



CIO Advisory

Security-Operation-Center

Cyberkriminalität sinnvoll begegnen



Security-Operation-Center (SOC): Funktion und Bausteine

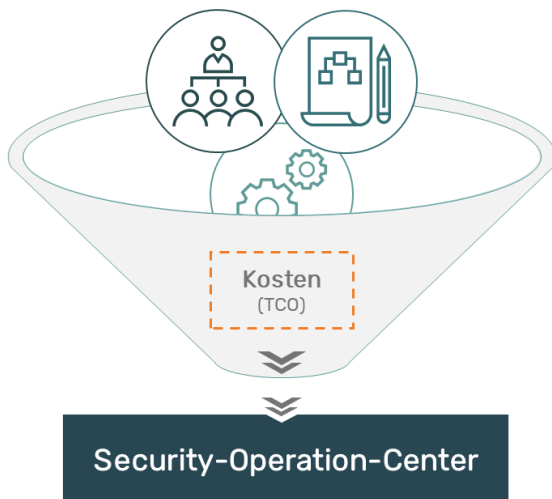
Früherkennung und effiziente Bekämpfung von Cyberangriffen sind bei den allgegenwärtigen Sicherheitsbedrohungen der heutigen digitalen Welt unverzichtbar geworden. Ein wichtiger Baustein für die Erfüllung von Business- und Compliance-Anforderungen sowie zur Wahrung und Stärkung des Vertrauens von Mitarbeitern, Kunden und Geschäftspartnern sind Informationen und deren Sicherheit. Ein Security-Operation-Center als zentrale Cybersicherheitsleitstelle verfolgt das Ziel, die digitalen Daten und Assets eines Unternehmens proaktiv zu schützen und so den Unternehmenserfolg dauerhaft sicherzustellen.

System zur Angriffserkennung

Ein Security-Operation-Center überwacht kontinuierlich die IT-, OT- und IoT-Geräte, Netzwerke und Anwendungen einer Organisation. Dabei werden Sicherheitsdaten von diesen Quellen gesammelt, in einem zentralen System miteinander korreliert und mit Hilfe von Algorithmen und Analysetools fortlaufend und in Echtzeit ausgewertet. Auf diese Weise können Muster und Verhaltensweisen in den gesammelten Daten identifiziert und - im Umkehrschluss - auch Abweichungen von diesen normalen Verhaltensmustern frühzeitig erkannt werden. Solche Abweichungen gelten als Anomalien, die auf einen potenziellen Angriff hindeuten und weiter untersucht und/oder eingedämmt werden müssen. Das Security-Operation-Center ist also ein System, das eine frühzeitige Angriffserkennung ermöglicht.

Weit mehr als nur Technologie

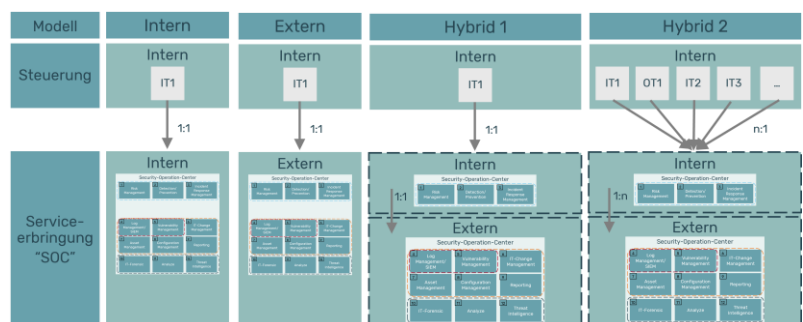
Ein Security-Operation-Center als System zur Angriffserkennung ist weitaus mehr als eine dedizierte Technologie. Die frühzeitige Erkennung von Angriffen ist schließlich nur so viel wert, wie auf einen erkannten Angriff oder Bedrohungen auch angemessen reagiert bzw. proaktiv gehandelt werden kann. Ein Security-Operation-Center ist daher eine hoch-spezialisierte Organisation, die darauf ausgerichtet ist, digitale Bedrohungen zu identifizieren, zu analysieren und angemessene Gegenmaßnahmen einzuleiten. Ein Security-Operation-Center ist als strategischer Sicherheitsansatz zu verstehen, der die Expertise von Menschen und Organisation, die Effizienz von Prozessen sowie die Leistungsfähigkeit von Produkten und Technologien integriert. Das nahtlose Ineinandergreifen dieser drei Aspekte ist der entscheidende Erfolgsfaktor für ein effektives Security-Operation-Center.



	Menschen & Organisation <ul style="list-style-type: none"> Integration des SOC in die unternehmerischen Ziele und Strukturen Sicherstellung, dass das Personal die richtigen Rollen mit den entsprechenden Fähigkeiten einnimmt Festlegung klarer Rollen und Aufgaben Entwicklung einer effektiven Kommunikation und Zusammenarbeit.
	Prozesse & Verfahren <ul style="list-style-type: none"> Erstellung von Standardarbeitsanweisungen Automatisierung/Kodifizierung von Prozessen, um manuelle Arbeit zu reduzieren Einführung von Maßnahmen zur Qualitätskontrolle Entwicklung eines Systems zur Verfolgung und Messung der Leistung
	Technologie & Produkte <ul style="list-style-type: none"> Sicherstellung, dass eingesetzte Technologien den Zielen des SOC sowie dem aktuellen Stand der Technik entsprechen Integration der SOC-Technologien in die vorhandene Infrastruktur Berücksichtigung von gesetzlichen und regulatorischen Vorgaben

Nachhaltige Resilienz: TCO-konformer SOC-Betrieb

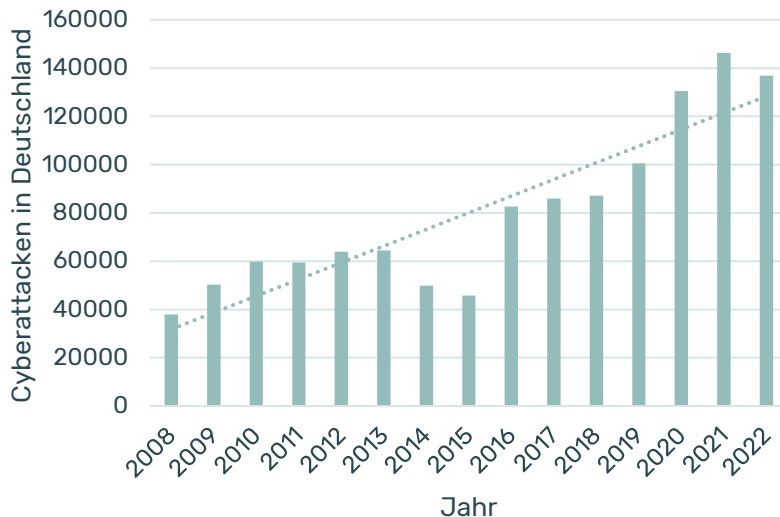
Die Investition in ein Security-Operation-Center ist eine langfristige Investition in die Cyber-Resilienz Ihrer Organisation. Daher ist eine nachhaltige und langfristige Kostenplanung unter Berücksichtigung der Gesamtbetriebskosten (Total Cost of Ownership) wichtig. Insbesondere bei der Bewertung und Evaluierung von Betriebsmodellen spielt dieser Aspekt eine entscheidende Rolle. Dies gilt sowohl für intern betriebene, extern betriebene als auch für hybride Security-Operation-Center.





Sicherheitsvorfälle beeinträchtigen Ihr Kerngeschäft. Cyber-Resilienz muss daher als strategisches Geschäftsziel betrachtet werden.

Die Anzahl an Cybersicherheitsvorfällen nimmt stetig zu. Die Cyberkriminalität professionalisiert sich zunehmend und die Angriffstechniken und -taktiken werden immer raffinierter. In der Vergangenheit haben sich Organisationen bei ihren Bemühungen um Cybersicherheit auf Präventivmaßnahmen konzentriert. In Hinblick auf die steigenden Angriffszahlen und die dadurch entstandenen Schäden zeigt sich, dass dies schon lange nicht mehr ausreichend ist. Cyber-Resilienz erfordert auch die Vorbereitung auf den Ernstfall und die Implementierung von Erkennungs- und Reaktionsmöglichkeiten, um Angriffe frühzeitig zu stoppen und den Schaden zu minimieren.



Quelle: BKA Bundeslagebilder Cybercrime 2012 bis 2022



Quelle: Bitkom e.V. (2023). Wirtschaftsschutz 2023

Für wen ist ein SOC empfehlenswert?

Ein Security-Operation-Center ist für Organisationen jeder Größe und Branche empfehlenswert, die ein erhöhtes Risiko für Cyberangriffe haben, deren Geschäftstätigkeit stark von der Verfügbarkeit und Integrität ihrer IT-Systeme abhängt sowie die bereits sorgfältig in eine grundlegende Sicherheits- und Präventionsorganisation investiert haben.

Für wen ist ein SOC weniger dringend?

Ein Security-Operation-Center mit seinen Erkennungs- und Reaktionsdiensten ist weniger dringlich bei Organisationen, bei denen Störungen in ihrer IT/OT geringe bis gar keine Auswirkungen auf ihre Geschäftstätigkeit haben, deren digitale Daten nicht sensibel sind sowie die bislang keinerlei präventive Maßnahmen und Technologien zur Bewältigung von digitalen Risiken einsetzen.

SOC ist nicht gleich SOC.

Frühzeitige Bedarfsanalyse und Anforderungserhebung führen langfristig zum Erfolg

Der Begriff „Security-Operation-Center“ ist nicht geschützt. Daher variieren SOC-Dienstleistungen sehr stark in ihrer Form, ihrer Größe, den eingesetzten Technologien und deren Möglichkeiten sowie schlussendlich im Preis. Die Erhebung von Anforderungen auf organisatorischer, technischer und prozessualer Ebene sowie die Ermittlung nachhaltiger Kostenvorgaben für den langfristigen SOC-Betrieb in Verbindung mit Resilienz- und Risikozielen sollte daher frühzeitig erfolgen, sodass der Service passgenau geschnitten werden kann.



Einflussfaktoren für eine solche SOC-Strategie liegen dabei keineswegs ausschließlich im Bereich der IT oder der OT. Auch grundlegende Geschäfts-, Unternehmens- oder Konzernstrategien liefern wichtige Inputs, mit denen die SOC-Strategie in Einklang gebracht werden sollte.

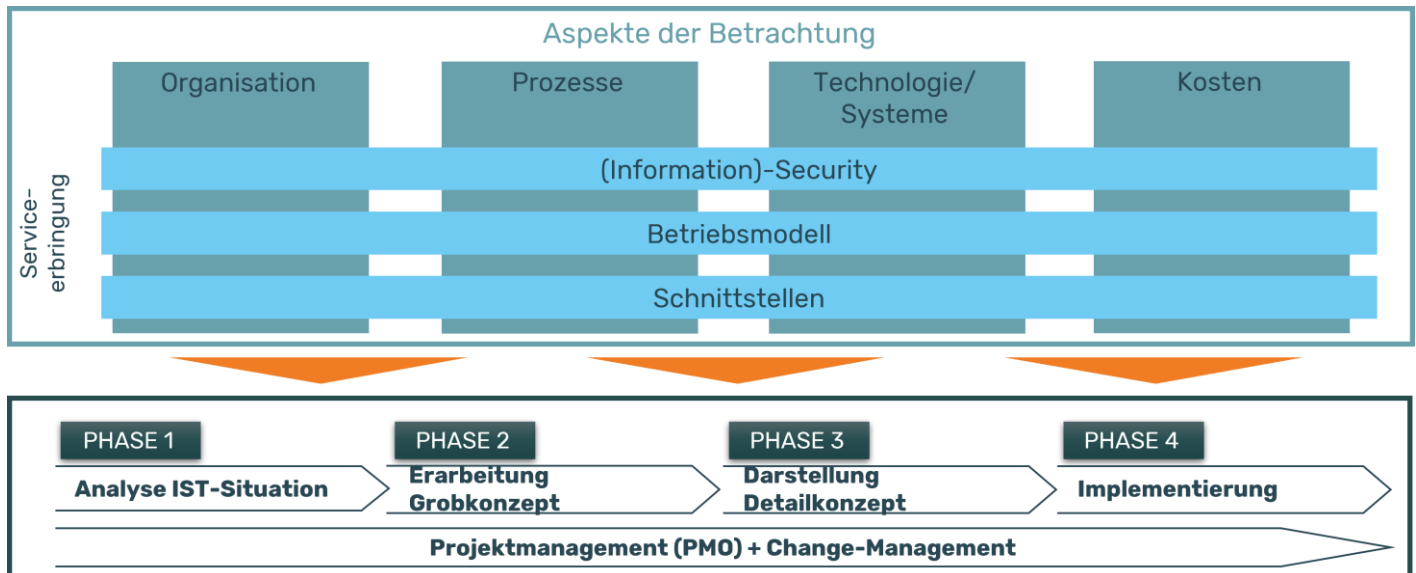
Ist das SOC-Leitbild entworfen und verabschiedet, so wird dies auf taktischer Ebene anhand von Richtlinien und Vorgaben konkreter ausdefiniert sowie in die bestehende Sicherheitsorganisation integriert.

Im SOC-Betrieb erfolgt schließlich die Operationalisierung und Umsetzung der konkreten Vorgaben und Richtlinien des SOC-Services.



Unsere Vorgehensweise für ein integriertes, bedarfsgerechtes SOC: Von der Analyse bis zur Implementierung

Unser Beratungsangebot kombiniert Expertise in gängigen Standards und SOC-Leistungen mit Erfahrungswissen aus aufsichtsrechtlichen Vorgaben und ausgewiesener, praxiserprobter Umsetzungskompetenz. Im Mittelpunkt unseres Beratungsansatzes steht immer die Integration der Organisation, Prozesse und Technologien in einen SOC-Service, der Ihren TCO-Vorgaben entspricht.



1 Analyse der Ist-Situation

Zu Beginn stehen Bestandsaufnahme und Bedarfsanalyse. Nur durch das Verständnis Ihrer Organisation ist es uns möglich, ein passendes SOC-Konzept für Sie zu entwickeln. Wir definieren gemeinsam die Rahmenbedingungen und Leitplanken, evaluieren Interessen und Notwendigkeiten sowie stimmen Anforderungen und Bedarfe (u. a. mittels Interviews und Workshops) mit Ihnen ab.

2 Grobkonzeption

In der Grobkonzeption gleichen wir die erhobene Ist-Situation mit unseren "Good-Practices" ab. Wir konkretisieren das Information-Security-Framework und entwickeln darauf basierend ein für Sie passendes SOC-Grobkonzept, welches die verschiedenen Service- bzw. Betriebsmodelle sowie deren Einbindungsmöglichkeiten in Ihre Aufbau- und Ablauforganisation bewertet und somit für Sie als Entscheidungsgrundlage dient.

plenum - profitieren sie von unseren erfahrungen

Unser Anspruch ist es, nachhaltige und wirksame Lösungen für Sie zu schaffen

- Wir bieten über 30 Jahre Beratungs- und Fachkompetenz, gepaart mit umfassendem Branchen- und Technologie-Know-how sowie ausgeprägter Management-Expertise.
- Wir beschränken uns nicht nur auf die strategische und konzeptionelle Ebene, sondern unterstützen unsere Kunden operativ bis zum erfolgreichen Abschluss der Umsetzung und darüber hinaus im Rahmen einer strategischen Partnerschaft.
- Wir stellen das Management der strategischen und operationellen Ausrichtung der Kunden in den Fokus. Durch die Kombination der Beraterqualität und der technischen Expertise bei der Umsetzung der Projekte erhalten unsere Kunden eine ganzheitliche Betreuung über den gesamten Lebenszyklus.

3 Detailkonzeption

In der Detailkonzeption wird das Betriebs- bzw. Servicemodell detailliert ausgestaltet. Es werden Zielbilder und Fertigungstiefen festgelegt, Implementierungspläne entwickelt sowie Schnittstellen und Werkzeuge definiert. Unser Fokus liegt hierbei auf der Sicherstellung eines langfristigen TCO-konformen SOC-Betriebes.

4 Implementierungsbegleitung

In der Phase der Implementierung begleiten wir Sie qualitätssichernd im Sinne der abgestimmten Konzeption von der Auswahl von Technologien und Service-Partnern bis hin zum prozessualen, technischen und organisatorischen Rollout Ihres SOC-Services. Als methodische Basis verwenden wir ein Reifegradmodell, um sowohl die vertragliche, technische als auch organisatorische und prozessuale Implementierungsreife des SOC-Service zu betrachten.