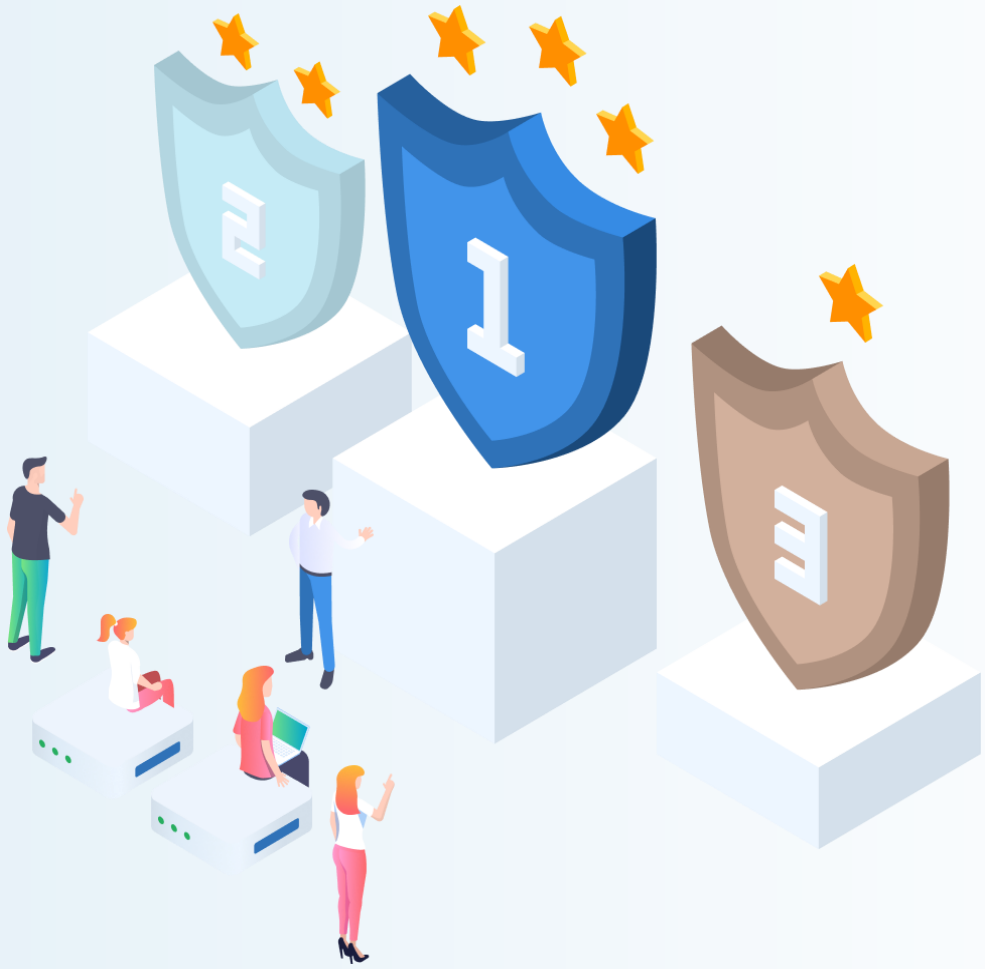


CyberCompare Whitepaper

Die erfolgreiche Auswahl eines Partners für ein Managed Security Operations Center

Ein Security Operations Center (SOC) hat die Aufgabe, eine definierte IT-Umgebung hinsichtlich sicherheitsrelevanter Ereignisse („Events“) dauerhaft zu beobachten. Dazu werden in der Regel Log-Dateien und/oder der Datenverkehr auf verdächtige Informationen hin analysiert. So sollen Bedrohungsszenarien aufgedeckt („Detect“) sowie entsprechende Gegenreaktionen („Response“) eingeleitet werden.

Große Unternehmen betreiben häufig eigene SOCs oder so genannte Cyber Defense Center (CDC). Dies lohnt sich für mittelständische Unternehmen oft nicht, da zum einen qualifizierte SOC-Analysten rar sind, viel Expertise in den Plattformen und Werkzeugen professioneller SOC-Anbieter steckt und die Komplexität bei einer 24/7-Überwachung noch deutlich steigt. Dieses 24/7-Modell wird oftmals als Standard angesehen, doch für kleine und mittelgroße Unternehmen eignen sich zum Einstieg oft auch reduzierte Umfänge, die z.B. über Bereitschaftsdienste ergänzt werden können.

Viele unserer Kunden beschäftigen sich derzeit mit einem SOC in der „Managed“-Variante, also über einen externen Partner (manchmal auch bezeichnet als SOC as a Service).

In diesem Whitepaper behandeln wir daher die wesentlichen Fragestellungen bei der Spezifikation der Anforderungen, sowie Erfolgskriterien im Auswahlprozess.

Was kostet ein Managed SOC?

Eine pauschale Antwort auf diese Frage kann nur falsch sein – zu stark hängen die Kosten von den gewählten Ansätzen und dem gewünschten Umfang ab. Soll z.B. noch ein SIEM (Security Information and Event Management) ggf. sogar on-premise implementiert werden, erhöht dies zwangsläufig die Kosten für Implementierung und Betrieb. Auch andere Faktoren beeinflussen die Kosten, z.B. die Tiefe der Bedrohungserkennung durch den Analysten, die im SLA (Service Level Agreement) vereinbart wurde.

Dennoch ist es für die Budgetierung eines Unternehmens notwendig, einige grundlegende Abschätzungen vorzunehmen:

Bei kleineren Unternehmen von z.B. 500 Mitarbeitenden sind monatliche Kosten von ca. 7.000 bis 14.000 EUR pro Monat realistisch.

Unternehmen mit ca. 5.000 Mitarbeitenden liegen eher bei 13.000 bis 20.000 EUR pro Monat.

Bei einer Größe von ca. 10.000 Mitarbeitenden können Unternehmen mit Kosten von 15.000 bis 25.000 EUR pro Monat rechnen.

Die größte Spannbreite zeigt sich bei den Kosten für die Implementierung. Diese ist teilweise im monatlichen Preis enthalten; für die meisten Unternehmen fallen jedoch einmalige Kosten an, die von 20.000 bis zu 250.000 EUR reichen können.

Nehmen Sie sich in jedem Fall ausreichend Zeit für die Ausschreibung und den Auswahlprozess. In der Regel dauert diese Phase zwischen drei und sechs Monaten. Eine unspezifische Auswahl aus zwei bis drei schnell eingeholten Angeboten kann hingegen keine zufriedenstellenden Ergebnisse liefern. Unserer Erfahrung nach unterscheiden sich die Kostenschätzungen teilweise um den Faktor 2 bis 3. Meist liegt dies an unterschiedlichen Annahmen und Servicelevels, aber manchmal fordern Anbieter für ihr Angebot schlicht einen zu hohen Preis, z.B. weil sie bereits gut ausgelastet sind und die Auftragsannahme Neueinstellungen erfordern könnte.

Wichtige Fragen für die Spezifikation der Anforderungen

Fragen Sie einen der vielen Managed-SOC-Anbieter nach den Kosten für seinen Service, wird seine Antwort wahrscheinlich lauten: „Es kommt drauf an. Lassen Sie uns gemeinsam die Anforderungen definieren. Wir beraten Sie gerne und zeigen Ihnen bei der Gelegenheit unser gesamtes Angebot …“.

Worauf kommt es also an?

Zunächst sollten Sie Ihr Projektziel definieren: Warum benötigen Sie ein SOC? Was wollen Sie damit erreichen? Welchen Sicherheitsgewinn versprechen Sie sich davon?

Natürlich empfehlen wir Ihnen an dieser Stelle, sich einen unabhängigen Partner zu suchen, der Sie bei der Anforderungsspezifikation und der Auswahl begleitet oder diesen Prozess ggf. sogar steuert. Alternativ können Sie auch z.B. in Ihrer CIO/CISO-Community nach Erfahrungen fragen oder – was Anbieter allerdings nicht gerne sehen – sich einfach ein erstes Angebot geben lassen und auf dieser Basis Ihre Fokusbereiche, Prioritäten und Anforderungen definieren.

Die meisten Anforderungen können folgenden Themenblöcken zugeordnet werden:

1. Allgemeines

a. Haben Sie spezielle Anforderungen an den Standort des Anbieters und die angebotenen Sprachen?

b. Benötigen Sie einen 24h/7-Service oder genügt vorerst auch eine 8h/5-Überwachung, bis das Gesamtsystem eingespielt ist?

c. Wie tief soll der Service gehen? Wir sehen bei vielen Kunden, dass sie Level 1 bis 2/3 an den Managed-SOC-Anbieter vergeben, Level 4 dann aber intern abdecken oder sogar über einen anderen, spezialisierten Incident-Response-Anbieter.

i. Level 1: Reines Monitoring

ii. Level 2: Triage von Ereignissen, Analyse und im Voraus definierte Reaktionen bei klarer Einordnung (anhand von Play- und Runbooks)

iii. Level 3: erweiterte Analyse von Logdaten, z.B. unter Nutzung der Threat Intelligence des SOC-Betreibers

iv. Level 4: aktive Incident Response, ggf. auch vor Ort; weitere Optionen: Unterstützung bei Forensik und schnelle Wiederherstellung des Normalbetriebs

d. Soll das Angebot weitere Services beinhalten, z.B. Schwachstellenmanagement oder Threat Intel?

2. Architektur und Umfang

a. Wo soll das Monitoring laufen: vor Ort in Ihrer Infrastruktur, cloudbasiert oder direkt beim SOC-Anbieter?

b. Welche Use Cases sind für Sie besonders relevant? Tipp: Starten Sie dabei besser mit zwei bis drei konkreten Use Cases und fügen Sie erst dann weitere hinzu, wenn diese optimal laufen.

c. Welche Rolle spielt die Automatisierung? Soll z.B. die Software des SOC-Anbieters im Notfall vorab definierte Playbooks durchlaufen und z.B. Gefährdete Programme isolieren?

d. Welche Aktivitäten soll das SOC grundsätzlich auf Ihrer IT durchführen dürfen?

Wichtige Fragen für die Spezifikation der Anforderungen *(fort.)*

3. Funktionen und Integration

a. Inwieweit soll die Produktionstechnik (OT) integriert werden? Nicht alle Anbieter können hier mit Referenzen aufwarten.

b. Wie sollen und können die Log-Quellen angezapft werden? Über softwarebasierte Adapter oder über zentrale Log-Server? Existiert ggf. bereits ein SIEM?

c. Wie soll das Reporting des Anbieters aussehen?

d. Wie genau sollen Ihre IT- und Security-Experten mit dem Anbieter im operativen Betrieb zusammenarbeiten: Wer ist z.B. verantwortlich für die Erstellung und Aktualisierung der Detektions-Regelsätze?

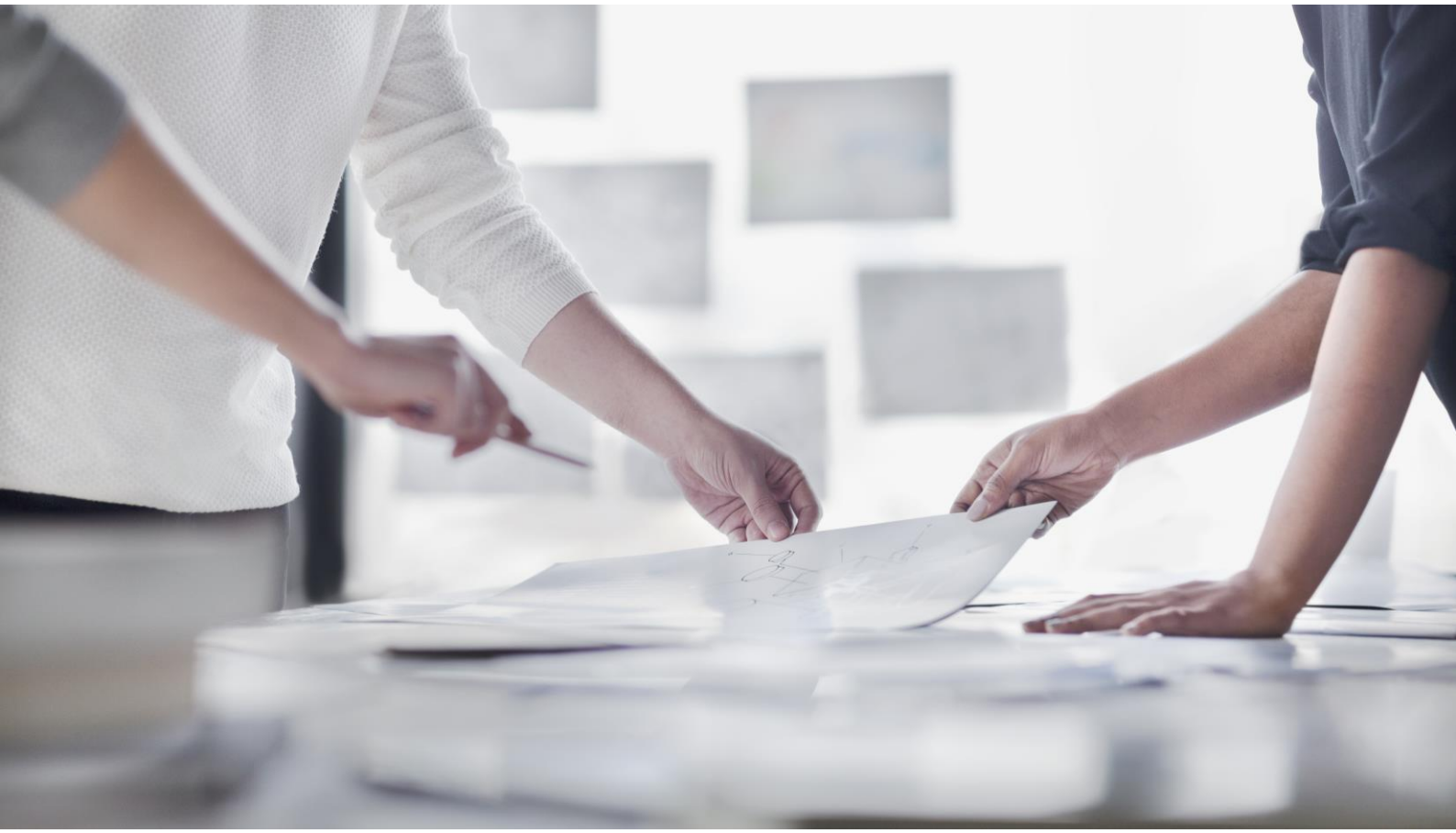
4. Geschäftsbedingungen

a. Branchenspezifische Anforderungen an die Regulatorik

b. Aufbewahrungspflichten

c. Datenschutzanforderungen, auch für Standorte außerhalb der EU

d. Zusatzangebote, z.B. einzelne Tage für weitere professionelle Dienstleistungen oder Trainings



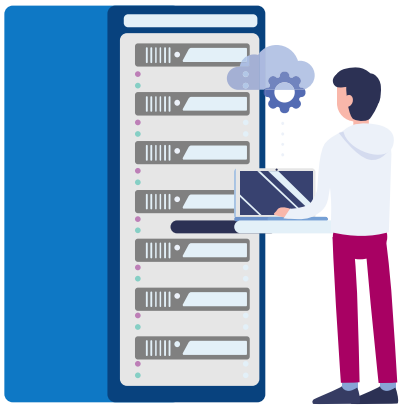
SIEM, XDR, EDR oder anbietereigene Lösungen – was ist die Ausgangsbasis?

Es wird viel diskutiert, ob man grundsätzlich mit einer SIEM-Lösung starten sollte oder eher mit einer EDR-Lösung (EDR: Endpoint Detection and Response; mit weiteren Log-Quellen auch XDR genannt: Extended Detection and Response). SIEM-Lösungen bieten in der Regel erweiterte Möglichkeiten im Bereich Log-Management und Compliance-Anforderungen, die Grenze zu EDR- und XDR-Lösungen verschwimmt jedoch zunehmend.

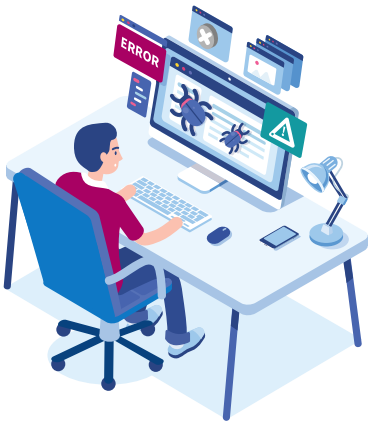
Wenn Sie dazu mehr wissen wollen, empfehlen wir Ihnen unser Whitepaper (Link).

Bei der Anbieterauswahl ist vor allem zu klären, ob Sie selbst auf die Monitoring-Plattform zugreifen oder sie sogar selbst betreiben wollen.

Grundsätzlich gibt es zwei Arten von Managed-SOC-Anbietern:



Anbieter, die ihre eigene Monitoring-Plattform nutzen. Diese kann ein gängiges SIEM-Produkt sein, welches der Anbieter selbst hostet, oder eine intern adaptierte oder entwickelte Lösung. Hier sammeln die Kunden Logging-Informationen und Events über einen Log-Server oder ihre eigene Hardware-Appliance und senden sie dann über sichere Verbindungen an den Anbieter.



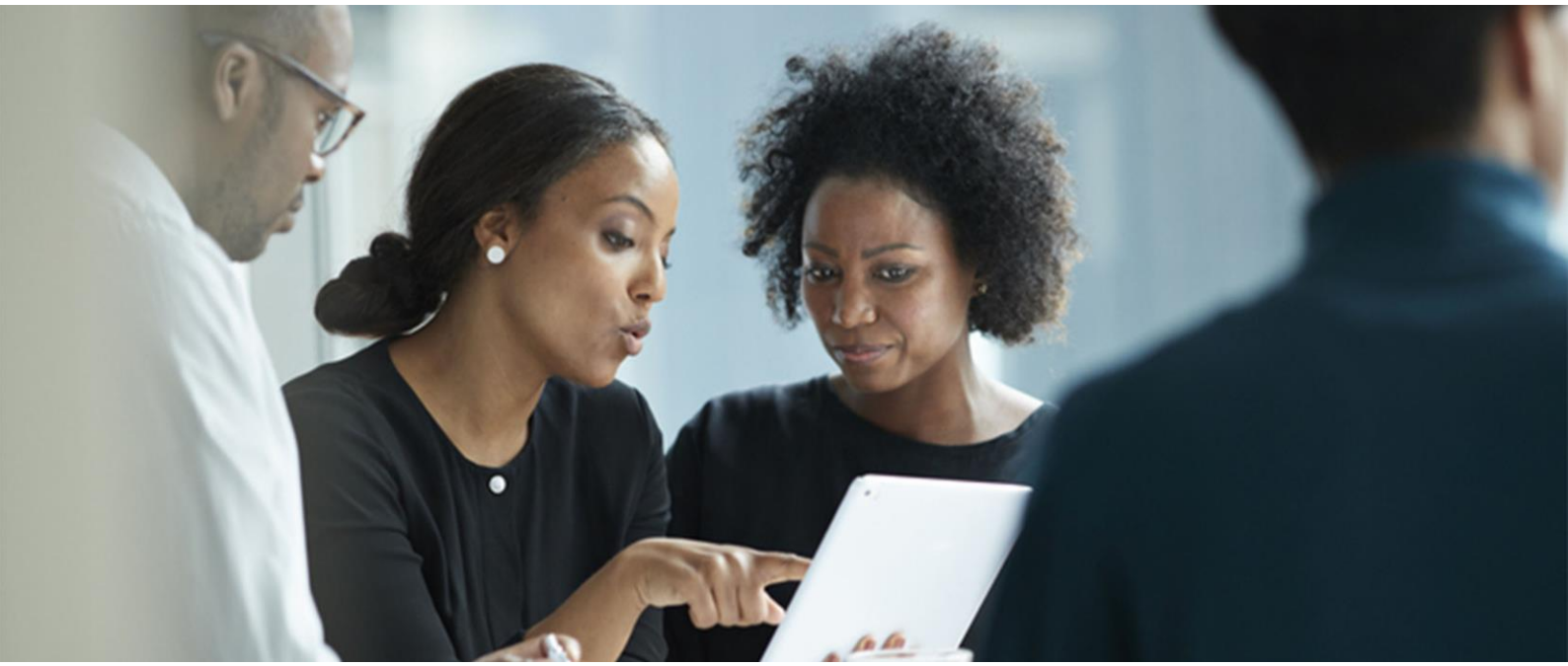
Anbieter, die die Monitoring-Plattform des Kunden nutzen oder eine solche als Teil ihres Auftrags mitbringen und implementieren. Diese kann wiederum der Kunde selbst betreiben oder der externe Anbieter im Rahmen des Projekts.

In beiden Szenarien liefern die Anbieter Use Cases, Konfigurationen und Korrelationsregeln, um das einfache Logging zum effektiven Alarmsystem auszubauen.

SIEM, XDR, EDR oder anbietereigene Lösungen – was ist die Ausgangsbasis? *(fort.)*

Die wichtigsten Vor- und Nachteile der beiden Ansätze zeigt die folgende Abbildung:

	Eigenes SIEM System mit externem SOC Betreiber	Integriertes SIEM / SOC bei externem Provider
Betriebsart	✓ **Reduzierte** Aufwände für **externes SOC** ✓ **SOC Anbieterwechsel** leichter möglich ✓ **Hybride Modelle** möglich	✓ Betrieb **komplett extern** ✓ Fokus auf **24x7 Überwachung**, **exakte Funktionsweise** der SIEM Plattform **weniger relevant**
Aufwand	✓ **Kostengünstiger Einstieg** möglich, z.B. über XDR mit Überwachungsfunktion ! **Interner Aufwand** für Betrieb + KnowHow nötig	✓ **Preisvorteile** der **SOC-Anbieter** für „Ihre“ SIEM Systeme
Funktions-umfänge	✓ **Incident Response** einfacher zu **steuern** ✓ **SIEM** kann auch für **non-Security Themen** verwendet werden ✓ Aufbau von **Know-How** im **Unternehmen** sorgt für höheres **Security-Bewusstsein**	✓ **Optimiertes KnowHow** der **SOC Anbieter** für „Ihre“ SIEM Systeme ! I.d.R. **keine volle Zugriffskontrolle** im Incident Reponse - Fall
	Wichtige Entscheidungshilfe ▪ Keine Nischenprodukte wählen ▪ Hohen internen Aufwand einplanen	**Wichtige Entscheidungshilfe** ▪ Planen von IR Management, da i.d.R. keinen direkten Zugriff auf SIEM System



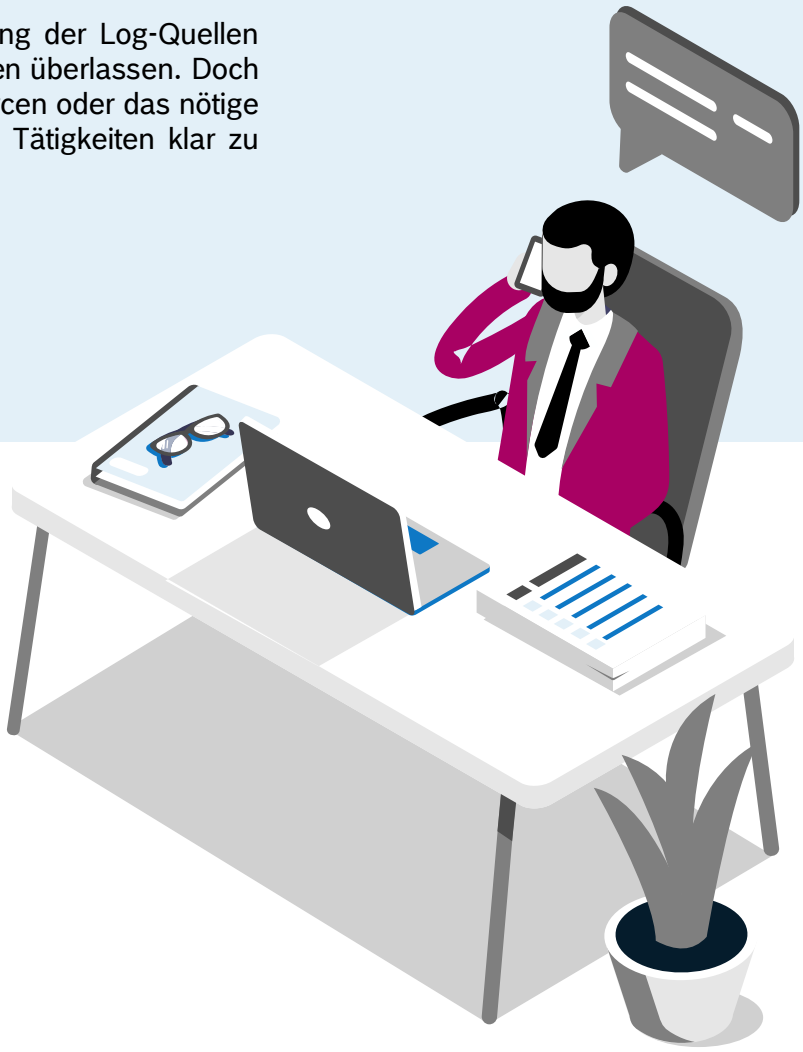
Definition der Zusammenarbeit mit dem SOC-Anbieter

Achten Sie wie bei klassischen IT-Services auch hier auf die Details der SLA. Die Reaktionszeiten der Anbieter können sehr unterschiedlich sein und sollten zu Ihren eigenen (Notfall-)Prozessen passen.

Im Krisenfall kann es entscheidend sein, ob ein SOC-Analyst nach spätestens 15 Minuten oder erst nach 2 Stunden einen kritischen Alert prüft.

Viele Anbieter versenden bereits mit ihrem Angebot eine RACI-Matrix, die festlegt, welche Verantwortlichkeiten bei Ihnen liegen und welche beim Anbieter. Ein exemplarisches RACI-Modell eines Anbieters kann hilfreich sein, um eigene Erwartungen zu definieren und dann den entsprechenden Anbieter zu wählen bzw. über Anpassungen zu verhandeln.

Missverständnisse können z.B. bei der Anbindung der Log-Quellen entstehen, die viele Anbieter zunächst den Kunden überlassen. Doch dort bestehen oft nicht die erforderlichen Ressourcen oder das nötige Wissen. Daher ist es wichtig, diese und andere Tätigkeiten klar zu verordnen.



Kriterien für Anbieter- und Angebotsvergleich

Es ist sicherlich sinnvoll, über Scoring-Modelle die Angebote den Anforderungen zuzuordnen. Unbedingt notwendige Anforderungen sollten dabei natürlich mehr Gewicht erhalten als optionale. Zu berücksichtigen sind z.B. die Fähigkeiten des Anbieters in der Operations Technology: Hat er hier nachgewiesene Erfahrung oder verweist er nur darauf, dass „alle Log-Quellen“ über entsprechende Adapter oder OT-Monitoringlösungen (z.B. Claroty, Nozomi) angebunden werden können?

Wir empfehlen jedoch, nicht nur den rein mathematischen Ansatz zu verfolgen, sondern immer auch das Gesamtbild im Blick zu behalten. Überprüfen Sie zunächst, inwiefern Ihre Anforderungen und Ausschlusskriterien zum Angebot passen, und ergänzen Sie dies um Preise, Referenzen und Ihren persönlichen Eindruck (Verlässlichkeit und Flexibilität). Auch das allgemeine Profil des Anbieters kann mit entscheiden, z.B. sollten Sie folgende Aspekte berücksichtigen: Ist der Anbieter auf SOC spezialisiert oder ist dies ein relativ neuer Zusatzservice? Bietet er ergänzende Services an, die im Krisenfall nützlich sein können (z.B. Incident Response)? Ist er global aufgestellt? Passt das zu Ihrem Setup? Ist sein Unternehmen krisenfest?

Rechnen Sie bei den Preisen am besten mit verschiedenen Szenarien: Jahr 1 inklusive Implementierung und ggf. phasenweiser Einstieg, Gesamtkosten auf drei Jahre sowie monatlich wiederkehrende Kosten (ohne Einmaleffekte). Achten Sie speziell auf die Annahmen des Anbieters: Sind diese vielleicht in Bezug auf Ihr tägliches Log-Volumen zu optimistisch? Investieren Sie hier lieber etwas mehr Aufwand, damit die Annahmen der Anbieter untereinander vergleichbar werden. Bitten Sie den Anbieter um die Möglichkeit, direkt mit seinen Bestandskunden zu sprechen und so ein ehrliches Kundenfeedback zu bekommen.

Abschließend sollten Sie den Implementierungsprozess des Anbieters unter die Lupe nehmen. Erweckt dieser eher den Eindruck eines „Quick & dirty“-Vorgehens oder liegt dem Angebot bereits ein indikativer Projektplan bei? Die Einführungsphase dauert in der Regel mindestens sechs Monate. Erste Log-Quellen lassen sich, insbesondere in Cloud-Szenarien, natürlich oft schon nach wenigen Tagen oder Wochen analysieren. Deutlich mehr Zeit vergeht jedoch, bis alle Details zu Ihrer Infrastruktur geklärt, alle relevanten Log-Quellen angebunden und die Use Cases adaptiert sind. Die wichtigste Aufgabe für den SOC-Anbieter, aber auch für Ihr eigenes Team liegt dann in der Feinabstimmung: Das Monitoring ist so zu konfigurieren, dass aus den zahlreichen Einzelevents verlässliche Alarmmeldungen generiert werden – und nicht nur ‚falsch positive‘ Meldungen. Nach der Einführung können dies z.B. Red- und Purple-Teaming-Ansätze unterstützen.

Fazit

Ein Managed SOC ist eine wichtige Komponente der Sicherheitsstrategie eines Unternehmens. Doch die Service- und Preisunterschiede der Anbieter sind enorm. Daher sollte dem Auswahlprozess auch entsprechend Zeit und Sorgfalt gewidmet werden.

Gut vorbereitet und mit einem projektbasierten Vorgehen kann jedes Unternehmen den richtigen Anbieter auswählen. Falls jedoch die Kapazität und das Know-how dafür nicht vorhanden sind, können spezialisierte externe Anbieter hilfreich sein.

Wir von Bosch CyberCompare beraten und unterstützen Sie gerne bei dieser Aufgabe – denn sie ist Teil unserer täglichen Arbeit.

Beleuchtet dieses Whitepaper wirklich alle Aspekte bei der Auswahl eines externen SOC? Nein, denn wir haben uns hier auf das Wesentliche fokussiert. Letztlich hat jedes Unternehmen individuelle zusätzliche Themen und jeder Anbieter wird weitere Fragen aufwerfen. Wir hoffen jedoch, dass wir Ihnen hiermit eine Orientierungshilfe und Denkanstöße liefern konnten. Und wie immer freuen wir uns über Ihr Feedback, gerne z.B. an cybercompare@bosch.com.

Kontaktieren Sie uns!

Zusammen stärken wir Ihre Cybersicherheit – vom transparenten Überblick über Ihr Risiko bis hin zur Auswahl passender Anbieter.

Individuell. Pragmatisch. Unabhängig.

Kontaktieren Sie das CyberCompare Management

Dr Jannis Stemmann (CEO)

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

Philipp Pelkmann (CTO)

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

Simeon Mussler (COO)

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

Verbände/Industriekooperationen von **Bosch CyberCompare**

Besuchen Sie unsere Website:
www.cybercompare.com