CyberCompare Whitepaper

3 mögliche SIEM-Lösungen für Ihr externes Managed SOC

Sie suchen den passenden Partner für Ihr Managed Security Operations Center (SOC) – doch wissen nicht, wie Sie dabei vorgehen sollen? Keine Sorge: Wir unterstützen Sie dabei. Bei der Wahl des richtigen Managed-SOC-Partners ist die Frage nach dem Umgang mit dem Security Information and Event Management (SIEM) von zentraler Bedeutung. Wir zeigen Ihnen im Folgenden alle Varianten mit ihren Vor- und Nachteilen – und erklären Ihnen auch, wie und aus welchen Gründen sich unsere Kunden für welche SIEM Variante entscheiden.

Die grundsätzlichen technischen Fragen zur Einführung einer SIEM-Lösung (bspw. Cloud vs. On Prem Nutzung) können im Rahmen dieses Whitepapers nicht abgehandelt werden. Wir unterstützen Sie aber auch hier sehr gerne individuell mit Konzeptberatung oder konkreten SIEM-Ausschreibungen und begleitenden Services.

3 mögliche SIEM-Lösungen für Ihr externes Managed SOC

Prinzipiell sehen wir drei Möglichkeiten, um das Theme Security Information and Event Monitoring für Ihr managed SOC sinnvoll umzusetzen:

- Variante a) Aufbau einer eigenen SIEM-Lösung. Sie entwickeln die Lösung selbstständig oder mit einem Partner.
- Variante b) Zugriff auf das SIEM des SOC-Anbieters. Sie überführen die Logs in das System des Managed-SOC-Anbieters, können jedoch auf die Daten zugreifen.
- Variante c) Kein Zugriff auf das SIEM des SOC-Anbieters. Der Partner betreibt ein SIEM, auf das Sie jedoch keinen Zugriff haben.

Während die Variante a) den Fokus vorrangig auf die vollständige Hoheit über die eingesetzte Technologie, die Funktionen und das technische Know-How legt, bietet Variante c) eine höhere Kosten-Effizienz und oftmals auch ein kürzere Ramp-Up Zeit. Der „Mittelweg“ ist klassischerweise die Variante b), die aus unserer Sicht Vorteile beider „Extremvarianten“ vereinen versucht, dabei aber auch gewisse Einschränkungen mit sich bringt.

Im Folgenden wollen wir Ihnen die drei Varianten anhang von konkreten Beispielen unserer Arbeit näher bringen und Ihnen so einen Leitfaden zur Auswahl der für Sie passendsten Variante geben. Das Thema Security Operations Center inkl. SIEM stellt einen wichtigen Schwerpunkt unserer Arbeit dar und wir stehen natürlich für alle Fragen und Anmerkungen zur Verfügung.

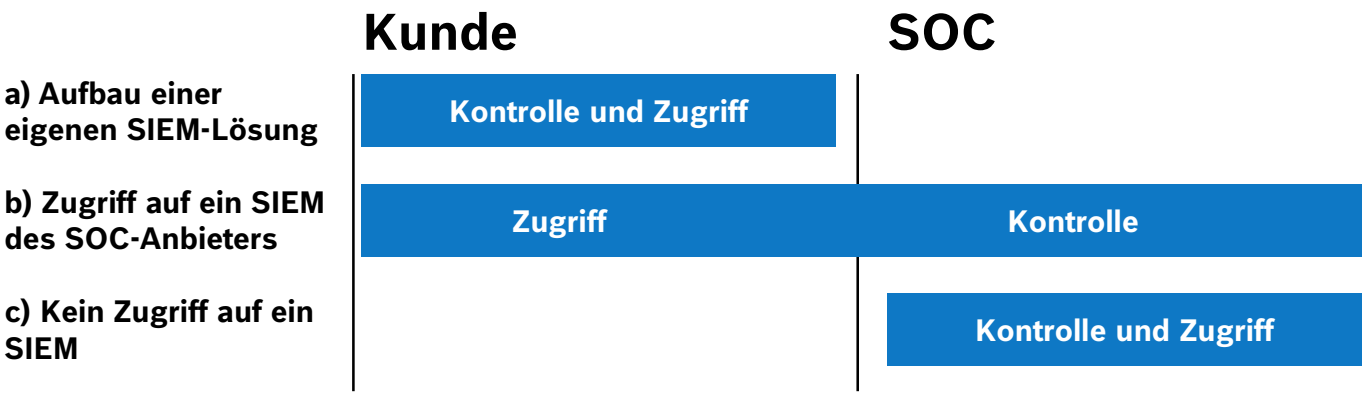
Die SIEM-Varianten im Detail – was sind die Vor- und Nachteile?

Abbildung 1: Unterschiede zwischen eigener SIEM-Lösung mit externem Managed-SOC-Part-ner und Managed SOC mit integriertem SIEM

Zu beachten
Vorteil

	Eigenes SIEM-System mit externem SOC-Betreiber	Integriertes SIEM/ SOC bei externem Provider
Betriebs-art	✓ **Reduzierte** Aufwände für **externes SOC** ✓ **SOC-Anbieterwechsel** leichter möglich ✓ **Hybride Modelle** möglich	✓ Betrieb **komplett extern** ✓ Fokus auf **24×7 Überwachung, exakte Funktionsweise** der SIEM-Plattform **weniger relevant**
Aufwand	✓ **Kostengünstiger Einstieg** möglich, z.B. über XDR mit Überwachungs-funktionen ! **Interner Aufwand** für Betrieb und Know-How 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 **Unterneh-men** sorgt für höheres **Security-Bewusstsein**	✓ **Optimiertes Know-How** der **SOC-Anbieter** für „Ihre“ SIEM-Systeme ! I.d.R. **keine volle Zugriffskontrolle** im Incident-Response-Fall
Wichtige Entschei-dungshilfe	! Keine Nischenprodukte wählen ! Hohen internen Aufwand einplanen	! Planen von IR-Management, da i.d.R. keinen direkten Zugriff auf SIEM-System

Abbildung 2: SIEM-Varianten im Überblick



BOSCH

Variante a) Aufbau einer eigenen SIEM-Lösung

Viele Unternehmen entschließen sich trotz des hohen Aufwands für den Aufbau einer eigenen SIEM-Lösung. Dabei können sie die Lösung entweder selbst oder mithilfe von Partnern im Unternehmen umsetzen und mit eigenen Ressourcen betreiben. Sie können auch ein „Managed SIEM“ einkaufen – dabei übernimmt ein Partner dann Implementierung und Betrieb. Diese Variante ist dann aber meist nur noch wenig von einem Managed SOC entfernt, bei dem dann zusätzlich die Security-Alarme analysiert werden.

Vorteile

- **Nutzung für umfangreiche Anwendungsfälle, über die reine Angriffserkennung hinaus**
  SIEM-Tools können Funktionen enthalten, um spezifische Anforderungen durch Standards und Regulatorik nachzuverfolgen. Ein Beispiel ist das klassische Log-Management: Die Daten können genutzt werden, um die Einhaltung von Compliance-Vorgaben zu überprüfen, Risiken einzuschätzen und bei möglichen Audits Transparenz herzustellen.
- **Geringer Aufwand beim Wechsel des Managed-SOC-Partners**
  Eine unabhängige SIEM-Lösung in eigener Verantwortung ermöglicht den Wechsel des Managed-SOC-Anbieters, ohne die Implementierung wieder von vorne zu starten. Ein gut laufendes SIEM-System benötigt üblicherweise einige Monate, bis das Finetuning abgeschlossen ist. Allerdings legt ein Managed-SOC-Anbieter seine Security-Konfigurationen meist nicht offen und zieht sie als Intelectual Property am Ende der Vertragslaufzeit wieder ab.
- **Individuelle Entscheidung des Unternehmens**
  In diesem Szenario kann sich ein Unternehmen für das am besten passende SIEM-Produkt entscheiden – bei den anderen Varianten wird die Auswahl in der Regel durch den SOC-Anbieter getroffen.

Nachteile

- **Hoher Aufwand und Bedarf an Experten**
  Die Einführung einer SIEM-Lösung ist mit hohem Aufwand verbunden: Bis alle Quellen angeschlossen sind, die Korrelation reibungslos funktioniert und die Alerts mit geringen „False-Positive“-Raten wirken, vergeht viel Zeit. Die Regeln müssen erstellt und gewartet und die Use Cases Schritt für Schritt eingeführt werden. Im eingeschwungenen Zustand sind meist zwei bis drei Mitarbeitende für den Betrieb der SIEM-Lösung notwendig – als Basisanforderung; bei komplexen Systemen sind noch mehr Mitarbeitende gefragt.
- **Höhere Kosten für Lizenzen**
  Je nach Vorgehen im Zusammenspiel mit dem Partner für das Managed SOC können bei einer eigenen SIEM-Lösung insgesamt höhere Lizenzkosten entstehen. Dies ist insbesondere davon abhängig, ob der Managed-SOC-Partner mit den Kundenlizenzen arbeitet oder ein eigenes SIEM betreibt, das ebenfalls lizenziert werden muss. Diese Kosten sind dann im Gesamtpreis des Managed SOC enthalten.
- **Know-how notwendig**
  Der Aufbau einer SIEM-Lösung verlangt neben den Fachkräften für die Ausführung auch (lösungs-)spezifisches Wissen. Solche Systeme sind hochkomplex und erfordern so entweder bereits erfahrene Mitarbeitende oder intensive Trainings, um die reibungslose Implementierung sowie den späteren Betrieb sicherzustellen.

Variante b) Zugriff auf das SIEM des SOC-Anbieters (1/2)

Zwischen „ganz oder gar nicht“ gibt es einen Raum für Zwischenlösungen. Hierbei wird das SIEM durch den Managed-SOC-Partner aufgesetzt, meist auch betrieben, und der Kunde kann darauf zugreifen – in verschiedenen Abstufungen (z.B. eigene Use Cases definieren oder nur lesen). Für diese Variante gibt es zwei Ausprägungen:

- **Der Kunde bezahlt eine Lizenz für eine SIEM-Lösung (Cloud oder On Prem).** Hier werden die verschiedenen Logs gesammelt. Der Managed-SOC-Partner zieht diese Daten dann meist in eine eigene Umgebung und definiert dort die Regeln, Use Cases etc. Teilweise macht der Anbieter dies auch direkt in der Kundenumgebung.
- **Der Managed-SOC-Anbieter betreibt ein SIEM und erlaubt dem Kunden den Zugriff.** Hierbei werden die Daten über Log-Kollektoren (bei Anbietern technisch unterschiedlich umgesetzt) auf die Systeme des Managed-SOC-Anbieters übertragen und dort weiterverarbeitet. Der Anbieter ermöglicht es dem Kunden jedoch, ebenfalls auf die SIEM-Lösung zuzugreifen.

In jedem Fall werden Anbieter auch hier meist ihre Intellectual Property, d.h. ihre Regeln und Konfigurationen, schützen.

Vorteile (1/2)

- **Eigene Überwachung und eigenes Reporting der Systeme möglich**
  Durch den direkten Zugriff können die Systeme auch teils selbst überwacht und die zentrale Protokollierung der Logs für unterschiedliche Auswertungen genutzt werden. Im Falle eines kritischen Incidents (nach dem Handover durch das SOC an den Kunden) kann der Kunde das SIEM zur Ursachenklärung und Lösung des Problems nutzen. Er kann die Incidents auch selbst verfolgen.
- **Aufbau von internem Wissen**
  Durch den Zugriff ohne den eigenen Betrieb kann der Kunde im Laufe der Zeit eigenes Wissen aufbauen, um zukünftig die SIEM-Lösung ggf. komplett intern zu betreiben
- **Einfacherer Wechsel**
  Je nach Ausprägung ist ein Wechsel einfacher, da die Logs bereits an zentraler Stelle protokolliert sind. So kann ein wechselnder Partner für den Managed-SOC-Service schneller implementiert werden. Der sicherheits-relevante Teil kommt jedoch über den entsprechenden (neuen) Anbieter – daher ist der Vorteil nicht so stark zu gewichten.

Nachteile

- **Einschränkung der Anbieter**
  Nicht alle Managed-SOC-Anbieter ermöglichen eine Lösung mit Kundenzugriff. Kunden haben daher weniger Auswahl, um ein gutes Preis-Leistungs-Verhältnis zu finden. In Projekten haben wir jedoch gesehen, dass ein guter Angebotsvergleich durchaus möglich sein kann.
- **Unklar definiert**
  Variante b) kann das Beste aller Varianten miteinander vereinen – oder auch das Schlechteste. Kunden sollten daher ganz genau hinsehen, damit sie am Ende wirklich den Service erhalten, den sie sich vorstellen. Wir begleiten zahlreiche Unternehmen in genau diesem Prozess.

Variante b) Zugriff auf das SIEM des SOC-Anbieters (2/2)

Zwischen „ganz oder gar nicht“ gibt es einen Raum für Zwischenlösungen. Hierbei wird das SIEM durch den Managed-SOC-Partner aufgesetzt, meist auch betrieben, und der Kunde kann darauf zugreifen – in verschiedenen Abstufungen (z.B. eigene Use Cases definieren oder nur lesen). Für diese Variante gibt es zwei Ausprägungen:

- **Der Kunde bezahlt eine Lizenz für eine SIEM-Lösung (Cloud oder On Prem).** Hier werden die verschiedenen Logs gesammelt. Der Managed-SOC-Partner zieht diese Daten dann meist in eine eigene Umgebung und definiert dort die Regeln, Use Cases etc. Teilweise macht der Anbieter dies auch direkt in der Kundenumgebung.
- **Der Managed-SOC-Anbieter betreibt ein SIEM und erlaubt dem Kunden den Zugriff.** Hierbei werden die Daten über Log-Kollektoren (bei Anbietern technisch unterschiedlich umgesetzt) auf die Systeme des Managed-SOC-Anbieters übertragen und dort weiterverarbeitet. Der Anbieter ermöglicht es dem Kunden jedoch, ebenfalls auf die SIEM-Lösung zuzugreifen.

In jedem Fall werden Anbieter auch hier meist ihre Intellectual Property, d.h. ihre Regeln und Konfigurationen, schützen.

Vorteile (2/2)

- **Ressourcenschonend und eigenes Know-how weniger relevant**
  Die Implementierung und der Betrieb durch einen externen Partner reduzieren sowohl den Umsetzungsaufwand als auch das benötigte interne Know-how. Das bedeutet aber nicht, dass der Kunde alles abgeben kann: Um die Vorteile zu nutzen, ist auch eigene Kapazität notwendig.

Nachteile

Variante c) Kein Zugriff auf das SIEM des SOC-Anbieters

Das ist der häufigste Fall bei einer Ausschreibung zu einem Managed SOC: Der Partner greift die Logs aus den verschiedenen Quellen auf (technisch je nach Anbieter unterschiedlich gelöst), verarbeitet sie in seinen Systemen und erzeugt damit Alerts. Der Kunde hat in der Regel zwar definierte Dashboards und Reports, häufig auch in Echtzeit, jedoch keine Möglichkeit, direkt zuzugreifen. Für viele Unternehmen ist diese Variante auch völlig ausreichend, da sie weder die Ressourcen noch das Know-how besitzen, um sich in die SIEM-Lösung einzuarbeiten.

Vorteile

- **Geringer Ressourcen- und Know-how-Bedarf**
  Die Lösung schneidet insgesamt meist am günstigsten ab im Vergleich zu den anderen beiden Varianten, da weniger eigene Mitarbeitende involviert sind und kaum bis gar kein Know-how benötigt wird. Die Implementierung bleibt aber dennoch zeitaufwendig.
- **Nutzung der Erfahrung der spezialisierten SOC-Anbieter**
  Bei Betrieb und Kontrolle der Log-Daten, Alerts und Use Cases durch den Partner sowie beim gesamten SOC-Prozess kann auf alle Vorlagen, Erfahrungswerte und Blueprints zurückgegriffen werden. Die Partner können mit ihrer präferierten SIEM-Lösung arbeiten, mit der sie auch für andere Kunden tätig sind, und so effizient und zielgerichtet vorgehen.
- **Großer Markt, viele Anbieter, gutes Angebot**
  Je weniger Vorgaben gestellt werden, und in dieser Variante sind es im Vergleich deutlich weniger, umso größer ist der Kreis möglicher Anbieter und die Konkurrenz um den Auftrag.

Nachteile

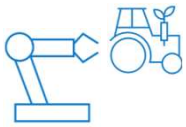
- **Möglichkeiten des SIEM-Zugriffs verhindert**
  Die in den vorherigen Abschnitten beschriebenen Vorteile, die ein Zugriff auf die SIEM-Lösung bietet, sind in dieser Variante nicht möglich.
- **Incident Response mit potenziell erschwertem Informationsfluss**
  Im Falle eines Angriffs ist der Zugang zu den Daten im SIEM erschwert (wenn der Managed-SOC-Anbieter nicht auch der Incident-Response-Partner ist – ebenfalls eine mögliche Aufstellung). Der Kunde sollte in der Angebots- und Implementierungsphase darauf achten, welche Daten beispielsweise für Forensik zur Verfügung gestellt werden können.

Beispiele – so entscheiden sich unsere Kunden für ein SIEM

Im Folgenden geben wir Ihnen zwei Beispiele aus unseren Kundenprojekten und zeigen auf, wie sich die Unternehmen für eine der drei Varianten entschieden haben:

Variante a) Aufbau einer eigenen SIEM-Lösung

Kunden-profil



Produzierendes Unternehmen im Agrarsektor mit globaler Aufstellung und mehreren tausend Mitarbeitenden

Anforderungen und Ergebnis des Angebotsvergleichs

Der Kunde hatte seine Log-Daten bereits in eine Azure-Sentinel-Cloud-Umgebung eingebracht und war aktiv dabei, diese SIEM-Lösung auch für eigene Auswertungen zu nutzen. Beim Thema Security und Monitoring war das Unternehmen gut aufgestellt und daher auch in der Lage, ein solches System zu betreiben und zu entwickeln. Der globale Footprint des Kunden machte die Situation jedoch komplexer.

Vorgabe war, dass der Partner für die 24/7-Überwachung im Rahmen eines Managed SOC in der Umgebung des Kunden arbeiten und diese mit seiner Erfahrung optimieren sollte, statt die Daten (wie in den meisten anderen Fällen) auf eine eigene Umgebung ziehen und erst dort zu verarbeiten. Dies führte zu zwei Einschränkungen bei der Auswahl:

- Einige Anbieter waren nicht bereit, Ihre Erfahrungen zu teilen und direkt die Kundenumgebung zu optimieren. Sie verwiesen dabei auf eine eigene IP sowie die Nutzung externer Quellen, beispielsweise für Threat Intelligence.
- Einige Anbieter hatten keine oder nur geringe Erfahrung mit Azure Sentinel. Eine solche Einschränkung kann häufig vorkommen, unabhängig von der Lösung.

Gemeinsam mit unserem Kunden konnten wir gemäß ihren Anforderungen passende Angebote einholen und ein gutes Preis-Leistungs-Verhältnis bei hoher Qualität sicherstellen.

Variante c) Kein Zugriff auf das SIEM des SOC-Anbieters

Kunden-profil

Ein Hersteller von Hobbyprodukten mit ca. 2.500 Mitarbeitenden im deutschsprachigen Raum und mit mehreren Standorten, alle regional im DACH-Raum

Anforderungen und Ergebnis des Angebotsvergleichs

Im Fokus des Angebotsvergleichs lag die 24/7-Abdeckung der Angriffserkennung und -reaktion. Die IT-Abteilung des Unternehmens war aufgrund der Personalkapazitäten und des Know-hows nicht darauf ausgelegt, selbst ein SIEM-System zu betreiben oder zu nutzen; auch die 24/7-Abdeckung der Analyse war intern nicht möglich.

Wir haben eine klare Angebotsabfrage und einen Angebotsvergleich für ein Managed-SOC durchgeführt. Dabei „sammelt“ der Managed-SOC-Anbieter die Security Logs auf den Kundensystemen und überführt sie in seine eigenen Systeme – dies wird von den Anbietern technisch unterschiedlich abgebildet.

- Viele angefragte Anbieter konnten nur ein („Ihr“) verwendetes SIEM abbilden. Je nach SIEM - System konnte die Anbindung zum Kundensystem besser oder schlechter dargestellt werden
- Die Anbieter konnten teilweise nur eingeschränkte Verfügbarkeiten für die 24/7-Analyse der Log-Dateien am Standort Deutschland anbieten. Für den Kunden war der Ort der Datenverarbeitung eine wichtige Anforderung, sodass manche Anbieter hier weniger in Frage kamen.

Der Managed-SOC-Anbieter ist also für die gesamte Kette zuständig: von der Log-Kollektion, der zentralen Protokollierung, Korrelation und Automatisierung (siehe auch: SOAR) bis hin zur Analyse der Alerts und der mit dem Kunden abgestimmten und freigegebenen Reaktion. Zusammen mit unseren Kunden konnten wir auf Basis der beschriebenen Anforderungen die besten Anbieter identifizieren, passende Angebote einholen und aufgrund der hohen Vergleichbarkeit attraktive finanzielle Rahmenbedingungen für den final ausgewählten Anbieter sichern.

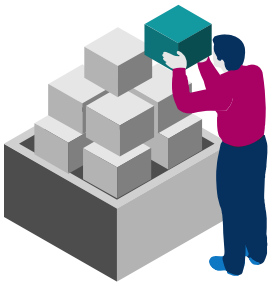
Das können wir Ihnen empfehlen

Die Frage nach dem richtigen SIEM für Ihr Unternehmen kann nur individuell beantwortet werden – dafür stehen wir Ihnen natürlich gern zur Verfügung. Sprechen Sie uns an, um Ihre spezifische Situation zu diskutieren.

Dennoch können wir Ihnen basierend auf unserer Erfahrung einige Empfehlungen abgeben:

5 Gründe für eine eigene SIEM-Lösung, auch bei einem Managed SOC

- Mit Ihrem eigenen Team bleibt die Sicherheit in Ihrer Hoheit.
- Bei einem Anbieterwechsel bleibt das bereits gut laufende System bei Ihnen.
- Wenn spezifische Use Cases (z.B. Compliance) notwendig sind, sind diese bei eigenem Zugriff auf die SIEM-Lösung einfacher umsetzbar.
- Bei komplexen globalen Organisationen mit vielen Standorten ist der Aufwand bei der Implementierung besonders hoch – hier kann die SIEM-Lösung wirklich bestmöglich individuell ausgewählt werden.
- Eine Zwischenlösung kann ein „Managed SIEM“ sein, bei dem ein Partner für Implementierung und Betrieb zuständig ist, Sie jedoch die Kontrolle behalten.



Grundsätzlich lässt sich sagen, dass bei großen und komplexen Organisationen sowie bei spezifischen Anforderungen der Aufbau einer eigenen SIEM-Lösung sinnvoll sein kann.

5 Gründe für ein komplettes Managed SOC (ohne eigene SIEM-Lösung)

- Die Lizenzkosten für eine eigene SIEM-Lösung sind in vielen Fällen reduziert (abhängig vom Modell entfallen sie sogar ganz).
- Es braucht weniger Mitarbeitende, besonders wenn das System schon eingespielt ist.
- Die IT-Architektur Ihres Unternehmens wird nicht komplexer (z.B. durch aufwändiges Software-Lizenz- und Lifecycle-Management).
- Es ist kein eigenes Know-how erforderlich – das SIEM wird von den Anbietern komplett verwaltet, Ihr Unternehmen hat kaum Berührungspunkte.
- Sie können das Managed Service als vollständige Leistung von extern beziehen und auf der Expertise und der unternehmensübergreifenden Erfahrung der Anbieter aufsetzen.

Die Variante eines kompletten Managed SOCs inklusive SIEM-Lösung kann aus unserer Perspektive vor allem für kleinere Unternehmen mit begrenzter Kapazität in IT und Security Fachbereich Sinn ergeben.

Was ist ein Security Operations Center?

Ein Security Operations Center (SOC) umfasst das dauerhafte Beobachten einer definierten IT-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.

Was ist ein SIEM?

SIEM-Lösungen wurden entwickelt, um Ereignisprotokolldaten aus mehreren Anwendungen, Systemen, Netzwerkgeräten und Servern zu aggregieren und zu analysieren, um verdächtige Ereignisse zu erkennen. Hierdurch lässt sich feststellen, ob die Sicherheit oder Geschäftskontinuität gefährdet sind. Durch die Kombination der Fähigkeiten der Sicherheitsereigniskorrelation (SEC), des Sicherheitsereignis-managements (SEM) und des Sicherheitsinformationsmanagements (SIM) bietet die SIEM-Lösung sowohl Echtzeit- als auch Verlaufsanalysen von Sicherheitsereignissen. Sie können bei der Untersuchung von Vorfällen und im Compliance-Reporting helfen, da sie Kontext-, Verlaufs- und Ereignisdaten aus mehreren Quellen in der gesamten IT-Infrastruktur gründlich analysieren. Moderne SIEM-Lösungen sind fortschrittlicher als frühe Systeme, die lediglich Daten aus verschiedenen Quellen gesammelt und protokolliert haben. Jetzt kann SIEM-Software typischerweise umfassende Einblicke in die Netzwerksicherheit und den Datenschutz liefern, indem sie nach anomalen Aktivitäten im IT-Netzwerk sucht, die auf Compliance-, Leistungs- und Sicherheitsprobleme hinweisen könnten. Durch das Sammeln und Analysieren detaillierter Protokolle von Ereignissen kann ein SIEM in Echtzeit Einblicke zu potenziellen Sicherheitsbedrohungen geben.

BOSCH

CyberCompare

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