sure[secure]
your security operations center

secure mag

SOC im FOCUS
Was ist drin im SOC-Service und wie funktioniert er?
(Seite 5+6)

Incident Management
Sicherheitsvorfälle professionell und rechtssicher bewältigen.
(Seite 9)

Onboarding in Google-Geschwindigkeit
Effizient und schnell zur erfolgreichen Partnerschaft
(Seite 10)

your

Security Operations Center

Wie wir die Cyberwelt jeden Tag ein Stück sicherer machen!

Warum, wieso, weshalb und wie eigentlich?

Im Jahre 2024 sind Cyberangriffe zum dritten Mal in Folge das weltweit größte Geschäftsrisiko. Die Unvorhersehbarkeit und der Impact sind unvergleichlich hoch und haben Unternehmen schon an den Rand der Insolvenz geführt.

Umso wichtiger ist es als Gesellschaft eine starke digitale Resilienz aufzubauen. Diese wird nun durch die Europäische Union eingefordert. Jedes Land setzt die EU-Richtlinie NIS2 im Jahr 2024 in ein nationales Gesetz um. In Deutschland wird es 2025 und ab dann läuft die Frist zur Umsetzung der deutlich stärkeren Auflagen im Bereich Security.

Die frühzeitige Erkennung und Abwehr von Cyberangriffen ist ein Schlüsselelement zur Risiko- und Schadensminderung. Das ist nicht trivial, da neben Technologien auch Expertise, funktionierende Prozesse und eine 24x7 Überwachung etabliert sein müssen.

Es braucht also einen strategischen Ansatz, um hier die Ressourcen effizient zur Zielerreichung einzusetzen. Eine der wirkungsvollsten Maßnahmen ist das Etablieren oder der Einkauf eines Security Operations Center Services.

Was denn nun? Make or Buy?

Pauschal ist das nicht zu beantworten. Es hängt immer von den Rahmenbedingungen ab. Zu Beginn muss klar definiert sein, welche Anforderungen und Ziele das SOC erfüllen soll. Entscheidende Faktoren, die den Entscheidungsprozess unterstützen können, sind:

- **Kosteneffizienz:** Wenn es einzig darum geht SIEM-Lizenzen zu kaufen, ist das nicht sonderlich aufwendig. Aber in der Regel ist das nicht ausreichend, um die Zieldefinition zu treffen. Denn ich brauche Personal, welches mit den Tools auch arbeiten kann. Je nach Gestaltung ist ein Basis-Setup nach Best-Practice mit mindestens 7-10 Mitarbeitenden zu besetzen. Es müssen unterschiedliche Expertisen, Schichtbetrieb und Vertretungsregelungen beachtet werden.

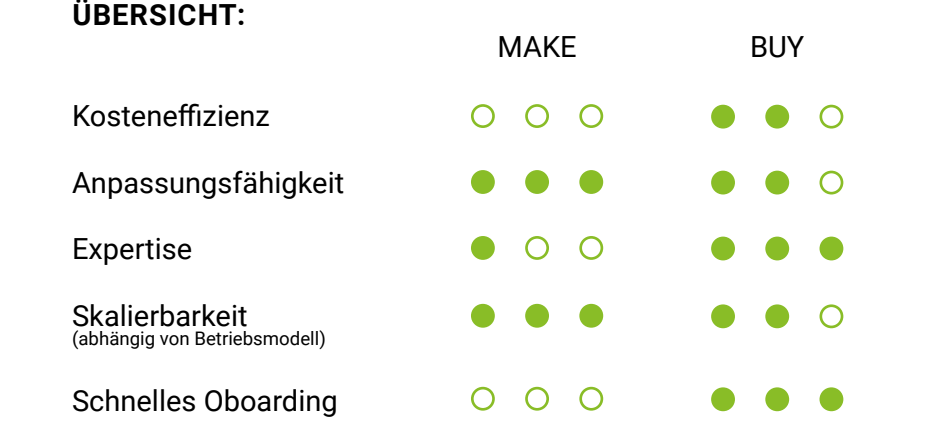
- **Anpassungsfähigkeit:** Volle Kontrolle und vollen Einfluss auf die Technologie, die Systeme und das Personal habe ich bei der MAKE-Variante. D. h. ich kann das SOC frei gestalten, während ich bei einem Service-Provider an gewisse Standards gebunden bin, die der Dienstleister vorgibt. In diesem Szenario muss ich das Leistungsangebot des Dienstleisters akzeptieren und kann ggf. nur auf Nuancen wie Dashboards oder Reporting Einfluss nehmen.

- **Expertise:** In diesem Bereich ist die Rekrutierung von Fachkräften nicht einfach, vor allem wenn ich nicht ein Mindestmaß an üblichen Benefits wie z. B. Home-Office, flexible Arbeitszeiten oder Weiterbildungsprogramme anbieten kann. SOC-Fachkräfte sind gefragt.

- **Skalierbarkeit:** In beiden Fällen ist die Skalierbarkeit gewährleistet. Ein wichtiger Hinweis -> Eine On-Prem-Lösung erfordert bei steigendem Volumen eine sukzessive Nachrüstung der Hardware, was zusätzliche Ressourcen und Kosten mit sich bringt.

- **Timeline:** Wenn es dringend ist, ist die MAKE-Option tatsächlich keine Option. Es sei denn, es gibt schon ausreichend Fachkräfte im Hause, die für solche Tätigkeiten in Frage kommen. Das Onboarding bei einem spezialisierten Provider erfolgt in der Regel innerhalb weniger Wochen.

ÜBERSICHT:



Beispielrechnung

Ein mittelständisches Unternehmen – MAKE-Option – Kosten pro Jahr:

Anzahl Mitarbeitende:	2.500
Branche:	Produzierendes Gewerbe
10 FTE + Nebenkosten + Fortbildung:	1.300.000 €
Lizensierung, Infrastruktur, Software:	200.000 €
Prozessaufbau, Zertifizierung usw.:	80.000 €
Gesamtkosten:	**1.580.000 €**

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 hohem Automatisierungsgrad dafür sorgt, dass die skalierbare Architektur mit SIEM und SOAR die IT-Infrastruktur optimal schützt.

Foto: Mohamed Abdelfattah - Senior SOC-Analyst

Bei uns 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:** Es braucht exzellente Detection Engineers, wenn ein SOC effizient arbeiten soll. Es wird an der Automatisierung gearbeitet, Playbooks und Detection Rules werden programmiert und ausgerollt, um die individuellen Ansprüche der Infrastrukturen zu berücksichtigen. So sind die Detection Rules immer auf dem neusten Stand und das Unternehmen dadurch noch besser geschützt.
- **Incident Manager:** Der Incident Manager übernimmt die Leitung bei einem Sicherheitsvorfall. Er koordiniert den gesamten Einsatz und ist dafür verantwortlich, die Betriebsfähigkeit des Unternehmens schnellstmöglich wiederherzustellen. Die ersten Stunden nach der Identifizierung des Vorfalls sind besonders entscheidend. 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 dafür sorgen, dass alles so läuft, wie es soll. Die Ergebnisse des SOC werden verständlich aufbereitet und in regelmäßigen Review-Meetings erläutert. Gleichzeitig gibt es die Gelegenheit für konsequente Feedbackschleifen.

Das SOC-Team der suresecure sorgt für die Sicherheit zahlreicher namhafter Unternehmen und wird laufend 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?

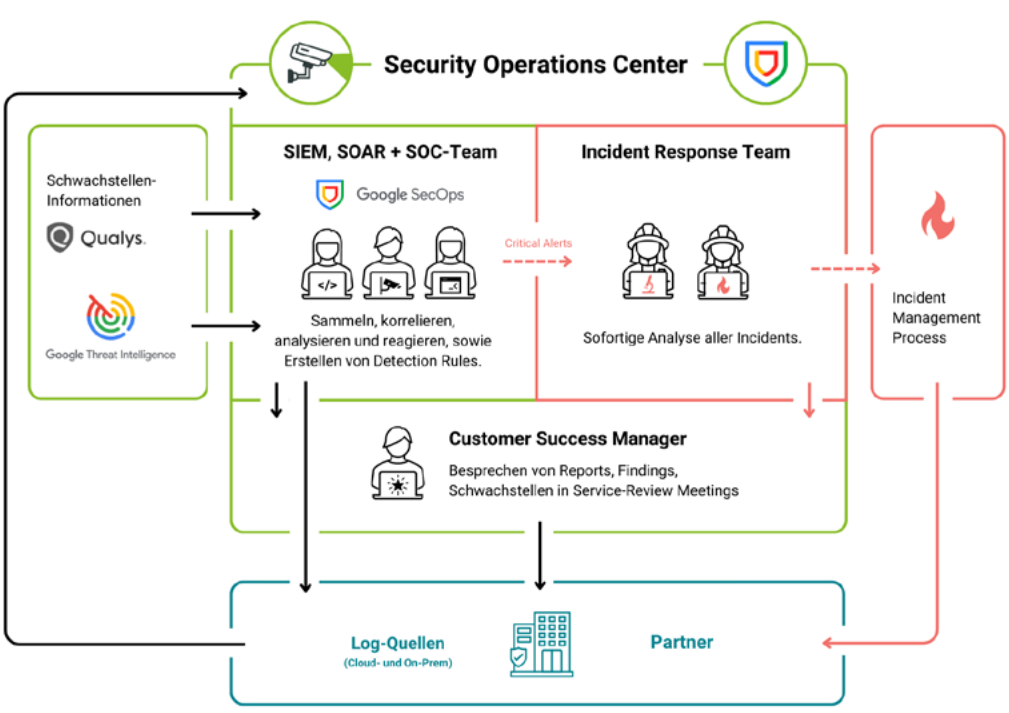
Unser SOC hat einen hohen Reifegrad erreicht und setzt auf eine Cloud-native Lösung von Google. Wenn Google etwas beherrscht, dann ist es die Suche und Korrelation von Daten. Zudem ist Google als Hyperscaler der ideale Partner für sämtliche Skalierungsmöglichkeiten. Genutzt werden das Security Event 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 gegebenenfalls wird der Incident Management Prozess eingeleitet. Über diesen Prozess wird der Partner umgehend 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 erhalten – in Form von sogenannten Indicators of Compromise (IOCs).

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.

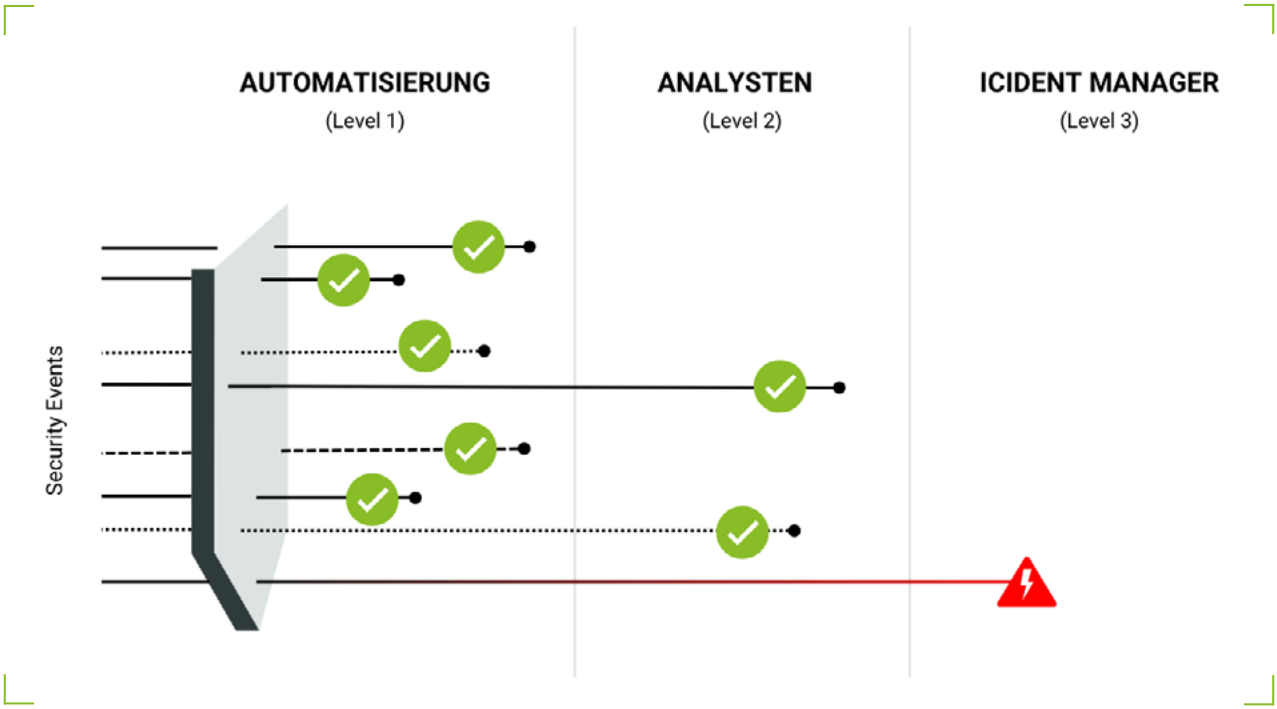
All diese Features bringen aber gar nichts ohne eine prozessuale Einbindung. Und Prozesse werden oftmals unterschätzt. Wir lieben Prozesse.

Foto: Philip Schildein (Head of Cyber Defense Center), Jona Ridderskamp (CTO) 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. Ein solches Konstrukt aufzubauen 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.

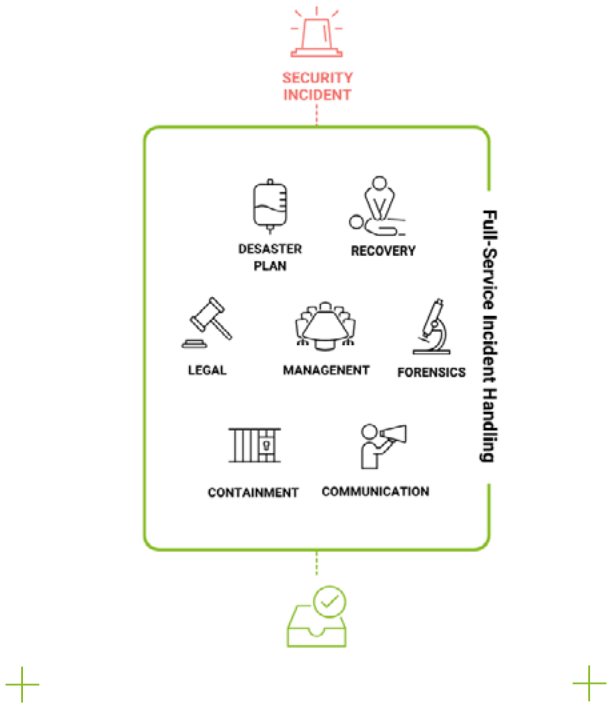


Incident Management ist integriert

Einen Sicherheitsvorfall zu bewältigen bedeutet weit mehr als nur technische Maßnahmen zu ergreifen. Neben tiefgehender technischer Expertise müssen auch Aspekte wie rechtliche Vorgaben und Kommunikation berücksichtigt werden, da hier gravierende Fehler gemacht 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, 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 benötigen eine vertrauensvolle Basis, und diese entsteht nur durch Transparenz und Expertise.

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 vier Wochen live. Im Anschluss werden noch letzte Aufgabenpakete abgeschlossen und die vollständige Überwachung durch unser SOC ist nach spätestens sechs Wochen in place.

Foto: Unsere Customer Success Manager: Adam Marciniak, Annabelle Gunzelmann, Tim Markus und Jonas Castello

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:

Wer Cyberbedrohungen nachhaltig entgegenwirken möchte, sollte sich Gedanken über ein Frühwarnsystem machen. Ein SOC, wie hier beschrieben, stellt derzeit die effektivste Verteidigung dar. Zwar garantiert auch ein SOC keine 100%ige Sicherheit, aber früh erkannte Angriffe führen in der Regel nur zu minimalen Folgeschäden. Sicherheit ist tief in unserer Kultur verankert, und wir setzen alles daran, eure digitale Souveränität zu gewährleisten. Wir freuen uns auf ein Kennenlernen.

Weitere Informationen zum Thema:

Podcast-Folge:

Los SOCos Security Operation Center - Make or Buy?

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

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