

# Alarmflut, Fachkräftemangel, fehlende Controls – so hilft MDR

# Agenda

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



# Alexander Schmidt

[alexander.schmidt@arcticwolf.com](mailto:alexander.schmidt@arcticwolf.com)

[linkedin.com/in/alexander-schmidt-arcticwolf](https://www.linkedin.com/in/alexander-schmidt-arcticwolf)



# Felix Guggenheim

[felix.guggenheim@arcticwolf.com](mailto:felix.guggenheim@arcticwolf.com)

[www.linkedin.com/in/fguggenheim](https://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



When CISO asks for CHF 100K to increase cybersecurity posture

When hacker asks for CHF 10M ransomware



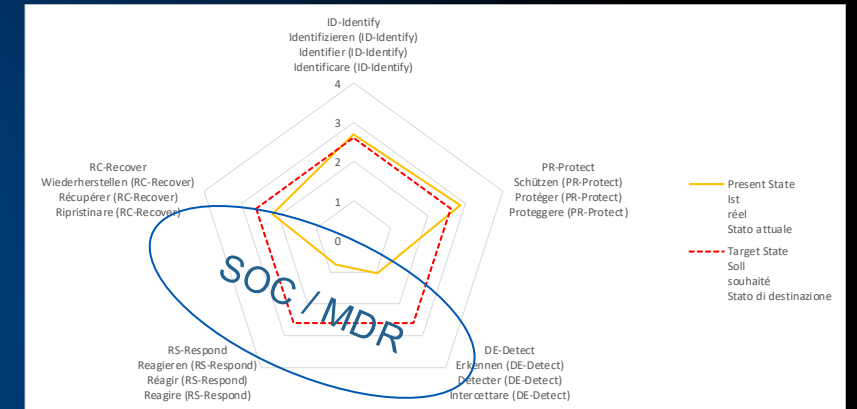
# Empfehlungen der Behörden

## IKT-Minimalstandard und CSRМ – 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<sup>50</sup> und im Hinblick auf möglicherweise erfolgte Angriffe möglichst zeitnah und automatisiert ausgewertet werden (z. B. im Rahmen eines SOC).

CSRМ: 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 Schwachstellenmanagement



Cyber Incident Response



Cyber Security Awareness Training und Phishing-Kampagnen



System Härungsmassnahmen



Logging und Monitoring / Netzwerkschutz



Umgang mit End-of-life-Systemen




IT-Lieferkette



# 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 Engadina,*

## 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.

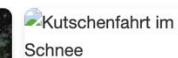
### 🎁 Winter-Sonderaktion:

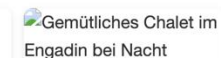
Genießen Sie **2 Übernachtungen zum Preis von 1!**

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**

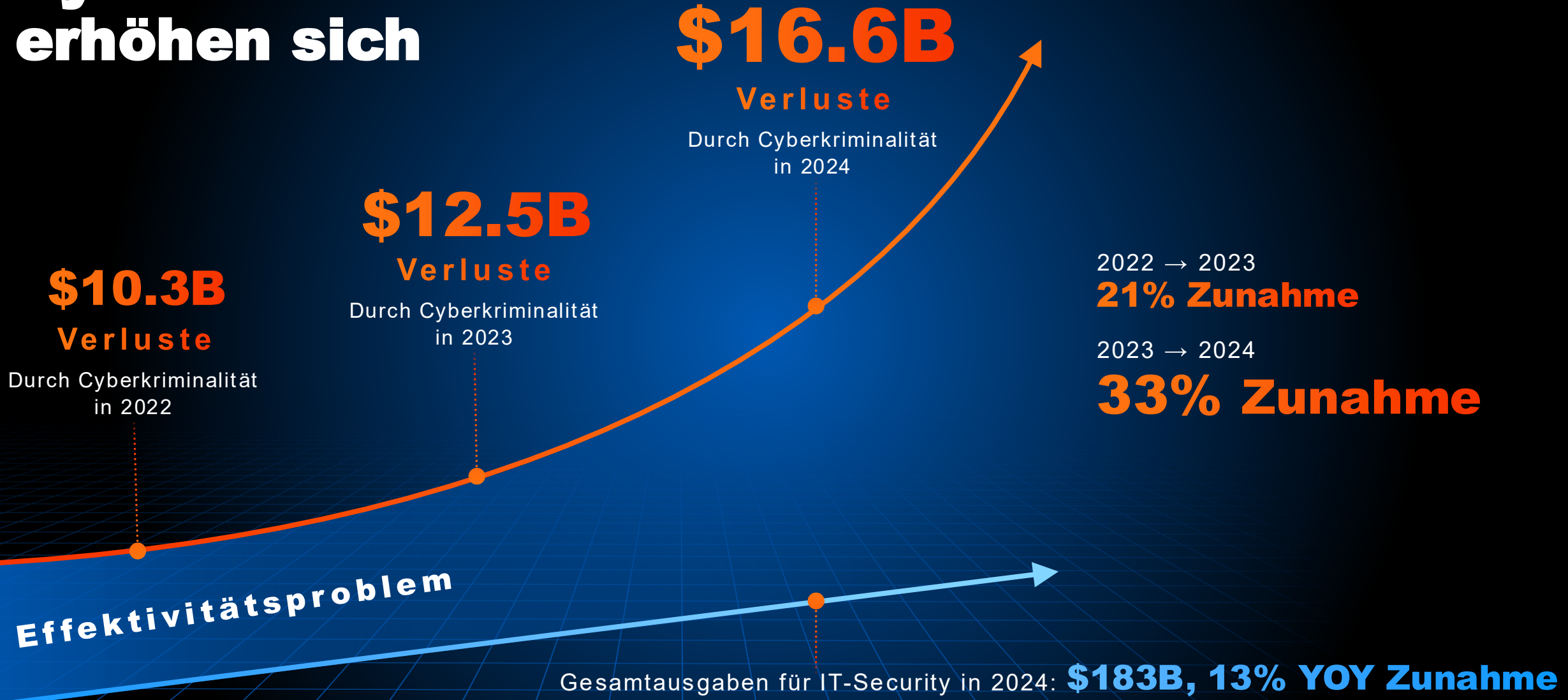
Ihr *Engadin Winterdreams Team*

Engadin Winterdreams AG · Via Muntanella 12 · 7500 St. Moritz  
+41 81 555 77 33 · [info@engadin-winterdreams.ch](mailto:info@engadin-winterdreams.ch)  
[Instagram](#) · [Facebook](#)

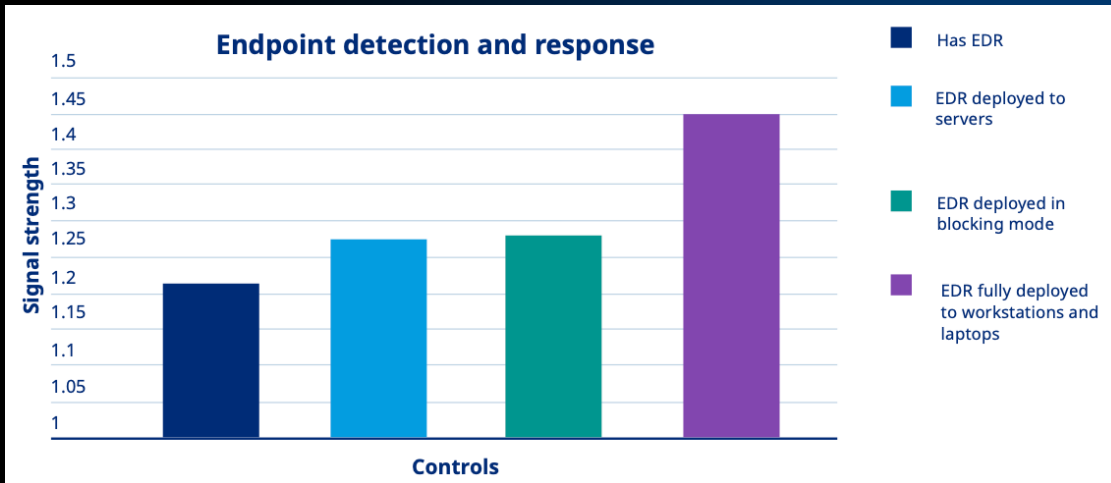
Fotos: Unsplash & Pixabay – frei verwendbar



# Cyber Risiken erhöhen sich



# EDR



Marsh: Connecting controls and incident outcomes, 2025

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

## 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

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





Generatives Phishing &  
Social Engineering



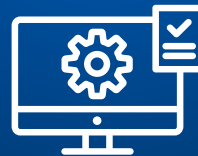
AI und Phishing  
Pattern Erkennung

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





# Beispiel: wenn Lösungen nur punktuell greifen

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (5)	Delay Execution	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Email Bombing
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Deploy Container	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Websites/Domains (3)	Valid Accounts (4)	Trusted Relationship	Native API	Event Triggered Execution (18)	Escape to Host	Direct Volume Access	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)	Hide Infrastructure	Scheduled Transfer	Financial Theft
Search Threat Vendor Data	Wi-Fi Networks	Valid Accounts (4)	Poisoned Pipeline Execution	Exclusive Control	Event Triggered Execution (18)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites			Scheduled Task/Job (5)	External Remote Services	Exploitation for Defense Evasion	Domain or Tenant Policy Modification (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
			Serverless Execution	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Email Spoofing	OS Credential Dumping (8)	File and Directory Discovery		Proxy (4)	Non-Application Layer Protocol		Network Denial of Service (2)
			Shared Modules	Implant Internal	Hijack Execution Flow (12)	Execution Guardrails (2)		Group Policy Discovery		Remote Access	Non-Standard Port		Resource Hijacking (4)
			Software Deployment Tools	Process Injection (12)	Hide Artifacts (14)	Exploitation for Defense Evasion		Local Storage Discovery			Protocol Tunneling		Service Stop
						File and Directory Permissions Modification (2)		Log Enumeration					System Shutdown/Reboot
						Hide Artifacts (14)		Network Service Discovery					



# Richtige Priorisierung



# Richtige Priorisierung



# Wie ein MDR hilft (am Beispiel von Arctic Wolf)

# “End Cyber Risk” mit dem Arctic Wolf SOC

Angriffsoberfläche  
sichtbar machen



Angriffe  
reduzieren und  
verlangsamen

Auswirkungen  
reduzieren

Notfallvorsorge  
betreiben

Restrisiko  
auslagern

- „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