransomware Activity Targeting SonicWall SSL VPN

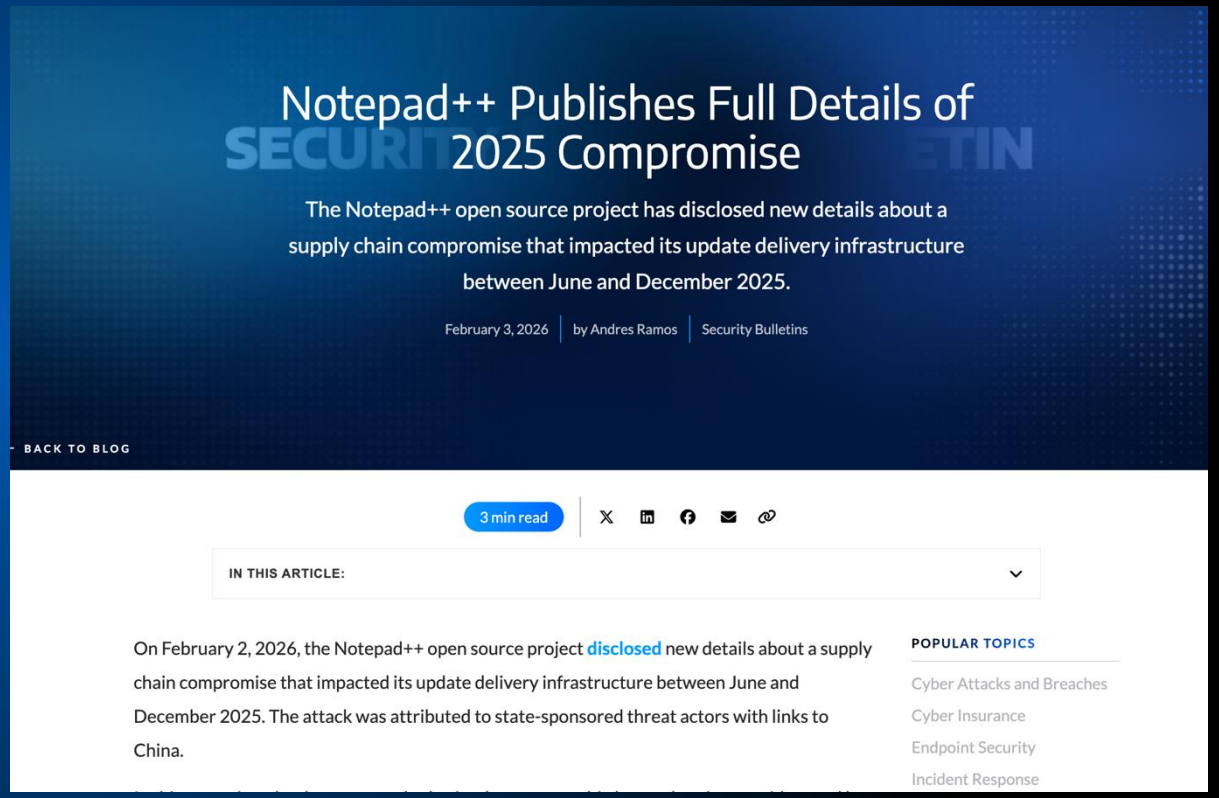
In late July 2025, Arctic Wolf observed an increase in ransomware activity targeting SonicWall firewall devices for initial access.

September 22, 2025 | by Julian Tuin | Security Bulletins

9 min read

Update 9/22/25: The indicators of compromise (IoCs) table has been updated to include new ASNs and IP addresses identified across dozens of cases related to this threat campaign.

Update 8/7/25: As of August 6, 2025, SonicWall has issued an updated product notice suggesting



Notepad++ Publishes Full Details of 2025 Compromise

The Notepad++ open source project has disclosed new details about a supply chain compromise that impacted its update delivery infrastructure between June and December 2025.

February 3, 2026 | by Andres Ramos | Security Bulletins

BACK TO BLOG

3 min read

IN THIS ARTICLE:

On February 2, 2026, the Notepad++ open source project disclosed new details about a supply chain compromise that impacted its update delivery infrastructure between June and December 2025. The attack was attributed to state-sponsored threat actors with links to China.

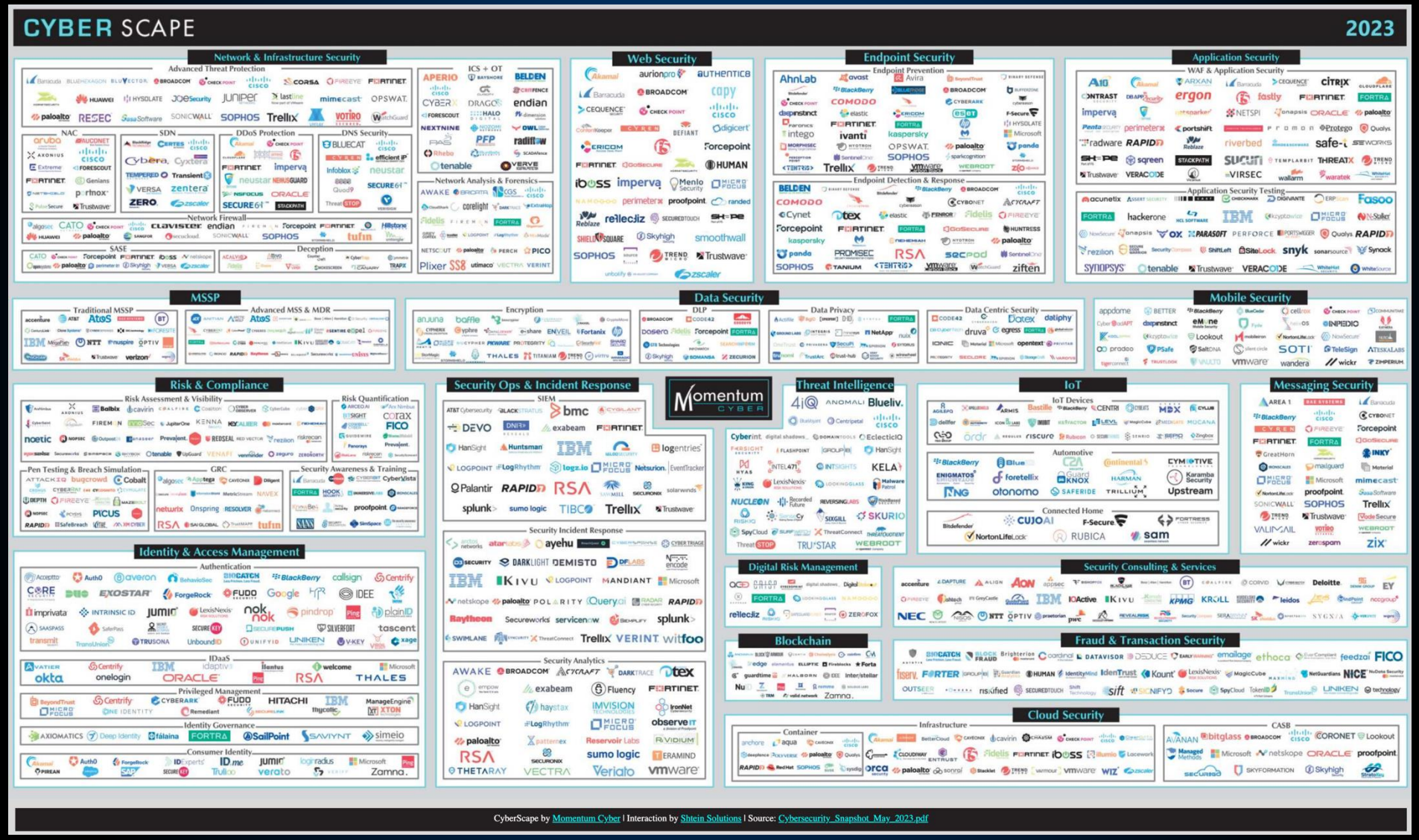
POPULAR TOPICS

Cyber Attacks and Breaches
Cyber Insurance
Endpoint Security
Incident Response

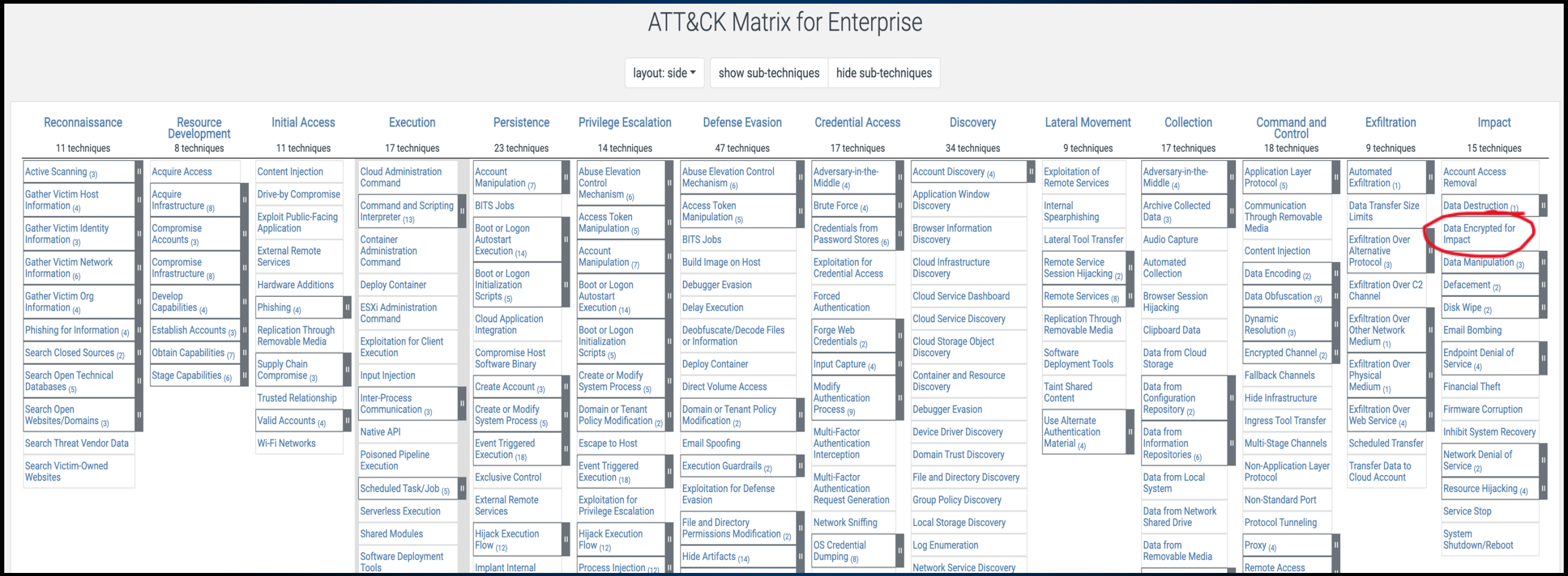
KI

Generatives Phishing & Social Engineering		AI und Phishing Pattern Erkennung
Environmental Learning zur Anomalie-Vermeidung		Verhaltensbasierte Anomalie-Erkennung
Generierung von realistischem White Noise		Massenverarbeitung von Logs und Alerts
Polymorphe Malware & Vibe Coding		Malware-Detektierung & Klassifizierung

Flut der Möglichkeiten



Beispiel: wenn Lösungen nur punktuell greifen

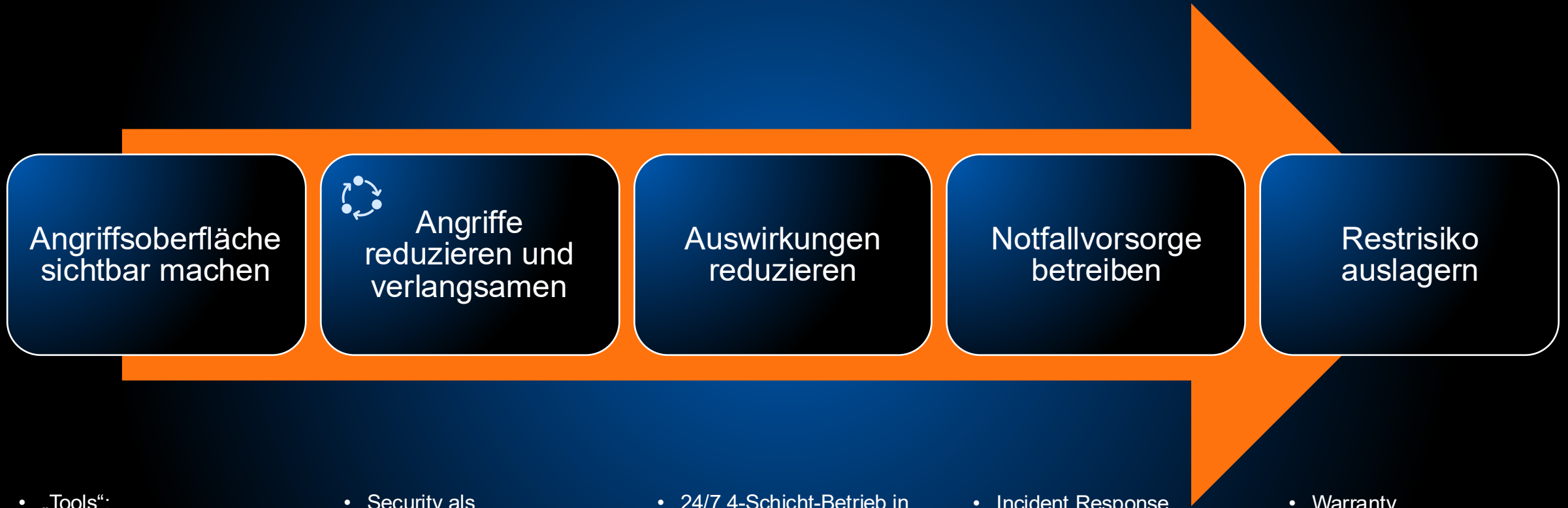


Richtige Priorisierung

Richtige Priorisierung

Wie ein MDR hilft (am Beispiel von Arctic Wolf)

“End Cyber Risk” mit dem Arctic Wolf SOC



- „Tools“:
- SIEM, SOAR
- Clients & Server
- Netzwerküberwachung
- Logs: AD, M365, Firewall, etc
- Evtl. Schwachstellenscanner

- Security als kontinuierlichen Verbesserungsprozess etablieren
- Consulting durch Concierge Team
- Systemhärtung

- 24/7 4-Schicht-Betrieb in Frankfurt
- Monitoring & Reaktion
- Zusammenarbeit mit deutschsprachigen Analysten

- Incident Response
- Forensik
- Planungstools

- Warranty
- Versicherbarkeit

Nutzen eines SOC

DWELL TIME

0:23

Durchschnittliche Zeit der Erkennung einer Intrusion beträgt 206 Tage. Arctic Wolf: 23 Minuten.

TIME OF ATTACKS

40%

Aller Bedrohungen werden zwischen 20:00 und 8:00 Uhr festgestellt

ADVANCED THREATS

62%

Aller Kunden hatten Advanced Threat Aktivitäten, welche nicht durch existierende Security Tools erkannt wurden

ACCOUNT TAKEOVER

54%

Aller Kunden hatten veröffentlichte Credentials zur Zeit des Onboardings

UNPATCHED VULNERABILITIES

20%

Reduktion in benötigter Zeit, um kritische Schwachstellen zu patchen

AWARENESS

90%

Reduktion in erfolgreichen Phishing-Attacken bei Kunden mit regelmässigem Awareness-Training

Q&A