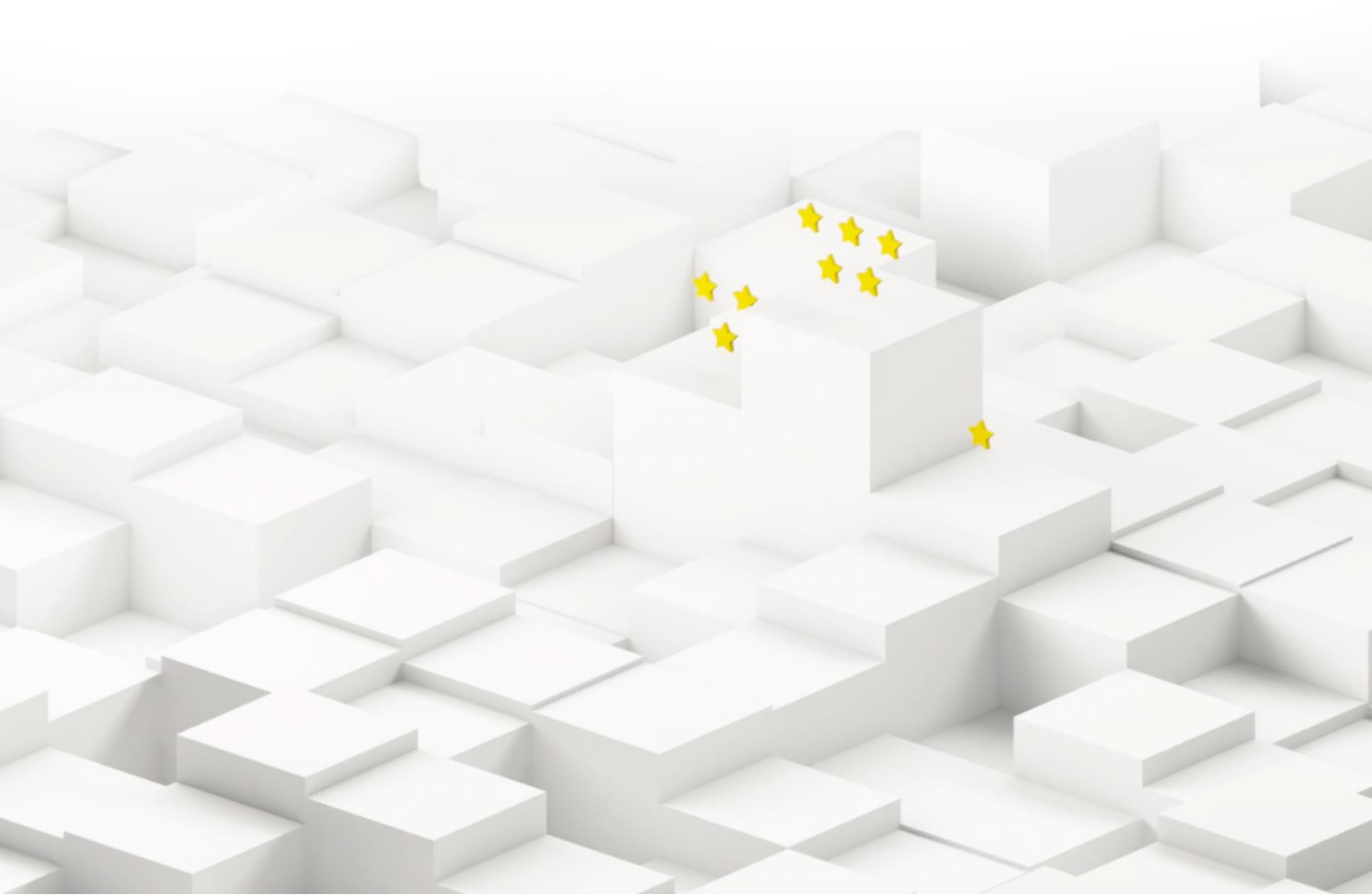
CyberCompare
A BOSCH BUSINESS

CyberCompare Whitepaper

Mit 10 Faktoren zur besten Preis-Leistung bei der Auswahl des richtigen SOC/MDR-Partners

Inkl. Kapitel zur Relevanz in öffentlichen Ausschreibungen



Agenda

1. Einleitung

Die Erkenntnis, dass die **durchgängige Überwachung** der Infrastruktur einen erheblichen Mehrwert an Sicherheit erzeugt, ist vom Mittelstand bis zum DAX-Konzern sowie im öffentlichen Sektor inzwischen verstanden. Viele Unternehmen und Kunden stehen hier vor der Entscheidung, dass Thema für die eigenen Bedürfnisse zu definieren und im Anschluss einen geeigneten Partner für die Erbringung der Leistung zu suchen.

Der **Markt ist dabei sehr unübersichtlich**, es drängen hunderte Anbieter mit teilweise unterschiedlichen technologischen Konzepten, Betriebsmodellen, Services und SLAs auf den Markt. Auf der anderen Seite ist die Investition im Bereich IT-/OT-Sicherheit von der Tragweite sowie dem Budget vermutlich die relevanteste überhaupt, was den Druck auf die Auswahl noch erhöht. Natürlich möchte die Leitung verstehen, warum da plötzlich jährlich sechsstellige Beträge überwiesen werden sollen, ob der identifizierte Partner wirklich das beste Preis-Leistungsverhältnis hat, ob man es nicht intern günstiger abbilden könnte und viele weitere relevante Rückfragen.

Aus der Erfahrung von über 70 Projekten im Bereich Security Operations Center (SOC) mit den verbundenen Themen wie der Auswahl von SIEM-Lösungen, einem MDR-Service (Managed Detection and Response - wird mal Synonym zu SOC verwendet, oder reduziert auf das Management der Endpoint Security) sehen wir folgende Bereiche im Auswahl Prozess als besonders relevant an:

Ein **klares Zielkonzept definierten**, inklusive:

1. Die technische Zielarchitektur
2. Betriebsmodell der möglichen SIEM-Lösung sowie des SOC-Betriebs
3. Reifegrad der IT-Sicherheit und Organisation
4. Integration der OT
5. Incident Response
6. Regulatorik und externe Anforderungen

Im **Angebotsvergleich** die Konzepte verstehen und bewerten, inklusive dem Fokus auf folgende Punkte:

7. Technologischer Ansatz
8. Preisbasis
9. Lizenz- und Volumenkosten
10. SLAs und Abgrenzung der Leistungen

Diese Punkte werden in den nachfolgenden Kapiteln jeweils betrachtet und mit Beispielen und Hinweisen aus unserer täglichen Praxis angereichert, um Ihnen die Auswahl auf der Suche nach einem geeigneten Partner zu vereinfachen.

Hintergrund: Managed Security Operations Center

Ein Security Operations Center (SOC) umfasst das dauerhafte Beobachten einer definierten IT- und ggf. OT-Umgebung in Bezug auf sicherheitsrelevante Ereignisse („Events“). Dazu werden in der Regel Log-Dateien und/oder Datenverkehr im Hinblick auf verdächtige Informationen analysiert. Es geht um das Aufdecken von Bedrohungsszenarien („Detect“) und der nachgelagerten, individuell passenden Gegenreaktion („Response“).

Während Großunternehmen häufig eigene SOC oder sog. Cyber Defense Center (CDC) betreiben, lohnt sich dies für mittelständische Unternehmen oft nicht: Zum einen sind qualifizierte SOC-Analysten rar, zum anderen liegt viel Expertise in den Plattformen und Werkzeugen professioneller SOC-Anbieter und die Komplexität nimmt letztlich bei einer 24/7-Überwachung zu.

Dieses 24/7-Modell wird oftmals als Standard angesehen – dabei eignen sich für kleine und mittelgroße Unternehmen zum Einstieg oft auch reduzierte Umfänge, die z.B. über Bereitschaftsdienste ergänzt werden können.

Da allein die laufenden Kosten schon bei einem kleineren Setup mindestens im sechsstelligen Euro-Bereich pro Jahr liegen und ein Onboarding in der Regel zwischen 4 – 6 Monaten benötigt, sollte ein gut strukturierter Auswahlprozess selbstverständlich sein. Unabhängige Spezialisten für den Einkauf von Cybersicherheit wie CyberCompare unterstützen CIOs und CISOs hier effizient und bringen die notwendige Struktur gleich mit.

Bei der Auswahl kann man in Summe 50 – 60 relevante Kriterien für die Differenzierung und Auswahl des passenden Managed Security Service Partner (MSSP) ansetzen, dabei setzen Unternehmen erfahrungsgemäß den Fokus auf wenige, offensichtliche Kriterien wie Preis, Ansatz der SIEM Monitoring Lösung, oder das 7x24 Modell. Je individueller Sie jedoch das SOC an die Unternehmensrisiken und das spezifische IT-Setup anpassen möchten, desto mehr sollten Sie sich mit den Services und Differenzierungsmerkmalen auseinandersetzen.

Abbildung 1

Gesteigerte Sicherheit durch ein Security Operations Center

2. Sechs Punkte für ein klares Zielkonzept

Ein klar formuliertes Zielkonzept ermöglicht eine strukturierte Ausschreibung und den Vergleich von Anbietern sowie die Sicherstellung der bestmöglichen Preis-Leistung für den Service. Gleichzeitig ist ein gutes Zielkonzept schwer zu ermitteln, da man oftmals eine Erstbeschaffung durchführt und noch keine Erfahrung damit hat, was bei der Auswahl eines Security Operations Centers relevant ist, worauf man achten muss und der Markt auch zu vertretbaren Kosten abdecken kann.

Bei der Erstellung sind viele Dimensionen relevant, auf Basis unserer Projekteerfahrung aus über 70 SIEM/SOC/MDR-Projekten, haben wir die, aus unserer Sicht relevantesten Punkte formuliert:

1. **Die technische Zielarchitektur**

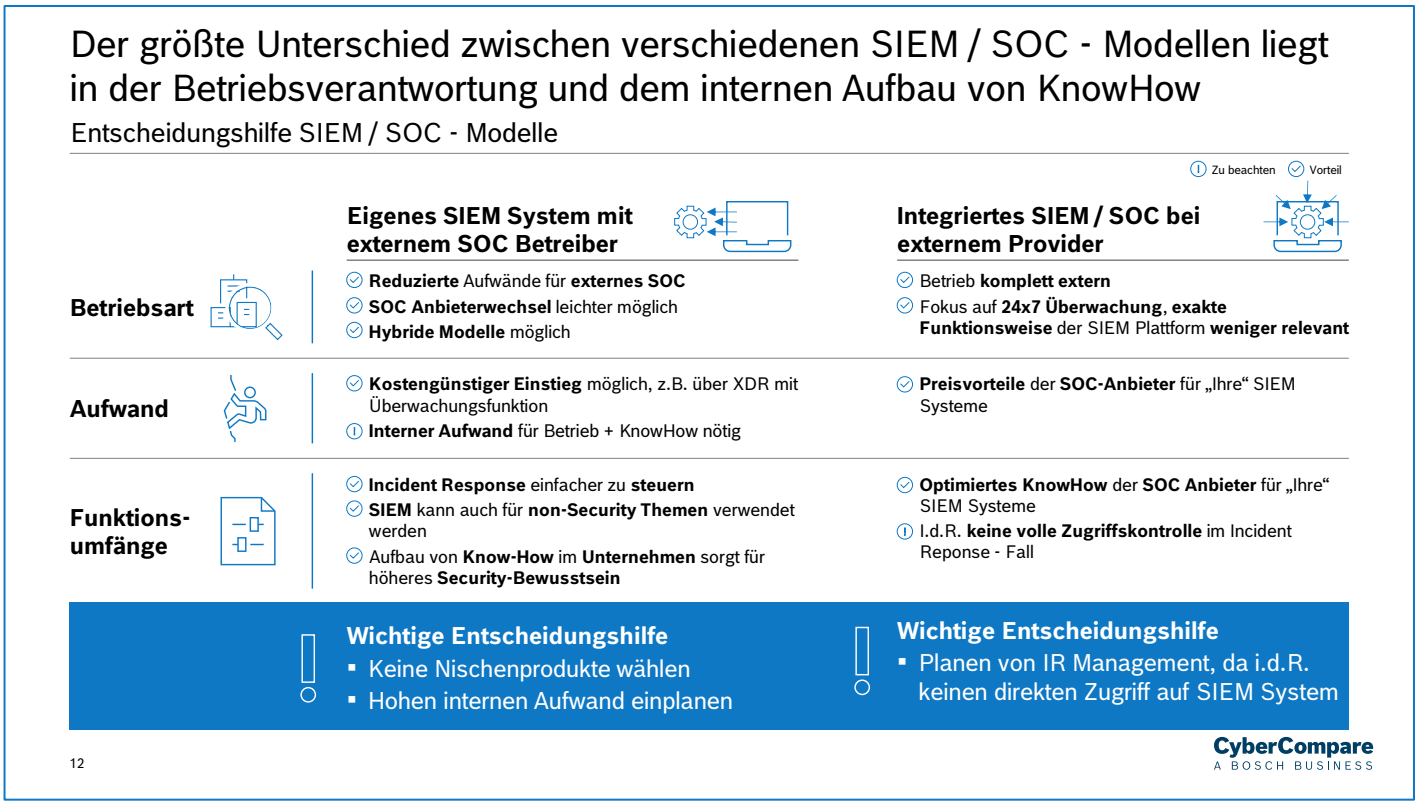
- **Soll das SOC/MDR EDR, XDR oder SIEM-basiert arbeiten?**
  Die Gretchenfrage bei der Auswahl und umfassend an dieser Stelle kaum zu beantworten. Eine erste Einschätzung zum derzeitigen Stand, wissend das bei der derzeitigen Entwicklung am Markt sich dies rasch ändern könnte.
  Ein **Endpunktbasierter Service (Basis EDR)** mit einer 7x24h Überwachung der Alarme bietet einen guten Zugewinn an Sicherheit und ist gleichzeitig in Implementierung und Kosten noch handhabbar. Einige Hersteller von EDR-Lösungen bieten diesen Service direkt an, oder man wendet sich an einen Dritten als MSSP.
  Die Erweiterung über eine XDR-Lösung, welche auf der EDR-Lösung aufbaut und weitere Quellen anschließt, erweitert die Absicherung, da auch die Datenbasis für die Angriffserkennung vergrößert wird. Das Vorgehen und die Anbieter sind ähnlich zu einem EDR-basierten Vorgehen.
  Die SIEM-basierte Variante ist der „Klassiker“, hier können vielfältig Log-Quellen angeschlossen und korreliert werden, die Protokollierung erfolgen und auch Non-Security Use-Cases umgesetzt werden. Hier gibt es die meisten Anbieter und zumindest bisher ist dieses Vorgehen am häufigsten. Durch die schnelle Entwicklung der XDR-Lösungen könnte hier jedoch zeitnah ein Paradigmenwechsel anstehen.

- **Auf Basis welcher Endpointsecurity Lösung soll der SOC-Service erbracht werden?**
  Dies ist relevant, da neben der Einbindung auch die Reaktion aus dem SOC häufig über die EDR-Lösung erfolgt. Ein SOC-Partner sollte also die bestehende Lösung integrieren können. Falls derzeit keine EDR-Lösung im Einsatz ist oder die bestehende Lösung zur Disposition steht, sollte eine Entscheidung zum Henne-Ei gefunden werden – entweder man definiert eine EDR-Lösung und sucht sich einen geeigneten SOC-Partner dafür oder man geht lösungsoffen in die Ausschreibung und nimmt dann die EDR-Lösung, die der SOC-Partner integrieren kann.

- **Gibt es weitere Lösungen, die integriert werden sollen?**
  Sind weitere Lösungen im Einsatz bzw. geplant und sollten diese zumindest angeschlossen werden bzw. ebenfalls vom SOC-Partner überwacht werden. Dies können Lösungen rund um NDR (Network Detection and Response), OT/IoMT Anomalie-Erkennung, IAM/PAM Lösungen, Schwachstellen-Scan etc. sein.

2. Betriebsmodell des Security Data Lakes (SIEM oder XDR-basiert)

- **Welche Umfänge intern abbilden, was soll nach außen gegeben werden?** Einige unserer Kunden wünschen den Security Data-Lake intern abzubilden. Dies kann v.a. mit Blick auf die Datenhoheit in Einzelfällen sinnvollsein, ist eine Abwägung zwischen vorhandenen Ressourcen, Know-how, das aufgebaut werden müsste und damit der Kosten inkl. Personal im Betrieb. Typischerweise liegt der Security Data-Lake in der SIEM-Lösung des Anbieters und wird somit in Anbindung und Betrieb nach extern vergeben.



- **Macht ein „Co-Managed“ oder „Hybrid“ Modell Sinn?**
  In einigen Fällen kann ein gemeinsames Konzept zwischen SOC-Partner und Kunde Sinn ergeben, wenn beispielsweise bereits eine Lösung intern im Einsatz ist oder interne Ressourcen und Wissen aufgebaut werden sollen. Eine solche Lösung bedarf einer exakten Beschreibung in der Ausschreibung und schränkt den Anbietermarkt deutlich ein. Dies kann sich sowohl auf die SIEM-Lösung als auch den SOC-Betrieb beziehen.

- **Wie wird die Protokollierung abgebildet, bspw. für forensische Analysen?** Die Protokollierung der Logs sollte im Konzept betrachtet werden, insbesondere bei kritischer Infrastruktur nach dem BSIG. Im Angriffsfalle sollten die Logs über einen längeren Zeitraum (meist 3-6 Monate) verfügbar sein. Es sind auch kostengünstigere Speicheroptionen möglich für ältere Logs („Cold-Storage“).

3. Reifegrad der IT-Sicherheit und Organisation

- **Sind wir in der Lage die Alarme des SOC-Partners auch abzuarbeiten und können eine 24/7-Abdeckung leisten?**
  Ein SOC, welches einen Angriff erkennt, nach vereinbarten Playbooks aber nicht direkt reagieren darf und dann telefonisch niemanden erreichen kann ist Geldverschwendung.
  Es muss auch intern an den Prozessen und der Verfügbarkeit bspw. über eine telefonische Bereitschaft gesprochen werden. Dies erfordert häufig interne Abstimmungen, da häufig Arbeitnehmervertreter einzubeziehen sind etc.

- **Soll der SOC-Partner direkt in das Netzwerk oder die Endpunkte eingreifen können?**
  Die Frage der Reaktion wird meist im Onboarding definiert. Es ist trotzdem sinnvoll bereits frühzeitig sich ein Bild zu machen und mögliche Interventionen auf in der Ausschreibung bereits zu berücksichtigen.

4. Integration der OT/IoMT/IoT und weitere

- **Habe ich Betriebstechnik in Form von OT, IoT oder IoMT aus der Produktion, den klinischen Netzen, der Gebäudetechnik, der Netzsteuerung oder weitere Quellen, die eingebunden werden sollen?**
  Diese Bereiche werden meist über eine dedizierte Lösung zur Anomalie-Erkennung abgedeckt und die Assets nicht einzeln in eine SIEM-Plattform o.ä. eingebunden. Die Alarme aus diesen Lösungen werden dann meist in das SOC geleitet und dort im Rahmen des 7x24h Monitorings analysiert.
  Daher ist es relevant, falls eine solche Lösung zum Einsatz kommen sollte, zum einen SOC-Partner zu finden, der mit der entsprechenden Lösung gut umgehen kann bzw. die Lösung als Paket direkt mit auszuschreiben. Ein weiterer Punkt ist das der SOC-Partner für die Analyse der Alarme aus den Betriebsnetzen eine entsprechende Kompetenz benötigt, um diese nachzuverfolgen, um bspw. einschätzen zu können ob es sich um einen Fehlalarm handeln könnte oder eskaliert werden muss.

5. Incident Response

- **Möchte ich neben dem SOC-Service auch die forensische Analyse und den Wiederanlauf durch den SOC-Partner durchführen lassen?**
  Viele unserer Kunden wünschen hier einen Service aus einer Hand, es gibt auch Gründe, die dagegen sprechen können. Eine kurze Zusammenfassung der Argumente für das jeweilige Vorgehen:

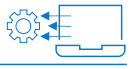
Servicemodelle von SIEM-/XDR- und SOC-Anbietern

ⓘ Zu beachten ✓ Vorteil

Incident Response wird auch vom SOC-Betreiber erbracht (im SOC-Angebot inkludiert)

- ✓ Der **Gesamt-Service** von Tier 1 bis Tier 4 wird **durchgängig** erbracht. Keine Diskussion der Verantwortlichkeiten
- ✓ Einmaliges **Onboarding** eines Anbieters (Ist-Erfassung, Geschäftskritische Prozesse, Ersatz-Kommunikationslösungen,...)
- ✓ ‚**Single Point of Contact**' Prinzip mit vereinfachter Kommunikation
- ✓ **Bündelung** der Services SOC und IR kann **Kostenvorteile** haben
- ✓ **Ergänzende Leistungen** wie Krisenübungen mit positivem Effekt auf SOC und IR

Incident Response findet außerhalb des SOC statt (zusätzlicher Anbieter contracted)



- ✓ Großer Markt an **spezialisierten IR-Anbietern**. Nicht jeder SOC-Anbieter hat dedizierte & gute IR-Fähigkeiten
- ✓ Der **IR-Service** kann in der Regel **individueller** gestaltet werden (Stundenpakete, SLA, ungenutzte Stunden für andere Services,...)
- ✓ Es kann sinnvoll sein, bewusst ein **Gegengewicht zum SOC-Anbieter** zu schaffen: IR kommt in der Regel ins Spiel, wenn das SOC den Angriff nicht frühzeitig erkannt hat
- ✓ **Preis-Leistung** kann durch eine separate Ausschreibung ggf. günstiger bezogen werden (besser Fit zu den individuellen Anforderungen)
- ✓ **Transparente Trennung** zw. Tier 1-3 und Tier 4 (IR) hilfreich für interne Aktivitäten im Krisenfall gemäß **Notfallplan**

20

CyberCompare
A BOSCH BUSINESS

6. Regulatorik und externe Anforderungen

- **Welche regulatorischen Anforderungen bzw. Kundenforderungen sind bereits vorhanden oder zukünftig absehbar (bspw. BSIG, DORA, B3S, Kunden-Audits und -Fragebögen)?**
  Der frühzeitige Check nach externen Anforderungen von Seiten Behörden, Verbände oder Kunden ist ein starker Einflussfaktor.
  Bei der behördlichen Seite sind die entsprechenden Anforderungen zu berücksichtigen, wie die Orientierungshilfe des BSI zu Systemen zur Angriffserkennung, wenn das BSIG zutrifft.
  Auch Anforderungen von Kunden sind sehr relevant, ob explizit als Zertifikat bzw. Audit oder auch durch die häufigen Rückfragen zu dedizierten Tools. So kann aus diesen Gründen beispielsweise der „klassische Weg“ über ein SIEM-basiertes System den etwas innovativeren und für diese Kundesituation möglicherweise ebenfalls passende XDR-basierte Ansatz vorzuziehen sein.

Diese und weitere Themen besprechen wir typischerweise mit unseren Kunden in mehreren Workshops und bringen dabei unsere Expertise sowie die Marktsicht ein, wenn eine Anforderung gestellt wird, was heißt das für den Anbietermarkt, den Preis und die Komplexität bei der Auswahl. Dabei gehen wir meist modular vor und erarbeiten methodisch die Anforderungen aus dem Zielkonzept um daraus die Ausschreibung als Lastenheft vorzubereiten und entsprechend vergleichbare Angebote der Anbieter einzuholen. Die ermöglicht eine effiziente Auswahl, eine bestmögliche Preis-Leistung sowie eine qualitativ hochwertige Entscheidung, die sich nach innen und außen transparent nachvollziehbar argumentieren lässt.

Exkurs: Zielkonzept eines SOC im Rahmen öffentlicher Ausschreibungen

Warum ist ein klares Zielkonzept bei öffentlichen Ausschreibungen im Fokus?

1. **EU-Schwellenwert meist überschritten**
   Eine SOC-Ausschreibung über 3 oder 5 Jahre liegt meist über dem Schwellenwert zu einer europaweiten Ausschreibung, selbst bei Sektorenauftraggebern. Dies erfordert eine hohe Genauigkeit und Qualität den Vergabedokumenten und klar definiertes Zielkonzept, um Bieterfragen und Rügen zu vermeiden.

2. **Je nach Vergabeform muss vorher sehr genau spezifiziert werden**
   Die Möglichkeit während der laufenden Ausschreibung noch den Ansatz zu ändern oder Anforderungen anzupassen sind bei einer öffentlichen Ausschreibung stark eingeschränkt – abhängig von der Vergabeart. Dies ist komplex, da es sich bei einem Managed Security Operations Center um ein Zusammenspiel aus Technik und Dienstleistung handelt. Hier in der Leistungsbeschreibung und dem Leistungsverzeichnis so trennscharf und spezifisch zu sein, um einen „guten Anbieter“ zu erhalten, ist eine große Herausforderung. Insbesondere bei einem offenen Verfahren ist die komplex, da die Wirtschaftlichkeit alleine papierbasiert mit den eingehenden Angeboten ermittelt wird und der beste Bieter hier den Zuschlag erhält. Wir raten eher zu einem Verhandlungsverfahren, um den Partner kennen zu lernen und die Feinheiten im Angebot gemeinsam durchzugehen bevor ein finales Angebot gelegt wird.

3. **Weniger Anpassungsmöglichkeiten im Verfahren**
   Bei öffentlichen Vergaben entfällt die Möglichkeit sich erstmal einige Anbieter anzuschauen und dann zu überlegen, was man „eigentlich wollte“. In Rahmen von Markterkundungen ist dies mit Abstrichen vielleicht möglich, aber auch hier muss auf die genauen Rahmenbedingungen geachtet werden und es verzögert den Ablauf.
   Die formalen Mindestanforderungen und Bewertungskriterien sind vorab bekannt, auf dieser Basis allein darf die Entscheidung fallen, dies setzt ein klares Zielkonzept und hohen Fokus auf die frühe Phase der Projekte, um geeignete Bieter und Angebote und eine gute Vergleichsbasis für die Entscheidung zu erhalten.

4. **Vergleichbarkeit relevant, sonst muss man günstigeren nehmen obwohl nicht „eigentlich“ gewünschte Leistung**
   Das Resultat einer nicht trennscharfen Bewertungsmatrix kann am Ende sein, dass an einen Bieter vergeben werden muss, der nicht unbedingt der Traumpartner ist. Natürlich kann man die Vergabe versuchen aufzuheben etc., aber das erzeugt das Risiko von Rügen, muss sehr gut begründet werden und verzögert den Prozess stark.
   Umso wichtiger sind die Punkte oben sowie die generelle methodische Vorgehensweise in Vorbereitung einer öffentlichen Ausschreibung

Insbesondere bei öffentlichen Kunden, haben wir hier die Projekte erheblich effizienter und mit höherer Qualität zum Abschluss bringen können. CyberCompare hat über 50 Projekte im öffentlichen Sektor begleitet, viele davon mi dem Fokus auf SzA/SOC/SIEM/MDR etc. Insgesamt sind es über 500 Projekte zu Beratung und Beschaffung von IT- und OT-Sicherheit inkl. Architektur der IT-Sicherheit und Angriffserkennung

Darunter auch Projekte mit folgenden öffentlichen Auftraggebern (Auswahl), häufig inkl. deutschland- bzw. europaweiter Ausschreibung und Vergabe:

- System zur Angriffserkennung bei Universitätskliniken in Deutschland
- NDR und SOC bei einem Krankenhaus in Niedersachsen
- OT-Anomalie-Erkennung inkl. SOC für einen Energie- und Gasnetzbetreiber in Norddeutschland
- Managed SIEM bei einem Flughafen in Süddeutschland
- Endpoint-Sicherheit und Awareness-Lösung für ein Krankenhaus in Norddeutschland
- System zur Angriffserkennung in IT und OT bei einem Nahverkehrsbetrieb in Süddeutschland sowie einem in Niedersachsen
- Endpoint Security für eine Stadtverwaltung in Norddeutschland
- Stadtwerke in Ostdeutschland für ein System zur Angriffserkennung (SzA)

3. Den passenden SOC-Anbieter auswählen entlang der vier Auswahlfaktoren

Ein methodisch ausgewählter SOC-Partner steigert nicht nur erheblich die Sicherheit, sondern ermöglicht auch erhebliche Kosteneinsparungen.

Ein klar definiertes Zielkonzept führt zu einem strukturierten und trennscharfen Lastenheft bzw. Leistungsverzeichnis. Daraus werden über die Ausschreibung aussagekräftige Angebote eingereicht, welche vergleichbar sind und dadurch die Auswahl der besten Preis-Leistung ermöglichen.

Der Vergleich der Angebote sind oft Äpfel und Birnen, die Preisspanne zwischen dem günstigsten und teuersten Anbieter ist oft >300%. Daher lohnt sicher der Fokus auf folgende Faktoren sieben bis zehn:

7. **Technologischer Ansatz**
   Wie bereits im Zielkonzept ausführlich beschrieben, hat der technologische Ansatz im Design und auch dem Vergleich der Angebote einen großen Einflussfaktor.
   Beim Security Data Lake und der Korrelation der Daten gibt es verschiedene Optionen. SOC/MDR, die auf EDR-Lösungen aufbauen, solche die zusätzliche Quellen Anbinden im Rahmen eines Extended Detection and Response ("XDR"). Die "klassische" Variante baut auf einer SIEM-Lösung auf (Varianten: Beim Anbieter, in der Cloud, beim Kunde) - alles hat Auswirkungen auf den Preis und die Komplexität.

8. **Preisbasis**
   Das klassische Preismodell basiert auf den Logvolumen pro Tag. Dies ist leider ein Schmerz bei jeder Ausschreibung und ein Henne-Ei-Dilemma. Der Anbieter will keinen Preis nennen, wenn er die Log-Volumen nicht kennt und der Kunde weiß ohne einen Security Data-Lake (den er ja gerade einkaufen möchte) nicht, welche Volumen er hat. Über Sizing und Rechner kann man sich annähern, aber es verbleibt ein Unterschied. Teilweise gehen Anbieter auch dazu über bspw. nach Anzahl Endpoints zu bepreisen, dies macht es erheblich einfacher.

9. **Lizenz- und Volumenkosten**
   Teilweise werden z.B. EDR-Lizenzen mit angeboten. Kompliziert wird es, wenn in einem Angebot die Kosten für die Log-Volumen enthalten sind und beim anderen nicht - oft in Verbindung mit MS Sentinel als SIEM-Lösung, da hier sowohl die Lizenz als auch die Log-Volumen (Achtung: ja, die muss man auch bezahlen) direkt vom Kunden bezahlt werden müssen. Hier kann man versuchen Schätzungen abzugeben, es ist jedoch immer nicht 100% vergleichbar zum Zeitpunkt der Entscheidung.

10. **SLAs und Abgrenzung der Leistungen**
    Bei den SLAs ist die Reaktionszeit auf einen Incident meist am kritischsten (logisch bei einem SOC...). Zum einen die angegebene Zeitspanne aber auch die Abgrenzung der Zeitspanne - also wann die Stoppuhr losgeht und wann sie angehalten wird. Hier sehen wir das unter 1 Stunde von der Alarmierung (bspw. Alert aus System, Anruf von Kunde) bis zur Einleitung einer Reaktion (bspw. Isolation Endpoint, Anruf bei Notfallkontakt) vergehen sollte. Manche Anbieter gehen da noch deutlich drunter.

Die Komplexität bei der Definition und dem Angebotsvergleich wird oft unterschätzt, hier lohnt sich die Zusammenarbeit mit einem unabhängigen Partner, wie CyberCompare. Das stellt sicher, dass die Qualität der Entscheidung hoch ist, die Ausschreibung effizient verläuft und die beste Preis-Leistung gewinnt.

Warum CyberCompare nutzen?

- Wir machen das jeden Tag
- Wir können auf Basis der Erfahrung eine Ausschreibung beschleunigen und die Qualität erhöhen, um ein optimales Preis-Leistungsverhältnis zu erzielen und einen geeigneten Partner bzw. Produkt auszuwählen
- Wir verstehen die Differenzierungsmerkmale von Lösungen und Leistungen
- Wir wissen, wie Anforderungen gestellt werden können, ohne den Wettbewerb zu stark einzuschränken und trotzdem spezifisch zu sein, die Abwägung zwischen internen Wünschen und der Marktsicht

Themen, die wir mit Kunden bearbeitet haben

- Architektur und Beschaffung von Security-Produkten und -Services
- Zielkonzepte, Leistungsverzeichnis/-beschreibung, Angebotsauswertung, Klärung von Bieterfragen bis zur Begleitung von europaweiten Ausschreibungen
- Ausschreibungsvorbereitung und -begleitung bei Themen wie Endpoint-Security (EDR, XDR) über Systeme zur Angriffserkennung, OT-Monitoring, Security Operations Center (SOC), SIEM-Lösung bis zu Incident Response

Ihre Vorteile mit CyberCompare als Plattform

- Unabhängige Plattform im Auftrag des Kunden, keine finanzielle Beziehung zu den Anbietern
- Standardisierte Spezifikationen sorgen für einen schnelle Start der Angebotseinholung
- Erfahrung mit öffentlichen Ausschreibungen und Vergaben sowie der Bereitstellung von Leistungsverzeichnissen und -beschreibungen
- Transparente und klare Empfehlungen erleichtern die Entscheidungsfindung bei der Auswahl von Produkten

CyberCompare
A BOSCH BUSINESS

Besuchen Sie
Unsere Webseite:
cybercompare.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
Jannis.Stemmann@de.bosch.com
Tel. +49 711 811-44954

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

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

Verbände/Industriekooperationen von **CyberCompare, A Bosch Business**

grow platform GmbH, Grönerstr. 9, 71636 Ludwigsburg, Germany