sure[secure]
your security operations center

secure mag

SOC im Einsatz für KRITIS

Die unsichtbare Rückgratgesellschaft

Intro

Ein Morgen ohne Strom, ohne Mobilfunknetz, ohne Trinkwasser. Kein Licht. Kein Kaffee. Kein Zugang zum Notruf. Was wie ein dystopischer Film klingt, ist gar nicht so weit entfernt, denn unsere Gesellschaft hängt an einer dünnen technischen Nabelschnur, die von den sogenannten kritischen Infrastrukturen gespeist wird.

KRITIS-Unternehmen sind das Rückgrat unseres Alltags.

Sie betreiben:

- Versorgungsunternehmen (Wasser-, Strom- und Gasnetze)
- Gesundheitswesen (z. B. Krankenhäuser und Labore)
- Transport und Verkehr
- Ernährung und Lebensmittelproduktion
- Informations- und Kommunikationstechnologien
- Zahlungsverkehr und Kommunikationsnetze
- Finanz- und Versicherungswesen

Ein Angriff auf diese Organisationen hat nicht nur für das Unternehmen selbst, sondern für uns alle Folgen. Und trotzdem: Viele dieser Unternehmen kämpfen mit veralteter Infrastruktur oder Technologie, Fachkräftemangel und zunehmendem regulatorischen Druck.

Was zählt als KRITIS?

In Deutschland ist dies in der BSI-Kritisverordnung (BSI-KritisV) auf der Grundlage des BSI-Gesetzes (BSIG) festgelegt. Je nach Branche gelten Schwellenwerte, beispielsweise nach Produktionsmenge oder Reichweite. Teilweise sind auch Dienstleister in der Lieferkette wie z.B. Security Provider betroffen. Die gesamte Liste der betroffenen Sektoren kann beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eingesehen werden:

BSI - Kritische Infrastrukturen

Doch die Regulierungen ändern sich rasant. Was gestern noch freiwillig war, ist morgen vielleicht schon Pflicht.

Gesetze, die keine Ausreden mehr zulassen

Spätestens mit dem IT-Sicherheitsgesetz 2.0 ist klar: Es geht nicht mehr um „sollte“, sondern um „muss“. Und der Druck steigt weiter, vor allem durch die neue NIS2-Richtlinie der EU, die bis Oktober 2024 in nationales Recht umgesetzt werden muss. Gut, das hat nicht ganz geklappt, aber im Laufe des Jahres 2025, spätestens 2026, wird es auch in Deutschland ein verabschiedetes NIS2-Umsetzungsgesetz geben. Hier folgt ein kurzer Überblick über die Regelwerke und ihre Differenzierung.

Die wichtigsten Regelwerke:

- BSI-Gesetz (BSIG): Das Grundgesetz für IT-Sicherheit in Deutschland mit Pflichten zu Mindeststandards, Meldewegen und Angriffserkennung.
- BSI-KritisV: Regelt konkret, welche Unternehmen als KRITIS gelten.
- IT-Sicherheitsgesetz 2.0 (seit 2021): Verschärft Anforderungen, z. B. durch verpflichtende Systeme zur Angriffserkennung und erweiterte Meldepflichten.
- NIS2-Richtlinie: Die EU legt nach. NIS2 betrifft deutlich mehr Unternehmen auch unterhalb der KRITIS-Schwelle. Neu sind z. B.:
    1. Meldepflicht binnen 24 Stunden
    2. Business-Continuity-Konzepte
    3. Cybersicherheitsverantwortliche auf Management-Ebene

Und dann wäre da noch das bereits geplante KRITIS-Dachgesetz, das den Fokus auf die physische Sicherheit legt - inkl. Zugangsschutz, Notfallplanung und Sicherheitskonzepten. Hierzu existiert bereits ein Gesetzesentwurf, der im Jahr 2025 ebenfalls verabschiedet werden soll.

Hier ein kurzer Überblick über die Regelwerke:

Regelwerk	Verpflichtend für Unternehmen	Kurzbeschreibung / Zielsetzung	Inkrafttreten	Anforderung für Früherkennung / Detektion
BSI-Gesetz (BSIG)	Ja, für KRITIS-Betreiber	Grundgesetz für die IT-Sicherheit in Deutschland; regelt Mindeststandards, Meldepflichten, Zusammenarbeit mit dem BSI	Erstversion: 2009 Aktuelle Fassung: 2021	Ja
BSI-Kritisverordnung	Ja, wenn Schwellenwerte erfüllt	Legt fest, welche Unternehmen als KRITIS gelten; sektorenspezifische Schwellenwerte	Erstversion: 2016 zuletzt aktualisiert: 2022	Ja
IT-Sicherheitsgesetz 2.0	Ja, für KRITIS & „Unternehmen im besonderen öffentlichen Interesse“	Erweiterung des BSIG mit Fokus auf Angriffserkennung, Bußgelder und Verpflichtung zu Systemen zur Angriffserkennung	In Kraft seit: Mai 2021	Ja
NIS2-Richtlinie (EU)	Ja, für „wesentliche“ und „wichtige Einrichtungen“	EU-weit harmonisierte Cybersecurity-Mindeststandards für deutlich mehr Unternehmen als zuvor (z. B. Zulieferer, Mittelstand)	Umsetzung bis: 17. Oktober 2024	Ja
KRITIS-Dachgesetz (geplant)	Geplant für alle KRITIS-relevanten Unternehmen	Vereinheitlichung der Sicherheitsanforderungen über alle KRITIS-Sektoren hinweg; Fokus auf physische und digitale Resilienz	Noch nicht verabschiedet (Entwurf 2024)	Voraussichtlich

Warum haben wir Früherkennung und Detektion in der Übersicht extra aufgeführt?

Es besteht ein kausaler Zusammenhang zwischen der Früherkennung von Cyberangriffen und dem daraus folgenden Schaden für das Unternehmen und damit für die Wirtschaft. Je länger ein Angreifer unbemerkt im Netzwerk aktiv sein kann, desto mehr Schaden richtet er in der Regel an.

Ist der Angreifer erst einmal in die Infrastruktur eingedrungen, richtet er sich dort ein und baut mehrere Einfallstore, sogenannte Backdoors, für den Fall, dass eine Tür sich schließt. Ist dies geschehen, kann er sich in Ruhe informieren und einen Plan schmieden, was er wann tun wird.

Deshalb: Wer keine Früherkennung, keine Notfallmechanismen und keine strukturierte Reaktion vorweisen kann, riskiert nicht nur Bußgelder, sondern das eigene Überleben.

Woran es in der Praxis oft scheitert

Trotz dieser Vorgaben bleiben viele KRITIS-nahe Unternehmen verwundbar, nicht aus Unwissenheit, sondern aus Überforderung. Die Bedrohungslage ist komplex, die Technik fragmentiert und die Ressourcen sind begrenzt.

Die fünf häufigsten Stolpersteine:

- **Fachkräftemangel:** Wer heute Cybersecurity-Analysten sucht, konkurriert mit Großkonzernen, Dienstleistern und Behörden.
- **Technische Altlasten:** Jahrzehnte alte Systeme, vor allem im OT-Bereich, lassen sich nicht mal eben patchen oder an ein modernes SOC anbinden.
- **Kostendruck:** Ein 24/7 Security Operations Center (SOC) selbst aufzubauen, ist wirtschaftlich meist nicht darstellbar.
- **Reaktionslücken:** Eine reine Alarmierung reicht nicht aus, es braucht Verantwortlichkeiten, etablierte Prozesse und Playbooks.
- **Überfordernde Compliance:** NIS2, BSI, ISO27001, IT-SiG - viele Mittelständler wissen nicht, wo sie anfangen sollen.

Ein CISO aus dem Energiesektor formulierte es einmal so:

„Wir sind verpflichtet, ein Schiff im Sturm zu steuern - ohne zu wissen, ob wir einen Kompass, ein Leck oder überhaupt eine Mannschaft haben."

Der Tag, an dem es zu spät war… Der Fall Eu-Rec

Die Eu-Rec GmbH, ein mittelständisches Recyclingunternehmen mit Sitz in Hermeskeil, Rheinland-Pfalz, wurde am 5. April 2025 Opfer eines schweren Cyberangriffs. Als Entsorgungsunternehmen mit dem Schwerpunkt Altpapier zählt das Unternehmen gemäß Branchendefinition zum KRITIS-Bereich. Die digitale Infrastruktur des Unternehmens wurde erheblich beschädigt, was zu massiven Störungen der betrieblichen Abläufe führte.

Bereits zuvor hatte Eu-Rec mit wirtschaftlichen Herausforderungen wie gestiegenen Energiepreisen und einer schwankenden Auftragslage zu kämpfen. Durch den Cyberangriff verschärfte sich die Situation jedoch so sehr, dass das Unternehmen schließlich beim Amtsgericht Trier einen Insolvenzantrag stellen musste.

Trotz der Insolvenz wird der Geschäftsbetrieb fortgeführt. Die Löhne der rund 50 Angestellten sind durch das Insolvenzgeld gesichert. Der vorläufige Insolvenzverwalter betonte, dass das Unternehmen über ein solides operatives Fundament, qualifiziertes Personal und etablierte Kundenstrukturen verfügt. Ziel des Insolvenzverfahrens ist klar. Es gilt, die wirtschaftlichen Rahmenbedingungen zu stabilisieren und gemeinsam mit der Geschäftsführung tragfähige Perspektiven für die Zukunft zu entwickeln.

Dieser Vorfall unterstreicht eindrücklich, wie wichtig eine robuste Cybersecurity-Strategie für Unternehmen ist, insbesondere für solche, die in kritischen Infrastrukturbereichen tätig sind.

„In einem SOC zu arbeiten heißt, Verantwortung für etwas zu übernehmen, das man nicht sehen kann - aber das jeder Mensch täglich braucht. Wir schützen kritische Infrastrukturen vor Angriffen, die oft im Verborgenen stattfinden. Es ist ein Job ohne Applaus, aber mit großer Wirkung."

Mohamed Abdelfattah, Senior SOC-Analyst, suresecure GmbH

Was man mit den richtigen Partnern absichern kann

Nicht jede Organisation muss selbst ein SOC betreiben. Viele Pflichten lassen sich durch Managed Services abdecken, ohne eigene Infrastruktur, ohne 24/7-Personal, ohne Compliance-Stress. Managed Detection and Response oder Managed SOC-Services sind echte Gamechanger in Sachen Cyber Resilience und Compliance. Denn hier kommen nicht nur Know-how, Technologie und Hardware schnell ins Unternehmen, sondern vor allem aber auch klare Prozesse, die so elementar sind, wenn es darum geht, der Früherkennung auch die richtigen Maßnahmen folgen zu lassen.

Typische Herausforderungen, die ein externer Dienst abfangen kann:

- Angriffsfrüherkennung in Echtzeit
- Rund-um-die-Uhr-Sicherheitsüberwachung (24/7)
- Sofortige Reaktion auf Vorfälle durch Playbooks & Incident Response
- Zentrale Dokumentation und Reporting für Audits
- Skalierbarkeit ohne Kapazitätsgrenzen

So können KRITIS-Unternehmen regulatorische Vorgaben wie § 8a BSIG oder NIS2 schneller und effizienter erfüllen und gewinnen zugleich etwas, das unbezahlbar ist: **Ruhe in der Nacht.**

Unser Managed SOC: Detektion mit Plan und Prinzip

Mit unserem ISO27001 zertifizierten Managed SOC „Made in Germany“ bieten wir genau das. Früherkennungssensorik, die nicht nur performant, sondern auch praxisnah und compliant istt.

Unser Fokus: Klarheit statt Komplexität. Geschwindigkeit statt Stillstand.

Das steckt drin:

- **24/7 Security Monitoring:** Unser Analystenteam erkennt Angriffe, bevor sie eskalieren, inklusive Alarmierung und Handlungsempfehlungen.
- **Threat Intelligence & KI-gestützte Erkennung:** Wir analysieren Bedrohungen auf Basis globaler Datenquellen und lernen kontinuierlich aus jedem Fall.
- **Reaktionspläne, die funktionieren:** Mit individuellen Playbooks und abgestimmten Prozessen sorgen wir dafür, dass keine Zeit verloren geht.
- **NIS2-Ready:** Unser Service erfüllt alle Anforderungen für Meldesysteme, Detektionspflichten und Risikomanagement.
- **DSGVO- und Audit-konform:** Vollständig dokumentiert, transparent, revisionssicher.
- **Volle Kontrolle trotz Auslagerung:** Das Unternehmen behält die Entscheidungshoheit, wir liefern die fundierte Lageeinschätzung.

Der perfekte Mix aus **People, Prozessen und einer skalierbaren Architektur** ist entscheidend für den richtigen Output und die Wirtschaftlichkeit eines Security Operations Centers. Dann habe ich ein interdisziplinäres Team, das 24x7 mit klaren Abläufen und Eskalationsstufen sowie einem hohem Automatisierungsgrad dafür sorgt, dass die skalierbare Architektur mit SIEM und SOAR die IT-Infrastruktur optimal schützt.

Bei der suresecure ist das SOC im FOCUS.

Interdisziplinär bedeutet, alle benötigten Expertisen mindestens doppelt zu besetzen. Unser SOC-Team besteht aus:

- **Platform Engineers:** Egal welche Plattform es ist: Wartung, Entwicklung und Automatisierung sind elementare Bestandteile, um kontinuierlich an der Effizienz zu arbeiten.
- **Incident Analysts:** Wenn das SOC anschlägt, dann muss sichergestellt sein, dass der Vorfall auch fachlich korrekt und gründlich aufgearbeitet wird. Nachlässigkeiten können schnell auch Fahrlässigkeit bedeuten. Incident Analysten verfügen über Wissen von APT-Angriffen, Spionage und weiteren komplexen Angriffsmustern.
- **SOC-Analysts:** Alles, was die Technologie nicht automatisch klären kann, wird manuell untersucht. Das ist wichtig, denn nicht alles lässt sich durch Automatisierung lösen. Sie ist zwar leistungsstark und deckt den Großteil ab, doch es gibt immer wieder Anomalien, die einer intensiven Prüfung bedürfen.
- **Detection Engineers:** Wenn ein SOC effizient arbeiten soll, dann braucht es exzellente Detection Engineers. Hier wird an der Automatisierung gearbeitet. Playbooks und Detection Rules werden programmiert und ausgerollt, um die individuellen Bedürfnisse der Infrastrukturen zu berücksichtigen. So sind die Detection Rules immer auf dem neusten Stand und das Unternehmen dadurch noch besser geschütz.
- **Incident Manager:** Bei einem Sicherheitsvorfall übernimmt der Incident Manager die Leitung. Er koordiniert den gesamten Einsatz und ist dafür verantwortlich, die Betriebsfähigkeit des Unternehmens schnellstmöglich wiederherzustellen. Besonders entscheidend sind die ersten Stunden nach der Identifizierung des Vorfalls. In dieser Phase müssen die richtigen Entscheidungen schnell und konsequent getroffen werden, um Folgeschäden zu verhindern.
- **Consultants:** Da mit einem SOC die Infrastruktur überwacht wird, ist es unabdingbar, dass sich Security Consultants regelmäßig Optimierungspotenziale anschauen. Gibt es irgendwo Blind-Spots, die angebunden werden sollten? Eine Infrastruktur ist immer dynamisch, weshalb auch die Security Infrastruktur nachgezogen werden muss.
- **Customer Success Manager.** Was ist ein Service wert, der sich nicht gut anfühlt? Wir haben ein Team von Customer Success Managern, die im ständigen Austausch mit den Unternehmen dafür sorgen, dass alles so läuft, wie es soll. In regelmäßigen Review-Meetings werden die Ergebnisse aus dem SOC aufbereitet und verständlich erklärt. Gleichzeitig gibt es die Gelegenheit für konsequente Feedbackschleifen

Das SOC-Team der suresecure sorgt für die Sicherheit zahlreicher namhafter Unternehmen und wird kontinuierlich punktuell verstärkt. Schulungen und Weiterbildungen sind für alle Teammitglieder verpflichtend, sodass auch neue Themen wie z. B. AI-Security direkt integriert werden können. Denn wenn wir eines ganz sicher nicht wollen, dann sind es erfolgreiche Cyberangriffe, unabhängig vom betroffenen Bereich. Dafür benötigen wir die passenden Technologien und sind stolz darauf, einer der wenigen Google Security Partner zu sein. Wir setzen auf Google SecOps..

Was ist drin im SOC-Service und wie funktioniert er?

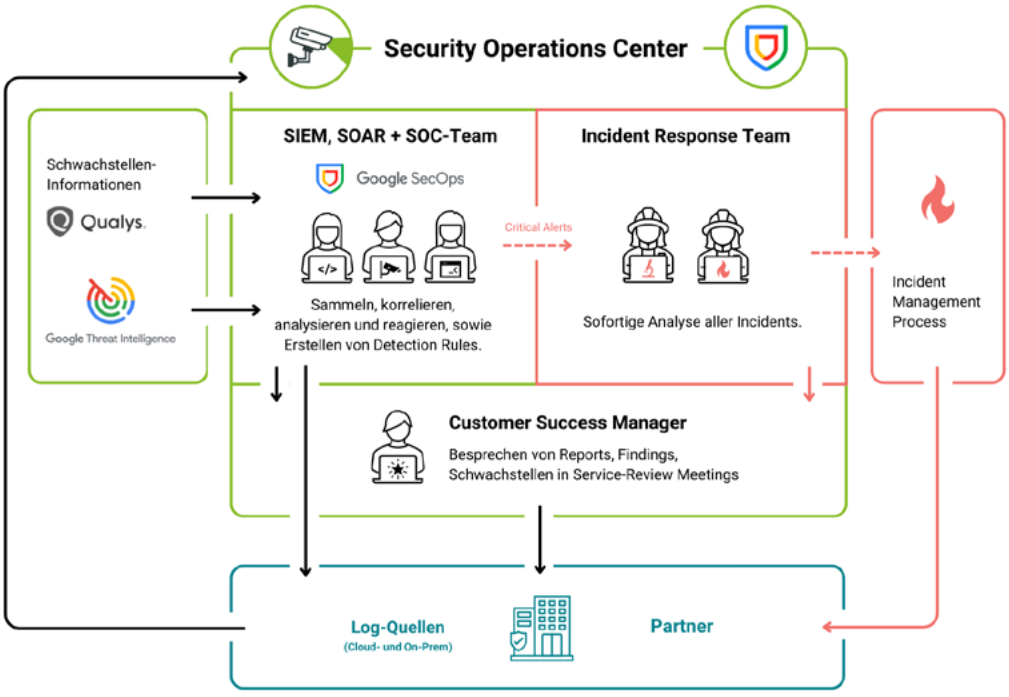
Unser SOC hat einen hohen Reifegrad erreicht und setzt auf eine Cloud-native Lösung von Google. Wenn Google etwas beherrscht, dann ist es die Suche und Korrelation von Daten. Zudem ist Google als Hyperscaler der ideale Partner für sämtliche Skalierungsmöglichkeiten. Genutzt werden das Security Event and Information Management System (SIEM), das Security Orchestration, Automation and Response (SOAR) Tool sowie Google Threat Intelligence (GTI).

Schauen wir uns die Begriffe kurz an.

- **SIEM:** Sammelt die Logs der relevanten und angebundenen Log-Quellen ein und korreliert diese, sodass die Daten nutzbar werden. Auf dieser Basis können dann Analysen durchgeführt werden. Anbinden lassen sich nahezu alle Log-Quellen. Per Standard können mehr als 300 Cloud-Log-Quellen und über 2.000 On-Prem Quellen via Parser schnell und effizient angebunden werden.
- **SOAR:** Führt automatisierte Reaktionen auf bestimmte Detections aus, wodurch Sicherheitsvorfälle schneller bearbeitet und manuelle Eingriffe reduziert werden. Dadurch gewinnt das SOC erheblich an Effizienz und kann Bedrohungen schneller eindämmen.

Zusätzlich verfügt unser SOC-Service über einen **integrierten Schwachstellen-Scanner**, der kontinuierlich kritische Schwachstellen automatisch erkennt und diese wichtigen Erkenntnisse an das SOC-Team übermittelt. Dort landen die Events, die nicht automatisiert gelöst werden können. Sollte sich darunter ein kritisches oder auffälliges Event befinden, wird es per Eskalation an das Incident Response Team weitergeleitet, und wenn nötig wird der Incident Management Prozess eingeleitet. Der Partner wird umgehend über diesen Prozess informiert und ist sofort auf dem neuesten Stand.

Diese Prozesse sind ein ganz wichtiger Faktor für den Mehrwert eines SOCs. Das SOC-Team lebt aber nicht nur von Partner-Daten und dem Schwachstellen-Scanner.



Google Threat Intelligence

Wir arbeiten mit Google Threat Intelligence, der derzeit größten Cybersecurity-Datenbank der Welt. Durch die Zukäufe von Mandiant und Virustotal verfügt Google über ein immenses Know-how im Bereich der Bedrohungsanalyse. Dies wird zusätzlich angereichert mit mehreren Milliarden Daten aus den Nutzerdaten von Google Chrome. So werden unter anderem täglich Millionen von maliziösen Webseiten blockiert. Google verfolgt dabei ein klares Credo, das wir leicht ergänzt und erweitert haben:

Detect Everything → Trust nothing → Know, what Google knows

Denn Google weiß bekanntlich verdammt viel, aber wir sagen: „Know, what Google & suresecure know“. Alle Erkenntnisse, die wir in Incidents sammeln, fließen per Prozess wieder in unsere Detection Rules ein. Das bedeutet, dass unsere SOC-Partner zusätzlich unser spezifisches Wissen über neue Angriffsmuster und deren Erkennung in Form von sogenannten Indicators of Compromise (IOCs) erhalten.

Neben der Datenbank liefert Google Threat Intelligence:

- **Digital Threat Monitoring:** Monitoring des DarkNets nach Credentials oder sonstigen Datenleaks
- **Attack Surface Management:** Ein ebenfalls automatisierter Scan gegen alle von außen erreichbaren digitalen Assets. Dadurch ergibt sich ein klares Bild über die eigene Angriffsfläche und gibt Ansätze, diese zu reduzieren.
- **KI-Unterstützung:** Die künstliche Intelligenz aus dem Hause Google - Hi. I’m Gemini -unterstützt im Hintergrund, um die Erkennung und Abwehr von Cyberbedrohungen zu verbessern.

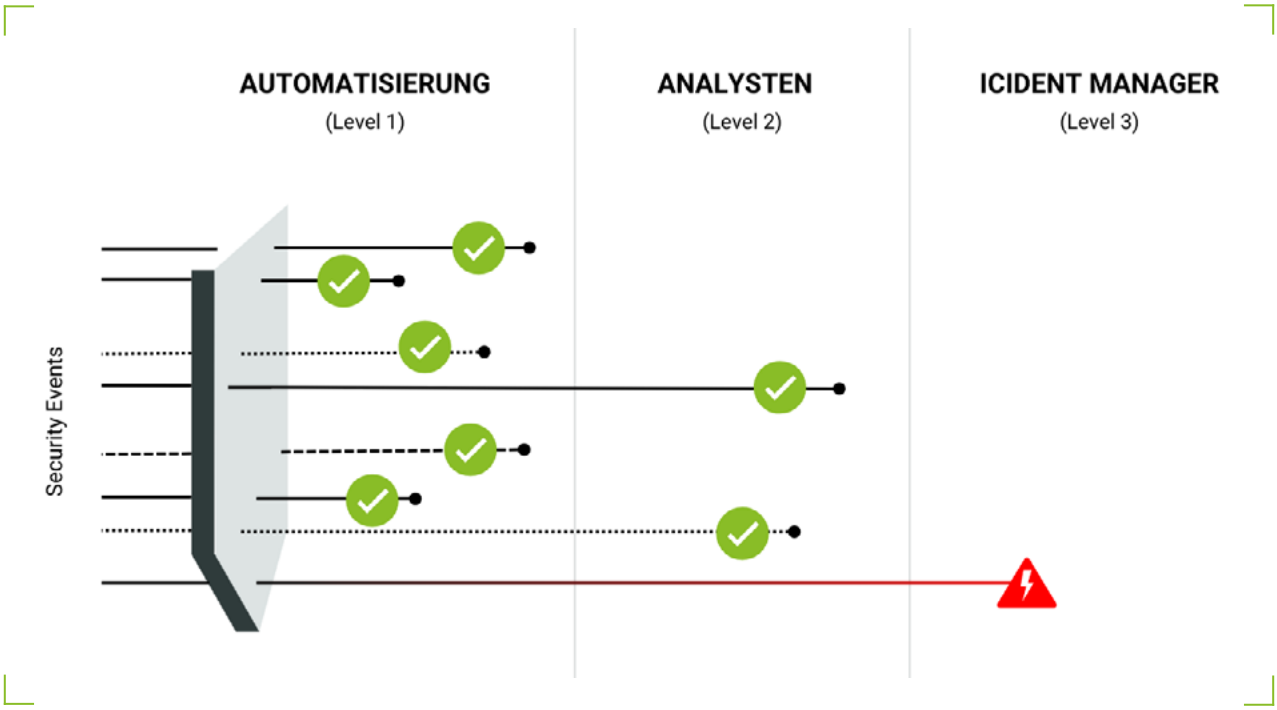
All diese Features bringen aber gar nichts ohne eine prozessuale Einbindung. Und Prozesse werden oftmals unterschätzt. Wir lieben Prozesse.

Foto: Philip Schildein (Head of Cyber Defense Center), Jona Ridderskamp (CEO) und Philip Hetkamp (Head of Consulting)

Prozesse sind für uns eine Herzensangelegenheit

Hier schlägt die Effizienz: Standards und Prozesse sorgen für konstante Qualität, die bei einem so sensiblen Service unerlässlich ist. Denn nichts ist wichtiger, als für die Cybersicherheit eines Unternehmens Verantwortung zu tragen. Dazu gehört nicht nur die Definition klarer Eskalationsstufen, sondern auch ein hoher Grad an Automatisierung durch Detection Rules und Playbooks. Der Aufbau einer solchen Konstrukts erfordert vor allem Erfahrung.

Und für den Fall der Fälle überführen wir die SOC-Prozesse direkt ins Incident Management, was bei uns weit über die Forensik hinaus geht.



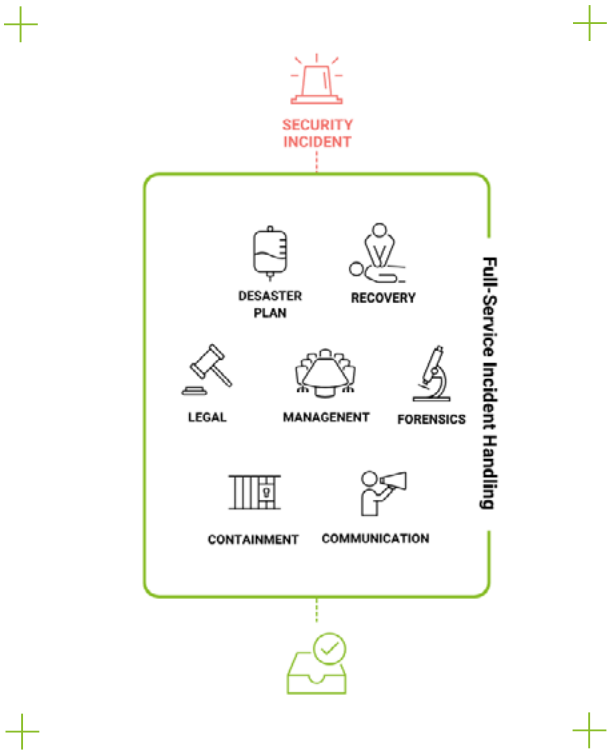
Incident Management ist integriert

Die Bewältigung eines Sicherheitsvorfalles geht weit über die Ergreifung technischer Maßnahmen hinaus. Neben tiefgehender technischer Expertise müssen auch Aspekte wie Kommunikation und rechtliche Vorgaben berücksichtigt werden, da hier schwerwiegende Fehler begangen werden können.

Es gibt Meldepflichten mit strengen Fristen, Informationspflichten gegenüber Betroffenen und einen vorgeschriebenen Umgang während der forensischen Analyse. Zudem müssen auch weitere Parteien, wie etwa die Cyberversicherung, umgehend informiert werden. All diese Faktoren erfordern eine koordinierte und gut strukturierte Reaktion, um den Vorfall effektiv zu bewältigen.

In einer Notsituation ist es schwierig, all diese Aspekte im Blick zu behalten. Deshalb bieten wir unseren Incident Retainer mit einem Service-Level-Agreement an, das eine 2-stündige Reaktionszeit und den Anspruch auf Vollständigkeit garantiert. Wir steuern nicht nur den Krisenstab, sondern stellen auch Expertisen für die Krisenkommunikation zur Verfügung. Darüber hinaus wissen wir genau, welche Behörden wir wann und auf welche Weise kontaktieren müssen, um eine schnelle und effiziente Reaktion zu gewährleisten.

Noch während wir die Erstinformation für die Mitarbeitenden abstimmen, beginnt in einem anderen Workstream bereits die Planung zur Wiederherstellung der Infrastruktur. Viele verschiedene Workstreams werden vom Incident Manager täglich koordiniert und dokumentiert. Das ist unser Verständnis einer ganzheitlichen Betreuung in einem Sicherheitsvorfall und genau das bietet unser SOC-Service.



Mit diesem Setup werden Cyberangriffe nicht nur frühzeitig identifiziert, sondern wirklich auch effizient abgewehrt.

Onboarding

Wir akzeptieren es nicht, dass Onboardings lange dauern. Daher investieren wir erheblich in die Optimierung der Abläufe. Vom ersten Tag an, an dem sich ein Partner für uns entscheidet, stellen wir einen Transition Manager bereit, der sicherstellt, dass das Onboarding reibungslos verläuft.

Unser Ziel ist es, eine langfristige Partnerschaft aufzubauen. Service Provider im Security-Sektor und Unternehmen brauchen eine Vertrauensbasis, die nur durch Transparenz und Kompetenz geschaffen werden kann.

Nach der Beauftragung beginnen wir sofort, alle relevanten Informationen für das Onboarding bereitzustellen. Dabei benötigen wir auch erste Informationen vom Partner. Bereits nach etwa einer Woche findet das Kick-Off statt, in dem wir uns über die gegenseitigen Erwartungen austauschen. Denn zur Wahrheit gehört, dass wir während des Onboardings auf die Zusammenarbeit und Zuarbeit des Partners angewiesen sind.

Wir benötigen unter anderem:

- Einen dedizierten Ansprechpartner für das Projekt
- Ressourcen in Form von Zeit für die technische Umsetzung
- Systembezogene Zugänge und Passwörter
- Enge, projektbegleitende Abstimmung

Wenn das alles gegeben ist und keine Komplikationen auftreten, geht unser Service bereits nach 4 Wochen live. Im Anschluss werden noch letzte Aufgabenpakete abgeschlossen und die vollständige Überwachung durch unser SOC ist nach spätestens 6 Wochen in place.

Unser SOC - ohne Kompromisse:

- Automated Response (SOAR)
- Standard Sources
- Cyberaudit
- Incident Response
- suresecure Detection Rules
- Incident Drill
- Customer Success Manager
- Attack Surface Monitoring
- SIEM
- Vulnerability Management
- Security Advisory

Google Security Operations

Google Threat Intelligence

Schlusswort: Verteidigen, was zählt

Kritische Infrastrukturen schützen nicht nur Systeme, sondern auch das, was uns als Gesellschaft zusammenhält: Versorgung, Sicherheit, Vertrauen.

KRITIS-Unternehmen stehen im Fadenkreuz moderner Angreifer - aber sie müssen dort nicht alleinstehen. Wer sich strategisch absichert, kann gesetzliche Pflichten nicht nur erfüllen, sondern auch **Widerstandsfähigkeit und Zukunftssicherheit gewinnen**.

Wir nennen das: **digitale Verteidigungsfähigkeit**.

Weitere Informationen zum Thema:

Podcast-Folge:

Detection Rules im SOC: Ein Blick unter die Motorhaube

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de