CyberCompare Whitepaper

Implementierung eines 24/7 SOC: Die Bedeutung eines effektiven Security Operations Centers (SOC)

Inhalt

1	Einleitung	3
Exkurs: Schäden in Millionenhöhe		4
Exkurs: Fachlicher und technischer Scope eines SOC		5
2	Das passende Modell wählen	7
3	Der Weg zur effektiven Implementierung	8
Exkurs: Die Rolle eines SIEM im SOC		10
Interviews: Wie Industrieunternehmen im KMU-Segment erfolgreich ein SOC implementierten		11
4	Den passenden SOC-Anbieter auswählen	13

1. Einleitung

Angesichts des stetigen Anstiegs von Cyberangriffen stehen Unternehmen und öffentliche Institutionen vor der Herausforderung, immer anspruchsvollere Sicherheitslösungen im IT-Bereich zu implementieren. Die traditionellen Abwehrtechniken wie Firewalls und Antivirenprogramme sind heute nicht mehr effektiv genug, um den hochprofessionellen Angreifergruppen mit ihren gezielten Ransomware-Angriffen und anderen ausgeklügelten Cyberattacken standzuhalten

Mit diesen wachsenden Herausforderungen entscheiden sich viele Organisationen dazu, ein Security Operations Center (SOC) einzurichten. Das SOC agiert dabei als eine eigenständige Organisationseinheit, die eine umfassende Überwachung und Analyse der IT-Systeme der zu schützenden Organisation durchführt. Hierbei werden alle relevanten Personen, Prozesse und Technologien im SOC zusammengeführt. Verschiedene Funktionsgruppen werden integriert, darunter Analysten, Sicherheitsingenieure und SOC-Manager, die erforderlich sind, um die Bedrohungslage einer Systemlandschaft angemessen zu bewerten. Der Vorteil eines SOC besteht darin, dass die Mitarbeiter sich auf eine effektive Cyberabwehr konzentrieren können, da sie oft vom regulären IT-Betrieb getrennt sind.

Die Einrichtung und der Betrieb eines eigenen SOCs sind jedoch für die meisten Organisationen, insbesondere für mittlere und kleinere Unternehmen, äußerst kostspielig und nur schwer umsetzbar. Ein kontinuierlicher 24/7-Betrieb erfordert beispielsweise mindestens 8 bis 12 hochqualifizierte Sicherheitsexperten. Aus diesem Grund entscheiden sich viele Organisationen für ein externes SOC, also das SOC an einen Managed Security Service Provider (MSSP) auszulagern. Nachfolgend beleuchten wir die Bedeutung eines SOC gehen und auf spezifische Implementierungsherausforderungen ein.

Abbildung 1

Gesteigerte Sicherheit durch ein Security Operations Center

Exkurs: Schäden in Millionenhöhe

Kosten von Lösegeldforderungen, Betriebsunterbrechungen und Reputationsverlusten.

Die finanziellen Auswirkungen der Cyberkriminalität sind beträchtlich, mit weltweiten Kosten von 1 Billion US-Dollar pro Jahr, was in etwa 1,2 Prozent des globalen Bruttoinlandsprodukts (BIP) entspricht. Diese Cyberangriffe verursachen Kosten auf drei unterschiedlichen Ebenen:

Kosten für die Zahlung von Lösegeldern, wie die 4,3 Mio. USD, die von der Colonial Pipeline Company gefordert wurden

Kosten für Geschäftsunterbrechungen, die Sich für große, multinationale Unternehmen häufig auf mehrere Millionen Dollar pro Tag belaufen

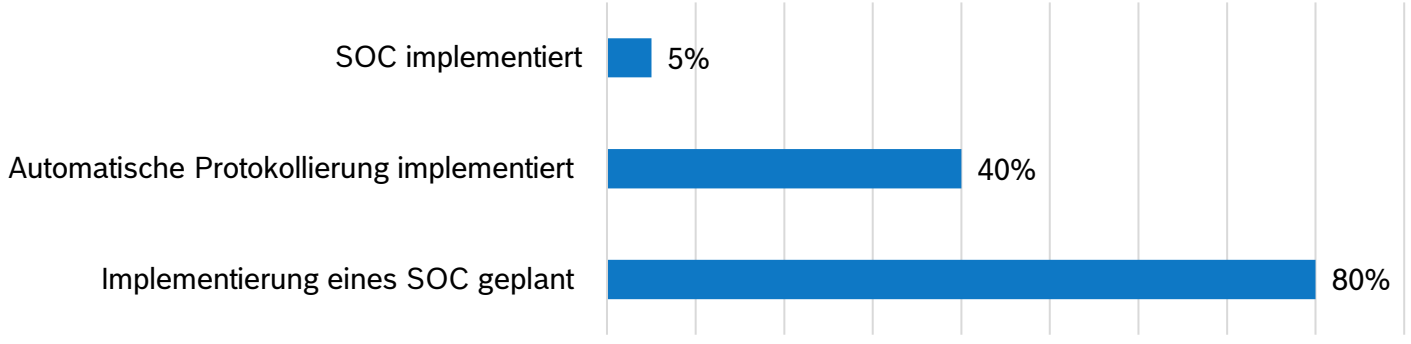
Langfristige Reputationskosten So besteht Schätzungen zufolge z.B. im Falle eines durchschnittlichen Cyberangriffs auf eine Bank bei 27 Prozent der Kunden ein hohes Risiko einer Kontoauflösung; gleichzeitig sinkt der Aktienkurs um 5 bis 7 Prozent

Vor diesem Hintergrund entbrennt in Unternehmen ein Wettlauf um den Ausbau von Cyberkompetenzen und den Schutz vor Cyber-Risiken. Banken investieren bereits beachtliche 2.691 USD pro Mitarbeiter in die Sicherung ihrer IT-Systeme. Diese Mittel fließen in den Aufbau von Abwehrmechanismen gegen Cyberangriffe, die Erkennung von Eindringlingen und das Management von Cyberattacken. Trotz der enormen Bedeutung des Schutzes vor Cyberangriffen lehrt uns die Geschichte, dass hundertprozentige Sicherheit eine Illusion ist. Daher ist die Erkennung und das Bewältigen von Cyberangriffen von ebenso großer Bedeutung.

Während unserer Beratungstätigkeit bei Bosch CyberCompare haben wir beobachtet, dass Best-Practice-Organisationen das SOC als zentrales Element für die Erkennung und das Management von Cyberangriffen etablieren. Dennoch stellen wir gleichzeitig fest, dass gerade im Segment der kleinen und mittleren Unternehmen (KMU) weniger als 5 Prozent unserer Kunden ein SOC flächendeckend implementiert haben (siehe Abbildung).

Abbildung 2

Bereitschaft unserer Kunden für die Implementierung eines SOC



Exkurs: Fachlicher und technischer Scope eines SOC

Der technische Scope umfasst den Schutz von Netzwerken, Websites, Datenbanken, Endpunkten (Clients und Server) und Applikationen. Die Log-Daten aller Systeme fließen zusammen und werden idealerweise in Echtzeit auf Anomalien überprüft. Dabei werden sowohl statistische Verfahren als auch vordefinierte Use Cases (Was ist „normal“? Was deutet auf einen Angriff hin?) festgelegt, um im Schadensfall eine kurze Reaktionszeit zu gewährleisten. Diese Aufgabe übernimmt in der Regel eine SIEM-Lösung (Security Information and Event Management), wie z.B. Splunk, QRadar oder LogRhythm, und bildet damit ein Kernelement des SOC (siehe Exkurs: Die Rolle eines SIEM im SOC).

Abbildung 3

Typische technishe Bestandteile eines SOC

Security Information Event Management (SIEM), in dem die Daten eingehen, normalisiert und analysiert werden

End Point Detection and Response (EDR), um Endpoints zuüberwachen

Sandboxes, um verdächtige Anwendungen sicher analysieren zu können

Security Orchestration, Automation, and Response (SOAR) um automatisiert reagieren zu können

Unternehmen kennen zwar die Bedeutung und Bestandteile eines SOC, sind aber häufig mit dessen Implementierung und Betrieb überfordert, denn es gilt, die Anforderungen und Use Cases zu ermitteln, die richtige Lösung zu finden und eine Reaktionsfähigkeit rund um die Uhr sicherzustellen. Bei diesem Prozess haben wir Unternehmen aus unterschiedlichsten Branchen unterstützt und drei zentrale Faktoren für die erfolgreiche Implementierung eines SOC ermittelt (siehe Abbildung).

Abbildung 4

Entscheidung über internes bzw. externes Management des SOC

Unternehmen müssen zuerst die notwendigen Kompetenzen aufbauen, bevor sie Sich für ein Insourcing des SOC-Managements entscheiden

Anforderungen ermitteln, klein anfangen und schnett iterieren

Anforderungen und Use Cases im Vorfeld genau definieren

Unterstützung anfordern

Mit professioneller Unterstützung das richtige SOC auswählent denn schließlich stehen Millionensummen und die Sicherheit des Unter nehmens auf dem Spiel

Der fachliche Scope eines SOC lässt sich in drei Rollen unterteilen (siehe Abbildung), denn auch wenn alle SOCs einem sicheren Betrieb der Systeme dienen, unterscheidet sich oft der jeweilige fachliche Scope. Die Kombination der drei Rollen innerhalb eines SOC bietet eine umfassende Sicherheitsstruktur, die sowohl auf die Erkennung von Bedrohungen als auch auf die Reaktion auf Sicherheitsvorfälle und die kontinuierliche Verbesserung der Sicherheit abzielt.

Kontrolle und Überwachung

Das SOC stellt einen sicheren Zustand der Systeme sicher, indem es den ordnungsgemäßen Betriebsablauf kontrolliert.

Behandlung

Das SOC konzentriert Sich darauf, Schadensereignisse zu identifizieren und zu analysieren, um ggf. darauf zu reagieren.

Operativer Betrieb

Das SOC kann auch eine sichere Administration der System sicherstellen (z.B. durch Identitäts- und Zugangsmanagement).

2: Das passende Modell wählen

Die Wahl zwischen der internen oder externen Verwaltung eines SOCs ist von entscheidender Bedeutung, da die Effektivität eines SOC stark von dem Team abhängt, das seine Überwachung und Management durchführt. Aufgrund der kontinuierlich steigenden und sich schnell ändernden Cyberrisiken erkennen Unternehmen zunehmend die strategische Bedeutung der Cybersicherheit.

Unsere Projekterfahrung hat verdeutlicht, dass die anfängliche Implementierung eines externen SOCs klare Vorteile bietet. Diese Herangehensweise gestattet Organisationen, schrittweise ihre internen Fähigkeiten aufzubauen und zu evaluieren, ob sie in der Lage sind, die erforderlichen Kompetenzen für das interne SOC-Management zu entwickeln. Insbesondere die rund um die Uhr erfolgende Überwachung und die effektive Reaktion auf Cyberangriffe erfordern nicht nur qualifiziertes Personal, sondern auch kontinuierliche Schulungen und die Weiterentwicklung des Teams.

Weiterhin erfordert der Aufbau eines internen SOCs häufig zusätzliches Personal, darunter mindestens fünf Experten im Bereich Cybersicherheit, welche eine rund um die Uhr besetztes SOC umsetzen sollen. Dies bedeutet, dass die Experten in Schichten arbeiten und dazu bereit sein müssen. Nach Schätzungen einiger Anbieter könnten die Kosten für ein selbstverwaltetes SOC in den ersten drei Jahren bis zu 1,4 Millionen Euro betragen. Dies umfasst die Ausgaben für die Einstellung und Schulung von Fachkräften, den Erwerb von Technologien und Infrastruktur sowie laufende Betriebskosten.

Unabhängig von der gewählten Option ist zu beachten, dass Unternehmen, die sich für ein extern verwaltetes SOC entscheiden, dennoch über interne Ressourcen verfügen müssen, um die Koordination des SOCs sicherzustellen und eine enge Zusammenarbeit mit den SOC-Experten zu gewährleisten. Dies ist insbesondere bei der Bearbeitung von Security Alerts im SOC von Bedeutung.

3: Der Weg zur effektiven Implementierung

Die Ermittlung der Anforderungen sollte mit einer schrittweisen und iterativen Vorgehensweise beginnen, um den Erfolg des SOCs zu gewährleisten. Von entscheidender Bedeutung ist die klare Definition der Use Cases von Anfang an und ein detaillierter Implementierungsprozess, der es dem Unternehmen ermöglicht, Tests durchzuführen und Erkenntnisse zu gewinnen. Hier sind einige Tipps, um dies zu ermöglichen.

SIEM-Meldungen: Berücksichtigen Sie Meldungen aus Security Information and Event Management (SIEM)-Systemen, wie die Korrelation im Netzwerkverkehr, Endpunkten, Firewalls und Serverprotokollen.

Active-Directory-Aktivitäten: Achten Sie auf verdächtige Aktivitäten im Active Directory, wie Anmeldungen von verschiedenen Standorten und laterale Bewegungen.

OT-Monitoring: Integrieren Sie Meldungen von Operational Technology (OT)-Überwachungssystemen, um Ereignisse in industriellen Netzwerken zu korrelieren und Ausfälle zu überwachen.

Endpoint Detection and Response (EDR/XDR): Nutzen Sie Meldungen von EDR- und XDR-Systemen zur Erkennung von verdächtigem Nutzerverhalten und Malware-Angriffen.

Angriffe auf Webserver: Überwachen Sie Webserver auf Distributed Denial of Service (DDoS)-Angriffe und verdächtige Aktivitäten an kritischen Ports.

Fernzugriffswarnungen: Achten Sie auf Warnungen im Zusammenhang mit Fernzugriffen, wie verdächtiges Verhalten von VPN-Nutzern und Brute-Force-Angriffe.

Physischer Zugang: Berücksichtigen Sie Meldungen zu physischen Barrieren, insbesondere mehrfach fehlgeschlagene Authentifizierungen.

Cloud-Performance: Überwachen Sie die Performance in der Cloud und reagieren Sie auf Verstöße gegen Service-Level Agreements (SLAs).

E-Mail-Sicherheit: Integrieren Sie Meldungen im Zusammenhang mit E-Mail-Sicherheit, wie Datenverlust und schädliche Anhänge.

Datenbanksysteme: Achten Sie auf Meldungen von Datenbanksystemen, insbesondere verdächtige Änderungen oder Datenverluste.

Die Berücksichtigung dieser verschiedenen Meldungsquellen und deren schrittweise Implementierung ermöglicht es dem SOC, effektiver auf Bedrohungen zu reagieren und Sicherheitsvorfälle besser zu managen. Dieser iterative Prozess hilft dem SOC-Team, seine Fähigkeiten und Abläufe kontinuierlich zu verbessern.

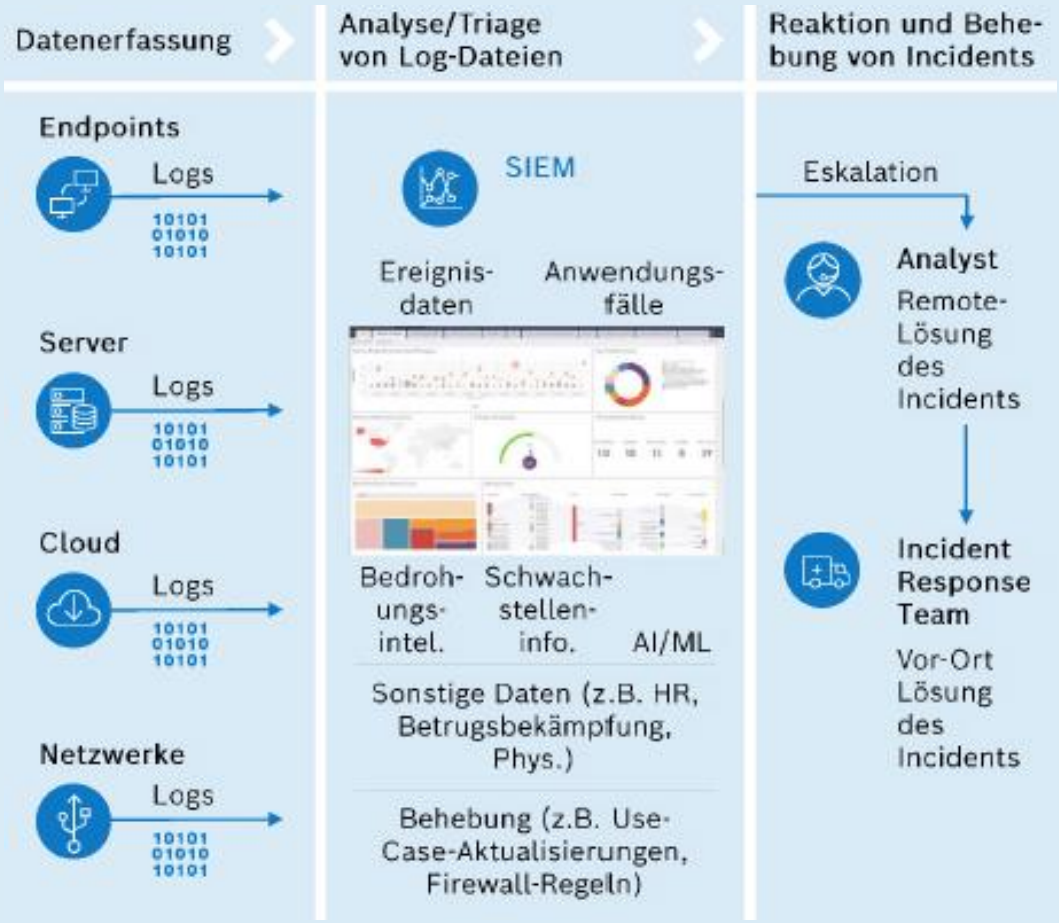
Die schrittweise Einführung eines SOCs in der gesamten Organisation ist besonders relevant, wenn es um Industrieunternehmen geht, die in der Regel in drei wichtige Bereiche unterteilt sind: IT, OT und IoT.

Der Implementierungsprozess gestaltet sich am effektivsten, wenn das Unternehmen zunächst einen dieser Bereiche auswählt, anstatt alle drei gleichzeitig anzugehen. Beispielsweise könnte das SOC zuerst in der IT-Abteilung eingeführt werden. Nachdem wertvolle Erkenntnisse aus dieser Phase gewonnen wurden, kann die Implementierung in den Bereichen OT und IoT in zwei weiteren Phasen erfolgen. Dieser schrittweise Ansatz ermöglicht eine gezielte Entwicklung und Anpassung des SOC entsprechend der spezifischen Anforderungen und Erfahrungen jedes Bereichs.

Exkurs: Die Role eines SIEM im SOC

Ein SIEM (Security Information and Event Management) kann als solide Grundlage für ein SOC dienen und spielt, wie die vereinfachte Abbildung zeigt, eine entscheidende Rolle bei der Stärkung der Cybersicherheit und dem Schutz vor potenziellen Bedrohungen. Das SIEM-System ermöglicht die Erfassung von Daten aus verschiedenen Quellen, einschließlich Endpoints und Anwendungsdaten, sowie die Analyse und Triage von Log-Dateien. Es bietet zudem die Möglichkeit, Ereignisse und Anomalien zu identifizieren und auf Bedrohungen sowie Schwachstellen in der Sicherheitsinfrastruktur hinzuweisen.

Monitoring-Architektur



Durch die Integration von künstlicher Intelligenz (AI) und maschinellem Lernen (ML) kann ein SIEM-System auch dazu beitragen, wertvolle Einblicke in Sicherheitsvorfälle zu gewinnen. Darüber hinaus ermöglicht es die Verarbeitung weiterer Daten, wie beispielsweise Informationen aus der Personalabteilung, zur Betrugsbekämpfung und physikalischen Sicherheit. Im weiteren Verlauf können Maßnahmen zur Behebung von Sicherheitsvorfällen ergriffen werden, darunter Aktualisierungen von Use Cases und Firewall-Regeln. Das SIEM-System unterstützt die Reaktion und Behebung von Incidents, wobei ein Incident Response Team in Aktion tritt, das entweder remote oder vor Ort tätig werden kann.

Einschub vom ganzen Interview, S. 10 bis 12

Interviews: Wie Industrieunternehmen im KMU-Segment erfolgreich ein SOC implementierten

Ein führendes Industrieunternehmen musste dringend seine Strategie und Kompetenzen im Bereich Cybersicherheit verbessern, nachdem das Unternehmen Opfer eines Ransomware-Angriffs geworden war und die Kerninfrastruktur – samt E-Mail-Systemen, Internetverbindungen, Dateidiensten und ERP-Systemen – vier Monate lang nicht funktionierte.

Nachdem das Unternehmen also schmerzlich zu spüren bekommen hatte, dass es keinen hundertprozentigen Schutz vor Cyberangriffen gibt, entwickelte es eine neue Strategie für Cybersicherheit: Hierbei fungiert das SOC als Kontrollinstanz, die Cyberangriffe in Echtzeit erkennt und das Unternehmen in die Lage versetzt, unmittelbar zu reagieren.

Und tatsächlich konnten weitere Cyberangriffe zwar nicht gänzlich verhindert, mit Hilfe des SOC aber frühzeitig erkannt werden. Nachfolgend beschreibt der CIO, wie das Unternehmen dabei vorgegangen war:

1 Warum haben Sie sich für ein SOC entschieden?

Unser SOC erfüllt inzwischen vielfältige Aufgaben und bei unserer Entscheidung dafür kamen zahlreiche Aspekte zum Tragen. Im Mittelpunkt unserer Überlegungen stand die Gewährleistung eines Betriebs rund um die Uhr. Darüber hinaus unterstützt uns das SOC bei der Schulung unserer Beschäftigten, die sich ständig neues Fachwissen aneignen und lernen, wie man mit sicherheitsrelevanten Zwischenfällen umgeht. Im Fokus des SOC steht die Sicherheit unserer Systeme, denn das Thema Sicherheit hat für uns einen höheren Stellenwert bekommen, und das SOC stellt sicher, dass unsere Systeme kontinuierlich gewartet werden. Abgesehen von den Sicherheits-aspekten versetzt uns das SOC auch in die Lage, die Funktionsfähigkeit unserer Anlagen zu überwachen.

2 Wie haben Sie die SOC-Aufgaben intern/extern aufgeteilt und was sind die Gründe dafür? Wie sind die Rollen im Falle eines Angriffs verteilt?

Der Betrieb wird gemeinsam gesteuert: Die operative Verantwortung obliegt dem SOC – wir haben immer noch Schreibrechte, müssen uns aber beim Änderungsmanagement an die Vorgaben des SOC halten.

Im Notfall greift ein Eskalationsprotokoll und die Entscheidungen werden von einem Gremium getroffen. Es handelt sich um ein globales Team, das Entscheidungen nach dem Sechs-Augen-Prinzip trifft. Konkret heißt das, dass ein Beschäftigter aus dem SOC und zwei Beschäftigte von uns zügig Entscheidungen treffen können, wobei die Führung jedoch dem SOC obliegt.

3 Welche Erkenntnisse haben Sie aus der Implementierung gewonnen, die Sie mit anderen mittelständischen Unternehmen teilen können?

Die Implementierung eines SOC ist ein umfassender Prozess. Es müssen Verfahren und Regeln entwickelt werden. Ein SOC lässt sich daher nicht in ein paar Tagen implementieren. Je besser der Übergang gelingt, desto schneller werden die Prozesse etabliert. Darüber hinaus erfordert ein Outsourcing der eigenen Sicherheit auch großes Vertrauen.

Interviews: Wie Industrieunternehmen im KMU-Segment erfolgreich ein SOC implementierten

Ein Hersteller von einbaufertigen Präzisionsteilen entschied sich aus ähnlichen Gründen für ein SOC, wie sein IT-Manager berichtet:

1 Warum haben Sie sich für ein SOC entschieden?

Im Rahmen unserer IT-Strategie wollten wir unsere Position stärken. Die Rund-um-die-Uhr-Überwachung unserer Systeme in einem SOC ist dabei zentraler Bestandteil unserer Maßnahmen. Darüber hinaus will unser Management sicherstellen, dass wir bei der Bekämpfung potenzieller Cyberangriffe unser Bestes geben. Die zunehmende Zahl von Angriffen auf Lieferketten führte auch zu höheren Anforderungen seitens unserer Kunden. Für die Zusammenarbeit mit Drittunternehmen sind häufig Zertifizierungen wie ISO2700x oder TISAX erforderlich. Ein SOC hilft uns dabei, diese und andere Richtlinien einzuhalten.

2 Wie haben Sie die SOC-Aufgaben intern/extern aufgeteilt und was sind die Gründe dafür? Wie sind die Rollen im Falle eines Angriffs verteilt?

Wir haben uns aus zwei Gründen für ein externes SOC entschieden: Erstens ist es für uns schwierig, die dafür erforderlichen internen Kompetenzen aufzubauen. Und zweitens wollten wir nicht in Eigenregie zusätzliche Software und Hardware aufbauen und warten.

Die Aufgaben sind klar zwischen internen Beschäftigten und dem Personal im SOC aufgeteilt. Bei einem Zwischenfall erhalten wir von den Experten im SOC weitere Informationen und Empfehlungen für die Lösung des Problems. Besteht das Problem weiterhin, erhalten wir Unterstützung von Incident-Response-Analysten im SOC-Team.

3 Welche Erkenntnisse haben Sie aus der Implementierung gewonnen, die Sie mit anderen mittelständischen Unternehmen teilen können?

Bei der Anbieterauswahl hat es sich für uns bewährt, befreundete Unternehmen nach ihren Erfahrungen zu fragen. Wir haben festgestellt, dass sich die Angebote im Hinblick auf Preis und Leistungsumfang stark unterscheiden. Daher war es wichtig, die unterschiedlichen Angebote auszuwerten. Maßgeblich für uns ist Flexibilität. Daher empfehlen wir kurze Vertragslaufzeiten und die Nutzung gängiger Soft- und Hardware, um Lock-in-Effekte zu vermeiden.

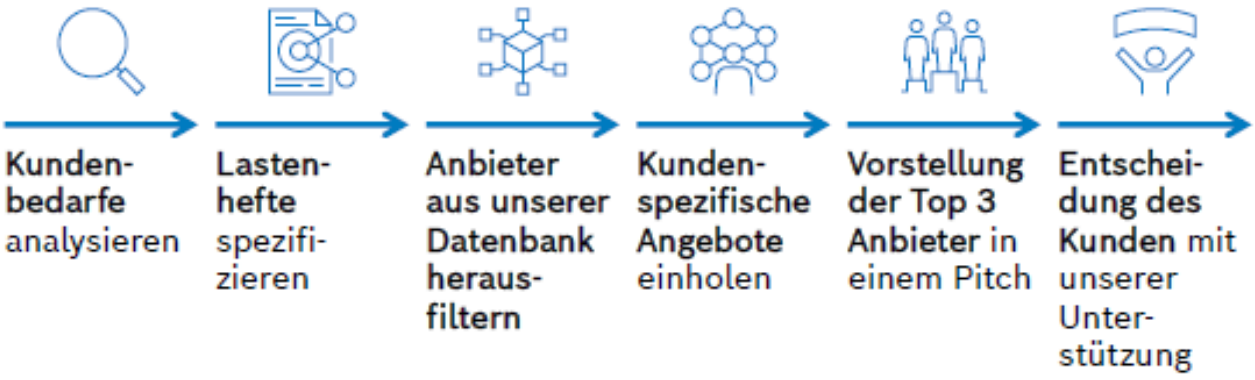
4: Den passenden SOC-Anbieter auswählen

Eine maßgeschneiderte SOC-Lösung steigert nicht nur erheblich die Sicherheit, sondern ermöglicht auch erhebliche Kosteneinsparungen. Dies wurde in einem konkreten Projekt deutlich: Unser Kunde, ein Unternehmen im Bereich erneuerbare Energien, entschied sich für eine anonyme Ausschreibung über unsere Vergleichsplattform. Anstatt ohne eine genaue Bedarfsanalyse die teuren Angebote von Full-Service-Anbietern für SOC zu nutzen, arbeiteten wir eng mit dem Energieunternehmen zusammen, um die benötigten Funktionalitäten, Servicelevel und Zielarchitekturen genau zu definieren.

Basierend auf dieser präzisen Bedarfsermittlung konnten wir gezielt in unserem Netzwerk nach qualifizierten Anbietern suchen und anonym ausschreiben. Das Ergebnis war nicht nur ein externes SOC, das die IT/OT-Systeme des Unternehmens optimal absicherte, sondern auch beeindruckende Kosteneinsparungen von etwa 10 Millionen USD allein in den ersten fünf Jahren.

Abbildung 5

Wie wir Ihnen einen passenden Anbieter vermitteln



Die Zusammenarbeit mit Bosch CyberCompare, der unabhängigen Vergleichsplattform im Kundenauftrag und ohne finanzielle Provision von Anbietern, kann äußerst vorteilhaft sein, wenn es um Ihr geplantes SOC-Projekt geht. Gemeinsam mit Bosch CyberCompare haben Sie die Möglichkeit, Ihr SOC-Projekt von der Konzeption bis zur anonymen Ausschreibung erfolgreich umzusetzen. Wir bieten umfassende Unterstützung, beginnend mit der Definition der Anforderungen bis hin zum Anbietervergleich, um sicherzustellen, dass Sie die besten Entscheidungen für die Sicherheit Ihrer Organisation treffen. Wir handeln ohne Partnerschaften mit Anbietern, wodurch unsere Unabhängigkeit gewährleistet ist und häufig zu wettbewerbsfähigeren Preisen führt. Darüber hinaus bieten transparente und klare Empfehlungen von Bosch CyberCompare wertvolle Unterstützung bei der Entscheidungsfindung, wenn es darum geht, Produkte auszuwählen.

Nutzen Sie diese Gelegenheit, um mit Bosch CyberCompare gemeinsam ein erstklassiges SOC zu implementieren und Ihr Unternehmen effektiv vor Cyberbedrohungen zu schützen.

BOSCH

CyberCompare

Nehmen Sie Kontakt auf!

Gemeinsam Ihre Cybersecurity erhöhen - von einem transparenten Überblick über Ihren Cyber-Bedarf bis hin zur Auswahl geeigneter Anbietender.

Individuell. Pragmatisch. Unabhängig.

Kontaktieren Sie das CyberCompare-Führungsteam

Dr Jannis Stemmann

Jannis.Stemmann@bosch.com
Telefon: +49 711 811-44954

Philipp Pelkmann

Philipp.Pelkmann@bosch.com
Telefon: +49 711 811-15519

Simeon Mussler

Simeon.Mussler@bosch.com
Telefon: +49 711 811-19893

Bosch CyberCompare Verbände und Branchenkooperationen

Allianz für Cyber-Sicherheit Partner | Security made in Germany | Security made in EU | ITSECURITY | TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V. | CYBERSECURITY MADE IN EUROPE

Besuchen Sie unsere Website:
www.cybercompare.com