plusserver | osanta
Teil der plusserver Gruppe

Security Operations Center im Reality-Check

Braucht Ihr Unternehmen ein SOC?
Fakten für Entscheider:innen und
Tipps zum Betrieb.

Whitepaper

Inhalt

Management Summary

Ransomware, Phishing und gezielte Attacken auf Unternehmensnetzwerke haben in den letzten Jahren dramatisch zugenommen. Laut der Bitkom-Studie „Wirtschaftsschutz 2025“ waren 87 Prozent der Unternehmen in den vergangenen zwölf Monaten von Datendiebstahl, Spionage oder Sabotage betroffen – mit einem Gesamtschaden von rund 290 Milliarden Euro. Kein Unternehmen ist dabei zu klein oder zu unbedeutend, um ins Visier von Cyberkriminellen zu geraten. Die Frage ist also nicht, ob eine Organisation angegriffen wird, sondern wann – und ob sie darauf vorbereitet ist.

Ein Security Operations Center (SOC) kann hier eine entscheidende Rolle spielen. Es schafft Transparenz, überwacht die IT-Umgebung rund um die Uhr, erkennt Bedrohungen frühzeitig und ermöglicht eine schnelle Reaktion auf Sicherheitsvorfälle. Doch der Aufbau eines eigen-en SOC ist mit einigen Herausforderungen verbunden: Es erfordert Investitionen, spezialisierte Fachkräfte und eine nahtlose Integration in bestehende IT-Sicherheitsstrukturen.

Nicht jedes Unternehmen kann oder will diesen Aufwand stemmen. Alternativen wie SOC as a Service bieten die Option, den SOC-Betrieb an externe Dienstleister auszulagern. Aber: Ist das die richtige Wahl für jedes Unternehmen? Welche Vorteile und Risiken bringt ein externes SOC mit sich? Und wie kann eine fundierte Entscheidung getroffen werden?

Dieses Whitepaper bietet IT-Verantwortlichen eine klare, faktenbasierte Grundlage, um den tatsächlichen Bedarf ihres Unternehmens an SOC-Dienstleistungen zu ermitteln. Es erläutert neben den Aufgaben und Vorteilen eines SOC auch die essenziellen Technologien sowie die typischen Herausforderungen beim Betrieb. Zudem stellt es Entscheidungshilfen zum passenden Betriebsmodell bereit.

Definition:

Was ist ein SOC?

Ein Security Operations Center ist die zentrale Einheit für die IT-Sicherheitsüberwachung eines Unternehmens. Hier laufen alle sicherheitsrelevanten Informationen zusammen. Datenströme werden analysiert, verdächtige Aktivitäten identifiziert und Cyberangriffe in Echtzeit abgewehrt.

Ein SOC überwacht Netzwerke, Endpunkte und Cloud-Umgebungen rund um die Uhr, um potenzielle Angriffe frühzeitig zu erkennen. Wenn verdächtige Aktivitäten auftreten, analysiert das SOC diese Vorfälle und entscheidet über geeignete Gegenmaßnahmen.

Eine zentrale Rolle spielt auch die sogenannte Threat Intelligence, also die systematische Auswertung von Bedrohungsinformationen:

Angriffsstrategien von Cyberkriminellen werden untersucht, um Sicherheitsmaßnahmen laufend zu verbessern. Sollte es dennoch zu einem erfolgreichen Angriff kommen, kann das SOC bei der Ursachenanalyse helfen und gezielte Gegenmaßnahmen einleiten.

Menschen, Technologien und Prozesse sind die drei tragenden Säulen eines jeden SOC. Neben erfahrenen Sicherheitsexpert:innen sind leistungsfähige Security-Tools erforderlich, die verdächtige Aktivitäten automatisiert erkennen und bewerten. Einheitliche Prozesse helfen dabei, Bedrohungen schnell und gezielt zu bekämpfen. Zudem muss das SOC nahtlos in die bestehende IT-Sicherheitsarchitektur integriert sein, um Daten aus verschiedenen Quellen nutzen zu können.

Ausgangslage:

Vom blinden Fleck zur Transparenz

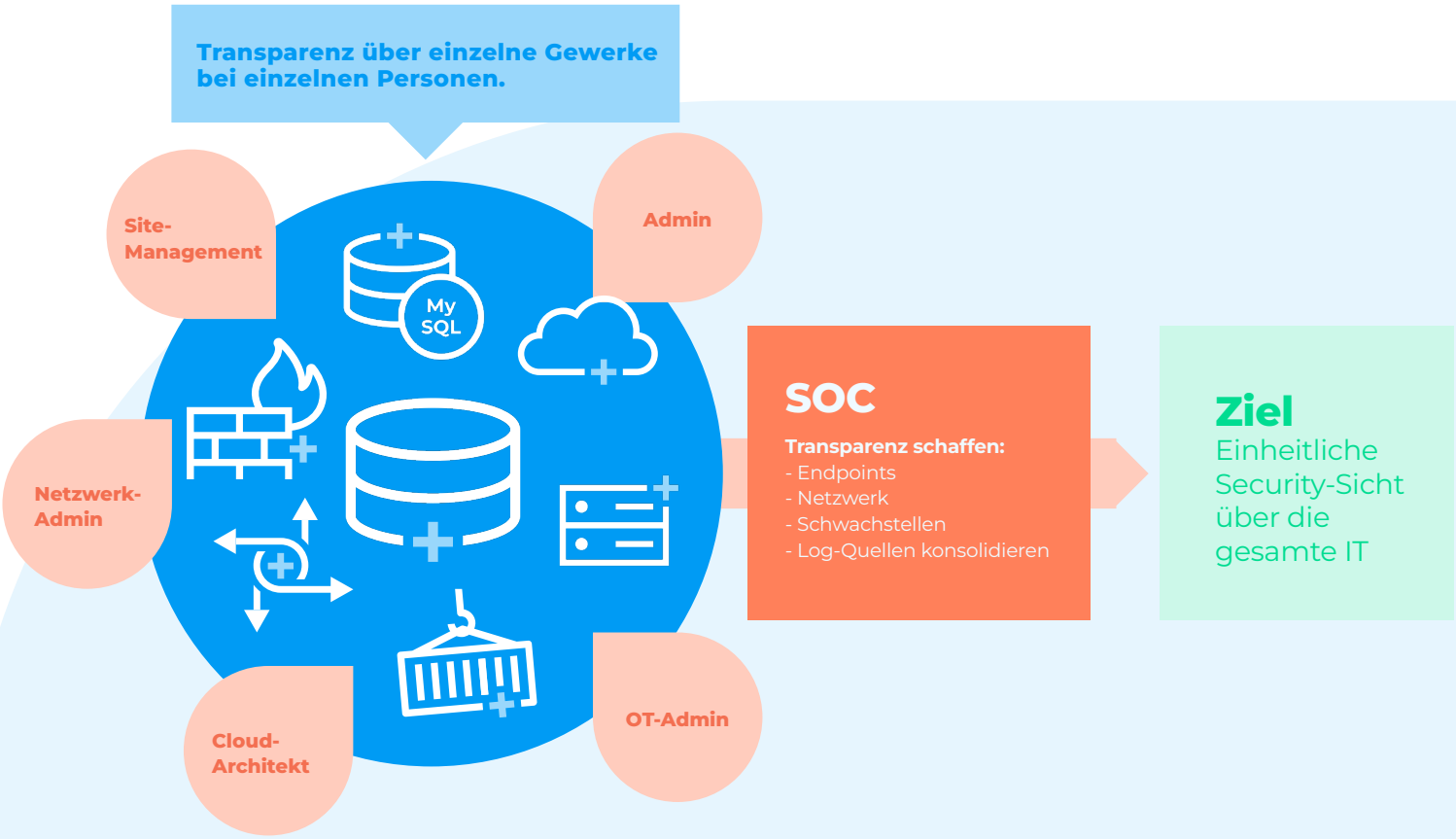
Viele Unternehmen beginnen ihre Reise im Bereich der IT-Sicherheit, ohne einen klaren Überblick über ihre eigene IT-Landschaft zu haben. Im Laufe der Zeit sind gewachsene Strukturen mit unterschiedlichen Tools, isolierten Systemen und dezentral verantworteten Bereichen entstanden. Netzwerk-, OT- und Cloud-Administratoren arbeiten oft nebeneinanderher, ohne sicherheitsrelevante Daten zu konsolidieren. So entsteht ein Flickenteppich aus Informationen, der potenzielle Angriffsflächen eher verdeckt als sichtbar macht.

Erst wenn ein Sicherheitsvorfall eintritt, zeigt sich, wie schwer es ist, die Ursache nachzuvollziehen oder den Umfang eines Angriffs einzuschätzen. Die Logs liegen verstreut in einzelnen Anwendungen, Verantwortlichkeiten sind unklar und ein Gesamtbild fehlt. Diese Intransparenz ist das eigentliche Risiko.

Der erste Schritt zu mehr Sicherheit ist daher immer, für Klarheit zu sorgen. Unternehmen beginnen in der Regel damit, ihre Systeme und Log-Quellen zu inventarisieren, Zuständigkeiten zu klären und Datenflüsse sichtbar zu machen. So entsteht nach und nach ein strukturiertes Sicherheitsbild, das als Grundlage für weitere Maßnahmen dient.

Ein Security Information and Event Management (SIEM) kann diese Informationen schließlich zusammenführen. Es sammelt Log-Daten aus allen Quellen, erkennt Anomalien und liefert ein ganzheitliches Lagebild. Damit ist der entscheidende Schritt zur Transparenz erreicht.

Ein Security Operations Center geht jedoch noch weiter: Es sorgt dafür, dass diese Transparenz nicht nur punktuell, sondern dauerhaft gewährleistet ist. Durch die Kombination aus SIEM, etablierten Prozessen, Automatisierung und kontinuierlicher Überwachung durch Expert:innen bleibt die Sicherheitslage rund um die Uhr und über alle Systeme hinweg aktuell. Es findet somit eine Entwicklung vom einmaligen Erfassen hin zu einer kontinuierlichen Sicherheitsüberwachung und aktiven Verteidigung statt. Oder auch vom Chaos über Transparenz hin zu nachhaltiger Kontrolle, wie die folgende Grafik verdeutlicht.



Sicher & resilient:

Argumente für Entscheider:innen

Cyberangriffe lassen sich nicht vollständig verhindern. Aber ein SOC kann den entscheidenden Unterschied machen, wenn es darum geht, Sicherheitsvorfälle frühzeitig zu erkennen und professionell darauf zu reagieren. Unternehmen, die ein SOC betreiben oder darauf zugreifen, profitieren von einer signifikanten Verbesserung ihrer Sicherheitslage und Resilienz.

Einer der größten Vorteile liegt in der kontinuierlichen Überwachung der IT-Infrastruktur. Während klassische Sicherheitsmaßnahmen wie Firewalls oder Antivirenprogramme oft nur einzelne Schutzmechanismen bieten, analysiert ein SOC sicherheitsrelevante Daten aus unterschiedlichsten Quellen in Echtzeit. Dadurch lassen sich verdächtige Aktivitäten frühzeitig erkennen und Angriffe oft stoppen, bevor sie Schaden anrichten.

Ein weiterer entscheidender Vorteil ist die verkürzte Reaktionszeit bei Sicherheitsvorfällen. Ohne SOC vergeht häufig wertvolle Zeit, bis Angriffe bemerkt und analysiert werden. In einem SOC übernehmen speziell ausgebildete Analyst:innen diese Aufgabe. Fortschrittliche Automatisierungstools, die Bedrohungen priorisieren und Handlungsempfehlungen liefern, unterstützen sie dabei. So lassen sich Cyber angriffe schneller eindämmen und Folgeschäden minimieren.

Auf diese Weise trägt ein SOC außerdem dazu bei, finanzielle Schäden sowie Reputationsverluste zu vermeiden. Betriebsunterbrechungen oder Lösegeldforderungen infolge von Ransomware-Attacken können hohe Kosten verursachen. Hinzu kommt der mögliche Vertrauensverlust bei Kunden und Partnern, wenn Daten gestohlen oder öffentlich zugänglich gemacht werden.

Bei der Erfüllung regulatorischer Anforderungen kann ein SOC ebenfalls unterstützen. Daher ist es beispielsweise für Unternehmen essenziell, die unter die KRITIS-Verordnung, NIS-2 oder den europäischen DORA-Regulierungsrahmen fallen. Es stellt nicht nur sicher, dass sicherheitsrelevante Vorfälle frühzeitig erkannt, sondern auch nachvollziehbar dokumentiert und gemäß den regulatorischen Anforderungen behandelt werden. Damit unterstützt das SOC neben der Betriebssicherheit auch die Compliance im Unternehmen.

Security-Strategie:

Die Rolle des SOC

IT-Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der verschiedene Maßnahmen und Strategien umfasst. Ein Security Operations Center spielt dabei eine entscheidende Rolle, indem es Transparenz schafft, Bedrohungen frühzeitig erkennt und auf Sicherheitsvorfälle reagiert. Doch für eine wirksame Security-Strategie reicht ein SOC allein nicht aus. Vielmehr zählt das Zusammenspiel mehrerer Aspekte.

Die vier Säulen einer ganzheitlichen Sicherheitsstrategie

1. Risikomanagement

Bevor Sicherheitsmaßnahmen ergriffen werden, müssen Risiken systematisch analysiert und bewertet werden. Dafür können unter anderem Security Assessments durch externe Spezialist:innen sorgen. Ein SOC kann bei diesem Punkt unterstützen, indem es die Basis für eine Security-Gap-Analyse liefert. Dazu macht es Schwachstellen durch kontinuierliche Überwachung und Analyse sicherheitsrelevanter Daten sichtbar.

2. Schutzmaßnahmen

Im Rahmen einer ganzheitlichen Sicherheitsstrategie kommt es auf ein abgestimmtes Zusammenspiel technischer, organisatorischer und prozessualer Maßnahmen an. Dazu zählen unter anderem die systematische Identifikation von Risiken, der Schutz kritischer Systeme durch segmentierte Netzwerke und mehrstufige Zugriffskontrollen sowie eine kontinuierliche Überwachung und Anomalieerkennung. Ergänzt werden diese Maßnahmen durch etablierte Prozesse zur Reaktion auf Sicherheitsvorfälle, regelmäßige Schwachstellenanalysen und die Schulung von Mitarbeitenden im sicheren Umgang mit IT-Systemen. Ziel ist es, die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken und den Geschäftsbetrieb auch im Falle von Angriffen aufrechtzuerhalten.

3. Wiederherstellung

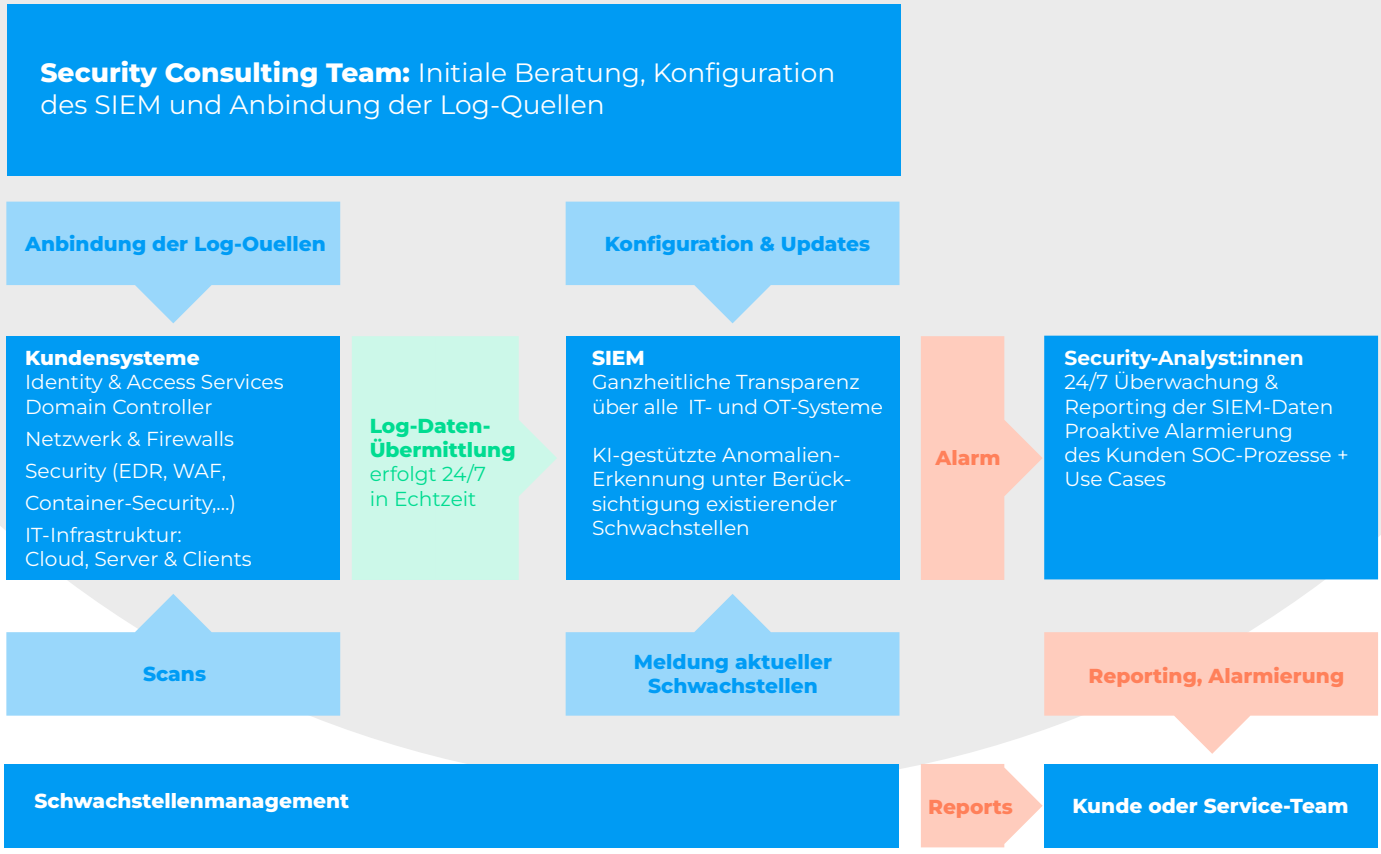
Trotz aller Schutzmaßnahmen bleibt das Risiko einer Sicherheitsverletzung bestehen. Eine robuste Backup- und Disaster-Recovery-Strategie stellt sicher, dass Daten und Systeme im Falle eines Angriffs schnell wiederhergestellt werden können. Forensische Analysen durch das SOC können herangezogen werden, um Wiederherstellungsprozesse zu optimieren.

Security-Strategie:

Die Rolle des SOC

4. Transparenz

Eine umfassende Sicherheitsstrategieer- fordert kontinuierliche Überwachung und Echtzeiteinblicke in sicherheitsrelevante Ereignisse. Ein SOC bietet mit integrierten Tools wie dem SIEM genau diese Transpa- renz über die gesamte Infrastruktur und fungiert als zentrale Schaltstelle für die Sicherheitsüberwachung.



Die Abbildung verdeutlicht, wie das SOC Transparenz und Handlungssicherheit schafft: Durch den durchgängigen Prozess aus Erkennung, Bewertung, Alarmierung und Reaktion behalten Unternehmen ihre Sicherheitslage jederzeit im Blick.

Der Maschinenraum:

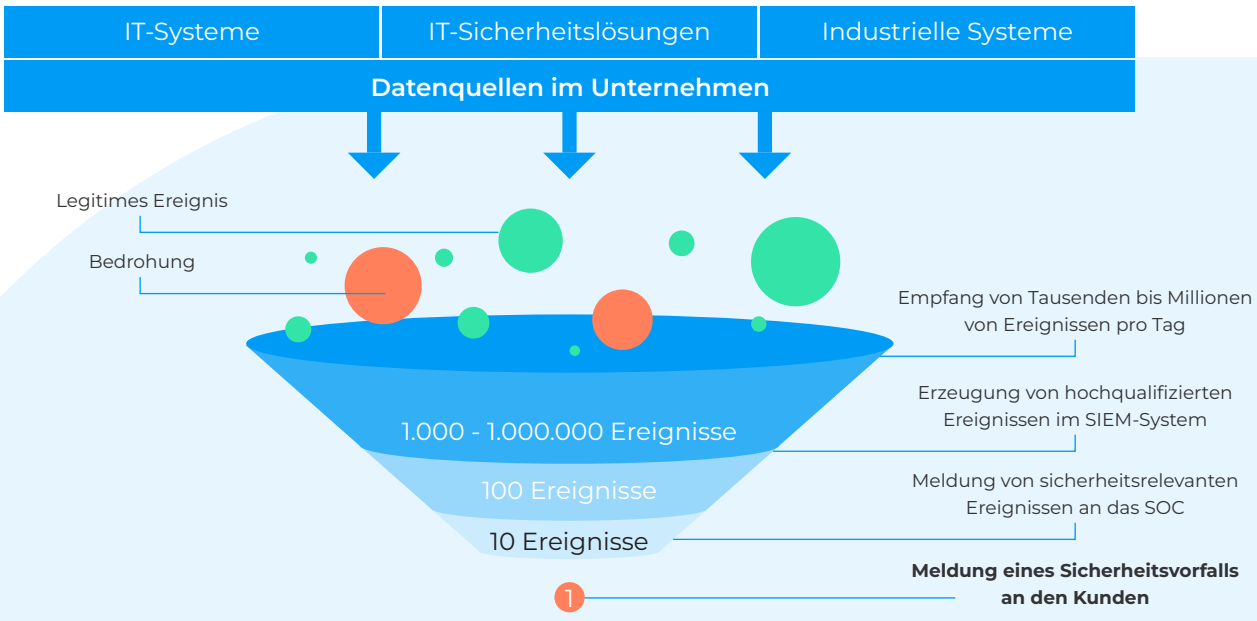
SOC-Tools und -Technologien

Um Bedrohungen zu erkennen, zu analysieren und darauf zu reagieren, benötigt ein SOC nicht nur Schnittstellen zu verschiedenen Sicherheitslösungen. Es sind auch verschiedene Werkzeuge erforderlich, um sicherheitsrelevante Daten zu sammeln und zu korrelieren, Prozesse zu automatisieren und eine schnelle, fundierte Entscheidungsfindung zu ermöglichen. Dadurch ergibt sich eine umfangreiche Tool-Landschaft, die implementiert, betrieben und gewartet werden muss.

SIEM (Security Information and Event Management)

Ein SIEM bildet das zentrale Analyse- und Steuerungselement eines SOC. Es sammelt sicherheitsrelevante Ereignisse aus verschiedenen angebundenen Quellen wie Firewalls, Endpunkt-Schutzlösungen, Netzwerksensoren und Identitätsmanagement-Systeme. Da nicht jedes erfasste Ereignis eine tatsächliche Bedrohung darstellt – moderne IT-Umgebungen generieren täglich Millionen von Log-Einträgen –, filtert und korreliert ein SIEM diese Informationen, um Muster und Anomalien zu erkennen. Dabei kommen regelbasierte Erkennungsmechanismen ebenso zum Einsatz wie maschinelles Lernen, das verdächtige Aktivitäten automatisch analysiert.

Ein entscheidender Vorteil eines SIEM ist die Priorisierung von Alarmen. Es trennt harmlose Auffälligkeiten von echten Sicherheitsvorfällen, um Fehlalarme zu minimieren und die Sicherheitsteams gezielt auf kritische Bedrohungen aufmerksam zu machen. Diese Reduktion der Alarmflut ist essenziell, damit Analyst:innen effizient arbeiten können und Alarmmüdigkeit gar nicht erst entsteht.



Mit einem SIEM lassen sich gemeldete Ereignisse aus unterschiedlichen Datenquellen sammeln und in Echtzeit so auswerten, dass die Datenflut auf wesentliche Alarme reduziert wird.

SOAR (Security Orchestration, Automation and Response)

Ein SOC muss nicht nur Bedrohungen erkennen, sondern auch effizient darauf eagieren. Genau hier setzt SOAR an. Eine SOAR-Plattform automatisiert sicherheitsrelevante Prozesse durch die Orchestrierung verschiedener Sicherheitslösungen – vom SIEM bis zur Firewall. So lassen sich Bedrohungen automatisch eindämmen, ohne dass jedes Mal manuell eingegriffen werden muss. Beispielsweise kann es verdächtige IP-Adressen automatisch blockieren, Phishing-Mails in Echtzeit analysieren oder Alarme aus dem SIEM mit Bedrohungsdaten abgleichen, um False Positives zu minimieren.

Threat-Intelligence-Plattformen

Die beste Verteidigung gegen Cyberangriffe ist das Wissen über aktuelle Bedrohungen. Threat-Intelligence-Plattformen sammeln und analysieren Informationen über neue Angriffsmethoden, Schadsoftware und Hackergruppen. Diese Erkenntnisse helfen einem SOC, Angriffe frühzeitig zu erkennen und Abwehrmaßnahmen gezielt zu optimieren. Durch die automatisierte Integration in SIEM- und SOAR-Systeme lassen sich Bedrohungen in Echtzeit mit aktuellen Intelligence-Daten abgleichen. Beispielsweise kann eine Threat-Intelligence-Plattform bekannte bösartige IP-Adressen oder Hashwerte von Malware automatisch an das SIEM übermitteln, das dann verdächtige Aktivitäten in den eigenen Systemen identifiziert.

EDR/XDR (Endpoint Detection & Response / Extended Detection & Response)

Der Fokus von EDR liegt auf der Überwachung einzelner Endgeräte. Es erkennt ungewöhnliches Verhalten auf Laptops, Servern oder Mobilgeräten und leitet Gegenmaßnahmen ein. XDR geht noch einen Schritt weiter und korreliert Informationen aus mehreren Sicherheitsbereichen, etwa Netzwerk, Cloud und Endpunkte, um Angriffe frühzeitig zu identifizieren.

Schwachstellenscanner

Ein wirksames Schwachstellenmanagement beginnt mit der zuverlässigen Erkennung potenzieller Sicherheitslücken. Schwachstellenscanner sind dafür essenzielle Werkzeuge im SOC-Betrieb. Sie durchsuchen Netzwerke, Systeme und Anwendungen regelmäßig nach bekannten Schwachstellen, werten diese automatisiert aus und liefern eine priorisierte Übersicht der Risiken. Moderne Scanner greifen dabei auf umfangreiche Datenbanken (CVE = Common Vulnerabilities and Exposures) zurück und bewerten Schwachstellen auch im Kontext der betroffenen Umgebung. Durch die Integration mit SIEM-, Ticketing- oder Patch-Management-Systemen können identifizierte Lücken direkt weiterverarbeitet und entsprechende Maßnahmen eingeleitet werden.

NIDS (Network Intrusion Detection System)

Ein weiteres essenzielles Werkzeug für ein SOC ist ein NIDS. Es überwacht den Netzwerkverkehr in Echtzeit und erkennt verdächtige Aktivitäten, die auf Cyberangriffe hinweisen könnten. Durch den Abgleich mit bekannten Angriffssignaturen und die Analyse auffälliger Verhaltensmuster hilft ein NIDS dabei, Bedrohungen wie unautorisierte Zugriffe, Port-Scans oder das Ausnutzen von Schwachstellen frühzeitig zu identifizieren. Gerade weil viele Angreifer versuchen, sich unbemerkt im Netzwerk zu bewegen, trägt ein NIDS entscheidend dazu bei, solche Aktivitäten sichtbar zu machen.

Weitere relevante Technologien

Neben diesen Kernlösungen gibt es weitere Tools, die ein SOC unterstützen. Log-Management-Systeme erleichtern die strukturierte Speicherung und Auswertung sicherheitsrelevanter Ereignisse. Deception-Technologien setzen bewusst falsche Fährten, um Angreifer zu identifizieren, bevor sie echten Schaden anrichten. Und moderne Cloud-Security-Plattformen helfen, Cloud-Umgebungen ebenso umfassend zu schützen wie klassische On-Premises-Infrastrukturen. Ein SOC kann nur dann optimal arbeiten, wenn die richtigen Tools intelligent miteinander verknüpft sind.

Die Wahl des Betriebsmodells:

SOC im Eigenbetrieb

Neben den oben genannten Technologien bestimmen klare Prozesse und der Faktor Mensch einen gelungenen SOC-Betrieb. Das bedeutet: Unternehmen müssen nicht nur investieren, sondern sich auch mit personellen, organisatorischen und technischen Herausforderungen auseinandersetzen.

Investitions- und Betriebskosten

Der Aufbau eines SOC ist kostenintensiv. Neben der Anschaffung der notwendigen Security-Tools fallen laufende Kosten für Infrastruktur, Lizenzen und Wartung an. Hinzu kommt der kontinuierliche Betrieb: Ein SOC muss rund um die Uhr aktiv sein, um Bedrohungen jederzeit zu erkennen und darauf zu reagieren. Das bedeutet entweder Schichtbetrieb mit eigenem Personal oder die Einbindung externer Dienstleister.

Integration in bestehende IT-Landschaften

Ein SOC ist kein isoliertes System, sondern muss sich nahtlos in die bestehende IT- und Sicherheitsarchitektur eines Unternehmens einfügen. Bestehende Security-Tools müssen angebunden, Log-Daten konsolidiert und Schnittstellen geschaffen werden. In heterogenen IT-Umgebungen mit einer Mischung aus On-Premises- und Cloud-Systemen kann das schnell zur Herausforderung werden.

Fachkräftemangel und Personalanforderungen

An qualifiziertem Personal mangelt es in vielen Unternehmen. SOC-Analyst:innen, Incident Responder und Threat Hunter sind ebenso gefragte wie rare Fachkräfte. Die wenigen Spezialist:innen auf dem Markt haben hohe Gehaltsvorstellungen und sind meist bereits fest angestellt. Hinzu kommt, dass SOC-Teams regelmäßig geschult werden müssen, um mit den neuesten Angriffstechniken und Abwehrstrategien Schritt zu halten. Cyberkriminelle entwickeln sich ständig weiter. Wer im SOC arbeitet, muss das auch tun.

Laufende Wartung und Weiterentwicklung

Was für das Personal gilt, gilt auch für das gesamte SOC. Es muss kontinuierlich optimiert und an neue Bedrohungsszenarien angepasst werden. Angreifer entwickeln neue Taktiken, Compliance-Anforderungen ändern sich und IT-Infrastrukturen wachsen. Einmal aufgebaute Regeln und Prozesse müssen regelmäßig überprüft und angepasst werden, um weiterhin wirksam zu bleiben.

Die Alternativen:

Externe Betriebsmodelle

Nicht jedes Unternehmen kann oder möchte die oben genannten Aufgaben stemmen. Aber es gibt Alternativen zum Eigenbetrieb. Unternehmen können entweder auf ein vollständig ausgelagertes SOC as a Service setzen oder ein 3rd Party SOC wählen.

3rd Party SOC

Bei einem 3rd Party SOC übernimmt ein externer Spezialist nicht den kompletten Betrieb, sondern stellt einzelne SOC-Funktionen oder -Leistungen als Service bereit. Unternehmen betreiben ihre Security-Tools – etwa EDR oder Schwachstellenmanagement – weiterhin selbst, während der 3rd-Party-Provider ergänzende Aufgaben wie SIEM, Analyse, Alarmbewertung oder Incident Response übernimmt.

Dieses Modell eignet sich insbesondere für Unternehmen, die bereits über eine gewisse Sicherheitsinfrastruktur verfügen, aber keine eigene 24/7-Überwachung aufbauen möchten oder können. Der 3rd-Party-Anbieter agiert hier als verlängerte Werkbank des internen Security-Teams und unterstützt bei der kontinuierlichen Bewertung von Sicherheitsereignissen sowie bei der Priorisierung von Maßnahmen.

SOC as a Service (SOCaaS)

Beim SOC as a Service betreibt ein externer Security-Dienstleister die oben beschriebenen SOC-Tools für mehrere Kunden in einer zentralen Infrastruktur, zum Beispiel in einer Cloud. Auch um das Recruiting gut ausgebildeter Security-Analyst:innen müssen sich die Kunden nicht selbst kümmern, da der SOCaaS-Anbieter ein zentrales Security-Team bereitstellt. Außerdem sorgt der Anbieter für die kontinuierliche Weiterentwicklung aller Systeme und Mitarbeitenden, um auch auf fortschrittliche Bedrohungen angemessen reagieren zu können.

Das Modell richtet sich vornehmlich an Unternehmen, die noch keine bis wenig eigenen Security-Lösungen betreiben, kein eigenes Security-Team aufgebaut haben oder einfach eine ganzheitliche Unterstützung bei Transparenz, Überwachung, Reaktion und Analysen wünschen.

Die Alternativen:

Externe Betriebsmodelle

Vergleichstabelle aller Modelle

Modell	Vorteile	Herausforderungen / Grenzen
Eigenes SOC	· Volle Kontrolle über Systeme, Daten und Prozesse · Maximale Anpassbarkeit an Unternehmensanforderungen · Direkte Einbindung in bestehende IT-Architektur	· Hoher Personal- und Kostenaufwand · Fachkräftemangel und Schulungsbedarf · Aufwändige Integration und Wartung
3rd Party SOC	· Ergänzung interner Kompetenzen durch externe Analyst:innen · Nutzung bestehender Systeme mit gezielter Unterstützung · Flexible Skalierung bei Bedarf · Hohe Anpassungsfähigkeit bei gleichzeitigem Kontrollerhalt	· Klare Prozess- und Rollen-abgrenzung erforderlich · Abhängigkeit von Service-qualität und Reaktionszeit · Abstimmungsaufwand mit externem Team
SOC as a Service	· Schnelle Implementierung und geringere Einstiegshürde · Planbare monatliche Kosten statt hoher Investitionen · Zugang zu spezialisierten Fachkräften · Skalierbar und rund um die Uhr verfügbar	· Weniger Individualisierung möglich · Externe Datenhaltung erfordert Vertrauen und vertragliche Regelungen · Abhängigkeit vom Anbieter

Implementierung:

Der SOC-Fahrplan

Sobald die Entscheidung für ein Betriebsmodell getroffen ist, geht es an die Umsetzung. In Anbetracht der steigenden Angriffszahlen heißt es, entsprechend gerüstet zu sein, um Bedrohungen mit aktueller Technologie, bewährten Prozessen und menschlicher Expertise gezielt zu begegnen. Ein detaillierter Fahrplan hilft, das gewählte Modell erfolgreich zu etablieren.

1
Strategie festlegen: Klare Ziele für das SOC definieren.

2
Anforderungen und Budget bestimmen: Welche Ressourcen sind verfügbar?

3
Partner und Technologien auswählen: Passende Security-Tools und ggf. externe Dienstleister evaluieren.

4
Mitarbeitende einbinden: Schulungen und klare Verantwortlichkeiten im Team festlegen.

5
Kontinuierlich optimieren: Regelmäßige Tests und Anpassungen sind essenziell.

1. Strategie festlegen

Eine klare Zielsetzung bildet die Grundlage für alle weiteren Schritte. Unternehmen müssen entscheiden, welche Ziele sie mit einem SOC verfolgen. Dies kann eine schnellere Reaktionszeit auf Vorfälle, die Erfüllung regulatorischer Anforderungen oder eine generelle Verbesserung der Cyber-Resilienz sein.

2. Anforderungen und Budget bestimmen

Die Einführung eines SOC erfordert ein realistisches Verständnis über die vorhandenen Ressourcen. Dazu gehören Budget, interne Kompetenzen und bestehende Security-Tools. Dieser Schritt dient der Priorisierung: Welche Systeme sind kritisch, welche Risiken bestehen und welche Sicherheitsmaßnahmen sind wirtschaftlich umsetzbar?

3. Partner und Technologien auswählen

Je nach gewähltem Betriebsmodell – Eigenbetrieb, 3rd Party SOC oder SOC as a Service – gilt es, passende Technologien bzw. Dienstleister auszuwählen. Neben technischen Kriterien spielt bei letzterem auch die Frage nach dem Standort oder der Support-Struktur eine zentrale Rolle.

4. Mitarbeitende einbinden

Schulungen und Awareness-Programme sind entscheidend, um Sicherheitsprozesse in den Unternehmensalltag zu integrieren. Sie stellen sicher, dass Mitarbeitende nicht zu Einfallstoren für Schadsoftware werden. Klare Verantwortlichkeiten und Kommunikationswege sorgen für eine saubere Einbindung externer Dienstleister.

5. Kontinuierlich optimieren

Auch wenn ein SOC extern betrieben wird, bleibt die kontinuierliche Optimierung ein gemeinsamer Prozess zwischen Anbieter und Kunde. Der Dienstleister sorgt für die technische Weiterentwicklung, etwa durch Updates, neue Use Cases, Threat-Intelligence-Feeds oder erweiterte Automatisierungen.

Auf Unternehmensseite ist entscheidend, dass Rückmeldungen aus dem Betrieb, Änderungen in der IT-Landschaft und neue Geschäftsprozesse regelmäßig an den SOC-Partner kommuniziert werden. Nur so kann dieser die Erkennungslogik, Alarmierungswege und Reports anpassen.

Cosanta und plusserver:

SOC Services in Deutschland

Sie wünschen Zugang zu einem SOC-Betrieb, der deutsche Compliance-Standards erfüllt und sich modular an en eigenen Reifegrad anpasst? Cosanta ist eine eigenständige Tochtergesellschaft der plusserver-Gruppe und unterstützt als Managed Security Service Provider Unternehmen in der DACH-Region bei ihrer Security-Strategie. Dabei orientiert sich das Angebot am IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Ein wesentlicher Vorteil der SOC-Dienstleistungen von Cosanta ist die modulare Struktur. Unternehmen können mit ein bis zwei angebundenen Security-Modulen starten und ihre SOC-Funktionalität nach Bedarf erweitern. Dies ermöglicht einen schrittweisen Einstieg in die professionelle Sicherheitsüberwachung und -analyse, ohne sofort die volle Bandbreite an Services nutzen zu müssen. Bereits vorhandene Security-Lösungen wie EDR oder Network Security können problemlos in das SOC von Cosanta integriert werden, sodass es als 3rd Party SOC genutzt wird. Alternativ bietet Cosanta die nötigen Security- Lösungen „as a Service“ an, wodurch Unternehmen flexibel entscheiden können, welche Komponenten sie selbst bereitstellen und welche sie von Cosanta beziehen.

+ **Technologie und Betrieb in der zertifizierten Cloud**
  Alle Systeme werden vollständig durch Cosanta in der eigenen zertifizierten Cloud von plusserver in Deutschland betrieben.

+ **Hohe Compliance-Standards**
  Ideal für Unternehmen mit besonderen Anforderungen an Datenschutz und Regulierung.

+ **Security Consulting**
  Entwickeln Sie mit Cosanta eine nachhaltige Security-Strategie, mit der Sie aktuelle und kommende Regularien erfüllen und Ihre Resilienz stärken.

Starten Sie jetzt mit einem Security Operations Center, das sich flexibel an die Sicherheitsbedürfnisse Ihres Unternehmens anpasst. Für maximalen Schutz bei minimalem Aufwand.

Jetzt persönlich beraten lassen ▸

plusserver

plusserver GmbH
Welserstraße 14
51149 Köln
+49 221 8282 8550
beratung@plusserver.com

shop.plusserver.com

Cosanta
Teil der plusserver Gruppe

Cosanta GmbH
Prinzenstraße 2a
42697 Solingen
+49 2125 208 2320
info@cosanta.de

www.cosanta.de

Eine souveräne, zukunftsfähige und sichere Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

Zertifiziert und testiert nach höchsten Sicherheitsstandards.
Genießen Sie Datenschutz und digitale Souveränität in der Cloud.

BSI C5 CLOUD SECURITY
ISAE 3402
DATENSCHUTZ IDW PH 9.860.1
ISO 50001:2018
TÜVRheinland CERTIFIED
www.tuv.com ID 9000036551