

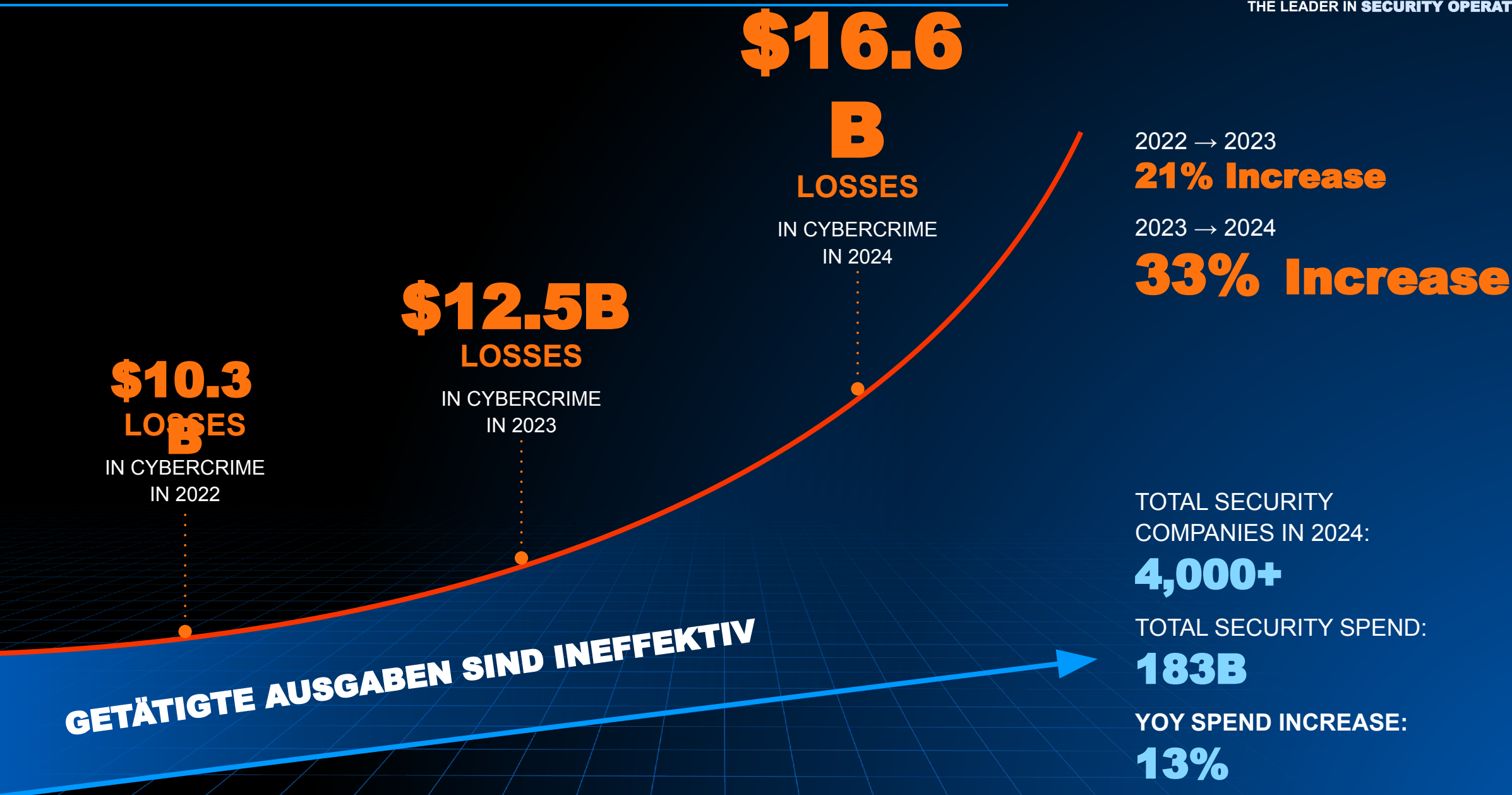


SOC selbst bauen oder kaufen? So vermeiden Sie teure Fehler



Felix Guggenheim

Sr. Solutions Engineer @ AWN
CISSP
[linkedin.com/in/fguggenheim](https://www.linkedin.com/in/fguggenheim)



Aktuelle Cyber Bedrohungen

Die meisten sind schwierig abzuwehren



Phishing



Leaked Passwords



Remote Work Exploitation



Zero-day Exploits



Business Email Compromise



Deepfakes & Identitätsdiebstahl



Ransomware Angriffe und
Double/Triple Extortion



Cloud Breaches / Takeovers

... Und viele weitere



Security Operations

Angestrebtes Sicherheitslevel

Security Operations **Lücke**

Die meisten Firmen stehen hier



BASIS

Passwörter / AD
Patch Management
Backups



PERIMETER

Firewalls
SPAM / Web Filters
WAF / Proxy



VERTEIDIGUNG IN DER TIEFE

Endpoint (NGAV, EDR)
DLP / SSL Inspection
Anti-DDoS / IPS / CASB



IDENTIFIZIEREN



SCHÜTZEN



ERKENNEN



REAGIEREN



WIEDERHERSTELLEN



WIDERSTANDS-FÄHIGKEIT

Proaktiv

Versicherbar

Konform (ISO, TISAX, KRITIS, NIS2, IKT, usw)





Security Operations

Angestrebtes Sicherheitslevel

Security Operations

Lücke

Die meisten Firmen stehen hier



WIDERSTANDS-FÄHIGKEIT

Proaktiv

Versicherbar

Konform (ISO, TISAX, KRITIS, NIS2)

SYSTEME ZUR ANGRIFFSERKENNUNG / DETECT&RESPOND

Protokollierung

Detektion

Reaktion

VERTEIDIGUNG IN DER TIEFE

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

PERIMETER



Firewalls

SPAM / Web Filters

WAF / Proxy



BASIS

Passwörter / AD

Patch Management

Backups



Systeme zur Angriffserkennung

Doch wieder nur ein neues Tool?





AUGENSCHÄDEN
durch Betrachten
völlig überladener Slides



Beispiel IKT Minimalstandard: Detektion

2.4.1 Auffälligkeiten und Vorfälle (Anomalies and Events)

Stellen Sie sicher, dass Auffälligkeiten (abnormes Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden und potenzielle Auswirkungen des Vorfalls verstanden werden.

Bezeichnung	Aufgabe
DE.AE-1	Definieren Sie Standardwerte für zulässige Netzwerkoperationen und die zu erwartenden Datenflüsse für Anwender und Systeme. Managen Sie diese Werte fortlaufend.
DE.AE-2	Stellen Sie sicher, dass entdeckte Cybersecurity-Vorfälle hinsichtlich ihrer Ziele und ihrer Methoden analysiert werden.
DE.AE-3	Stellen Sie sicher, dass Informationen zu Cybersecurity-Vorfällen aus verschiedenen Quellen und Sensoren aggregiert und aufbereitet werden.
DE.AE-4	Bestimmen sie die Auswirkungen möglicher Ereignissen.
DE.AE-5	Definieren sie Schwellenwerte die für Vorfallswarnungen festgelegt sind.

2.4.2 Überwachung (Security Continuous Monitoring)

Stellen Sie sicher, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Intervallen überwacht wird, um einerseits Cybersecurity-Vorfälle zu entdecken und andererseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring/Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware entdeckt werden kann.
DE.CM-5	Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten entdeckt werden kann.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistern überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können.
DE.CM-7	Überwachen Sie Ihre Systeme laufend, um sicherzustellen, dass Aktivitäten/Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden.
DE.CM-8	Führen Sie Verwundbarkeitsscans durch.

Tabelle 29: Aufgaben DE.CM



“Das macht bei uns der Patrick!”



Beispiel NIS2: Systeme zur Angriffserkennung

Doch wieder nur ein neues Tool?

„Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme.“

§ 2 Absatz 9b BSIG

„Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.“

§ 8a Absatz 1a BSIG

- Protokollierung
- Detektion
- Reaktion

Siehe <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf>



Systeme zur Angriffserkennung

Orientierungshilfe: Was wird mindestens gebraucht?

Protokollierung

- Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden
- Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein. Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.
- Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.
- Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

Detektion

- Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.
- Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen.
- Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.
- Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.
- Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten

Reaktion

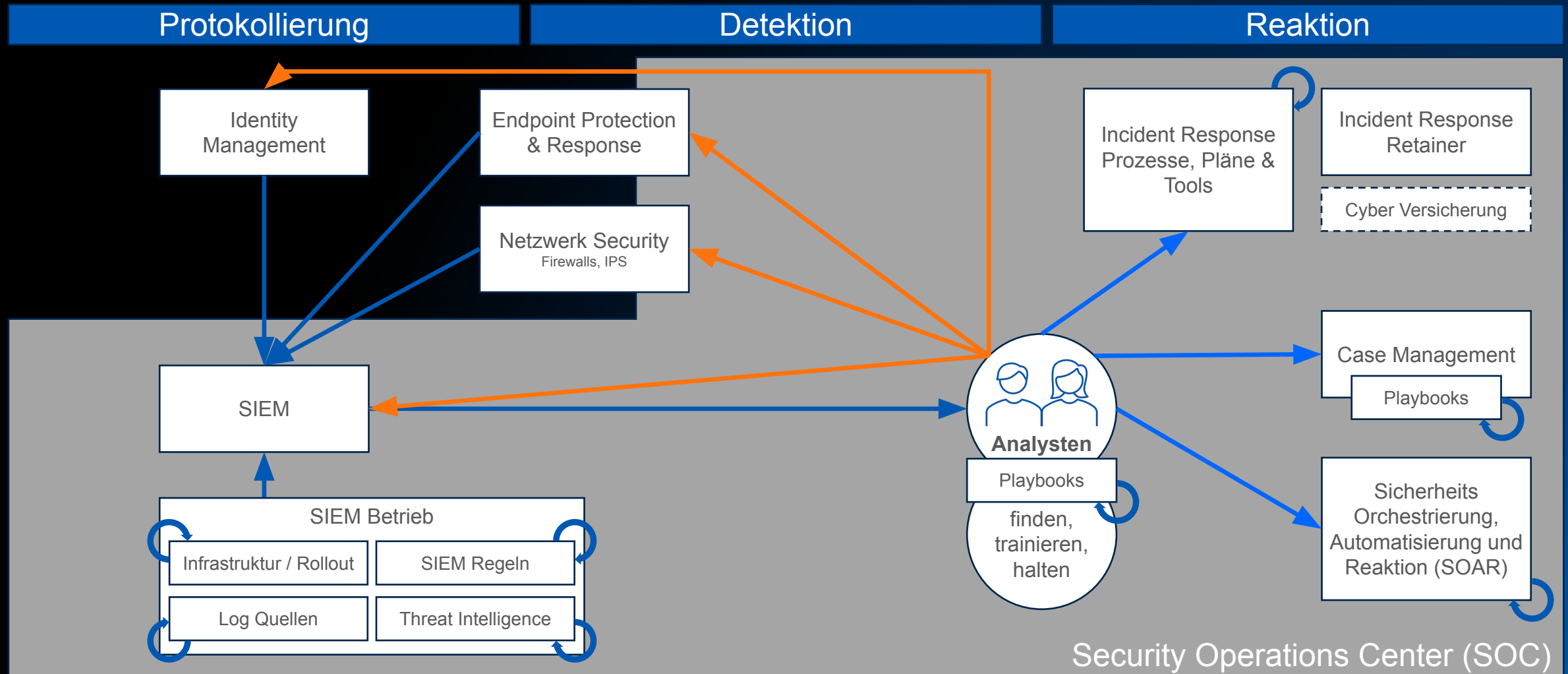
- Bei einem sicherheitsrelevanten Ereignis MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.
- Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.

Siehe: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf>



Was brauchen Sie konkret

Eine nicht abschliessende Übersicht



Typische Probleme beim Aufbau eines SOC

1. Finden, Trainieren und Halten der SOC Analysten
2. SOC Betrieb nur von Montag bis Freitag – Schichten vs Pikett
3. Fehlende Befugnisse und Beratungsgewalt des SOC
4. Unterschätzen des Aufwands den SOC in den vorhandenen Stack und die Prozesse zu integrieren
 - Technologische Integrationen
 - Prozess Integrationen
5. Unterschätzen des Aufwands für die Feinabstimmung der Analyse
 - Verheddert in Details
 - Einfaches Monitoring vs. 100% Abdeckung der Kronjuwelen
6. Mangel an Threat Intelligence Informationen
7. Nur auf Vorfälle ausgerichtete Arbeit, ohne Folgemaassnahmen und proaktive Sicherheitsverbesserungen
8. Konzentration auf punktuelle Lösungen und Vertrauen in das Marketing der Security Hersteller
- ...
999. Der Glaube, dass Machine Learning und KI alle oben genannten Probleme löst



KI&ML kann den Menschen noch nicht ersetzen

Cow
Height: 1.7 meter
Length: 5.2 meter

Search: cheese not sticking to pizza

All Images Videos Forums Shopping News We

★ AI Overview Learn more

Cheese can slide off pizza for a number of reasons, including too much sauce, too much cheese, or thickened sauce. Here are some things you can try:

- Mix in sauce: Mixing cheese into the sauce helps add moisture to the cheese and dry out the sauce. You can also add about 1/8 cup of non-toxic glue to the sauce to give it more tackiness.
- Let the pizza cool: The cheese will settle and bond

95%



Aber sie kann ihn effizienter machen!

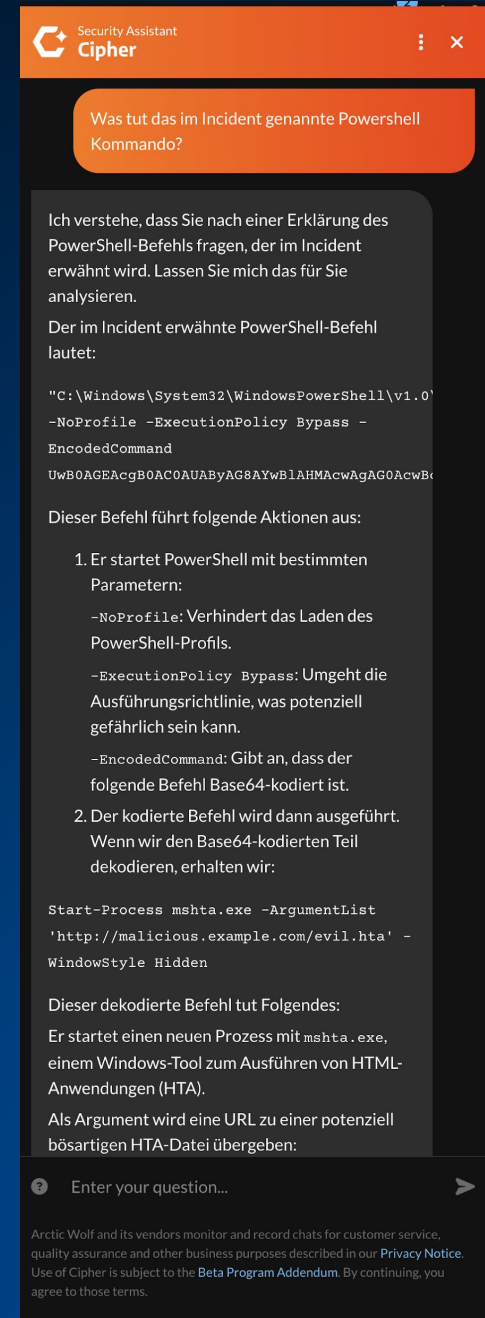
Kein Analyst kann alles wissen

Informationen zur richtigen Zeit, am richtigen Ort

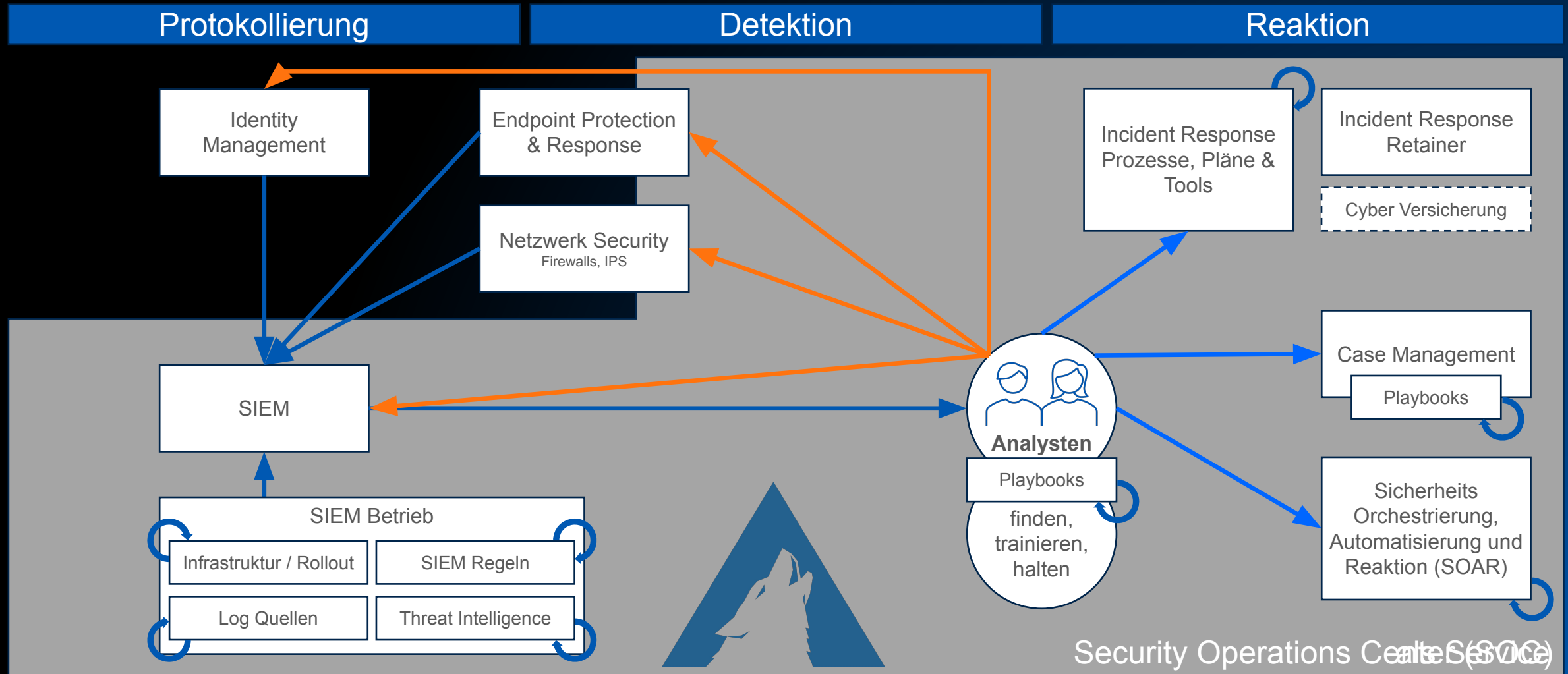
- CVE-Details
- Kommandoanlaysen
- Erläuterung typischer Remediation-Schritte
- Hersteller-spezifische Anleitungen zur Implementierung

Interaktion in natürlicher Sprache

- Generierung von Datenabfragen
- Dekodieren und Analyse von Artefakten



Wie sie viele Probleme umschiffen



Die Arctic Wolf Security Operations Cloud



Produkt



Service Ergebnis



Produkt



Service Ergebnis



Vielen Dank

