# 6 Tipps für den Aufbau eines Physical Security Operations Center

Seit ich vor fünf Jahren die britische Armee verlassen habe, um im Bereich Unternehmenssicherheit und Risikomanagement zu arbeiten, habe ich von zahlreichen Sicherheitsverantwortlichen gehört, habe ich zahlreiche Sicherheitsverantwortlichen gehört, die mit Überzeugung für oder gegen die Einrichtung eines Security Operations Center (SOC) eintreten. Die Vorteile eines SOC liegen zwar auf der Hand – einschließlich einer stärkeren Sicherheitsstruktur und einer verbesserten Transparenz potenzieller Risiken – aber nicht jedes Unternehmen sieht die Notwendigkeit oder ist bereit, seine Sicherheitsabläufe zu zentralisieren.

Diejenigen, die dazu bereit sind, fallen in der Regel in eine von zwei Kategorien:

1. Ihr Unternehmen hat eine kritische Masse an Infrastruktur, Mitarbeitern und Ansehen erreicht, die nun mehr Aufsicht und Kontrolle erfordert.

2. Sie haben sich bisher auf ein gut vernetztes Netzwerk regionaler und länderspezifischer Sicherheitsmanager verlassen, um Risiken auf lokaler Ebene zu erkennen und zu managen, benötigen nun aber einen zentraleren Ansatz.

Jüngste Ereignisse und Herausforderungen – von den durch die COVID-19-Pandemie ausgelösten neuen und erhöhten Risiken bis hin zu der steigenden Zahl immer raffinierterer Cyberangriffe – sprechen ebenfalls für den Aufbau eines SOC.

Unabhängig von den Gründen dafür hat mich die Erfahrung gelehrt, dass der Aufbau eines SOC von den Verantwortlichen für Sicherheit und Risiken aber zunächst einmal die richtige Denkweise erfordert. Nachfolgend finden Sie sechs wichtige Tipps, wie Sie dies erreichen können. Beachten Sie, dass es sich hierbei nicht um eine erschöpfende Liste von Anleitungen handelt, sondern um einen kurzen Überblick darüber, was Sicherheits- und Risikofachleute wissen und tun sollten, um ihre Sicherheitsfunktionen erfolgreich zu zentralisieren.





Dataminr

## #1: Setzen Sie nichts voraus

Wahrscheinlich verfügen Sie über ein bestehendes Sicherheitsnetzwerk, um das herum oder auf das Sie Ihr SOC aufbauen können. Das SOC wird jedoch ein neues Betriebsmodell mit neuen Arbeitsweisen haben. Setzen Sie also nicht voraus, dass jeder in der Organisation versteht, was ein SOC ist oder was es leisten soll.

Gehen Sie stattdessen besser davon aus, dass niemand weiß, was ein SOC ist und wie es aufgebaut werden soll. Vergewissern Sie sich von Anfang an, dass alle Beteiligten zustimmen, steuern Sie Ihre Kommunikation sorgfältig und schaffen Sie klare Kommunikationswege zwischen dem SOC-Team und den wichtigsten Geschäftsbereichen und Partnern.

## #2: Betonen Sie die Bedeutung von Schnelligkeit und Präzision

Leistungsstarke SOCs werden durch genaue Echtzeitinformationen angetrieben. Es ist schwierig, die Präzision und Schnelligkeit von Informationen vor der Aktivierung vollständig zu testen, und die Verantwortlichen sollten darauf vorbereitet sein, dass Mängel in Echtzeit aufgedeckt werden. Dies ist zwar eine der größten Herausforderungen bei der Inbetriebnahme Ihres SOC, aber auch eine der am einfachsten zu lösenden.

Widerstehen Sie dem Drang, unter der Prämisse zu arbeiten, dass jede Information, die im SOC eingeht, nur dem SOC bekannt sein wird. Das ist ein weit verbreiteter Fehler, der dazu führt, dass aus der Angst heraus, andere zu stören, Informationen gehortet werden. Dies kann durch eine Kultur vermieden werden, in der es unendlich viel besser ist, Geschäftspartner ein paar Mal zu stören oder abzulenken, als sie ein einziges Mal mit einer Horrornachricht schockieren zu müssen.

Bestimmen Sie als Best Practice:

- Was als erstes mit den Informationen zu tun ist
- Was die Auswirkungen zweiter und dritter Ordnung sind
- Wer außer dem unmittelbaren Sicherheitsumfeld im Unternehmen die Informationen noch kennen muss

## #3: Stellen Sie Mitarbeitern Fähigkeiten zur Verfügung, statt Mitarbeiter an Fähigkeiten zu binden

Es gibt eine scheinbar endlose Reihe von Technologien zur Unterstützung von Sicherheitsoperationen. In Kombination mit internen Überwachungssystemen kann die Technologie den Eindruck erwecken, dass sie Sie steuert und nicht umgekehrt. Übernehmen Sie die Kontrolle, indem Sie eine Übersicht erstellen:

- Was wird benötigt, um einen gewissen Grad an Voraussicht zu schaffen?

- Was ist erforderlich, um Ereignisse zu erkennen, sobald sie eintreten?
- Wie lässt sich der Informationsfluss, der durch die Verknüpfung von Technologie und Menschen entsteht, optimieren?

In einer idealen Welt gäbe es eine nahtlose Integration und Arbeitsabläufe mit minimalen Informationsüberschneidungen, aber so funktioniert es selten. Wenn Sie einen klaren Endzustand, ein Betriebsmodell und eine Systemarchitektur haben, die auf den Menschen ausgerichtet ist, können Sie Ihre Entscheidungen mit klarem Verstand treffen.

## #4: Versuchen Sie, Mehrwert zu schaffen

Sicherheit ist eine Kostenstelle. Die erste Frage, die Ihr Führungsteam wahrscheinlich stellen wird, lautet: „Wie viel?“ Um das Gespräch in die richtige Richtung zu lenken, erstellen Sie einen Geschäftsplan, der den Wert des SOC für das gesamte Unternehmen aufzeigt. Es ist wichtig, dass Sie über Ihr Team hinausblicken und Möglichkeiten identifizieren, die andere Teile des Unternehmens unterstützen.

Die wichtigsten Fragen, um den Mehrwert des SOC aufzuzeigen, sind:

- Wo kann ich greifbare und nicht greifbare Beziehungen aufbauen, die zum Business Case beitragen?
- Wie kann ich anderen Geschäftsbereichen helfen, ihren Wert effektiver zu steigern, ohne ihr eigenes Fachwissen oder ihre Fähigkeiten zu gefährden?
- Wie kann ich auf eine bestehende Fähigkeit zurückgreifen und Partnerschaften aufbauen, um sie zu unterstützen?

Auf den ersten Blick wird es wahrscheinlich so aussehen, als ob der größte Teil der Kosten des SOC durch die Zentralisierung der Sicherheitsabläufe und die dadurch erzielten Effizienzgewinne gedeckt wird. Diese Annahme wird mehr kosten, als Sie denken – vor allem, wenn Ihr SOC rund um die Uhr aktiv sein soll. Deshalb ist es umso wichtiger, dass Sie den Wert, den das SOC bieten wird, klar formulieren.

## #5: Planen Sie von Anfang an Redundanzen ein

Man wird Ihnen unweigerlich mehr abverlangen, als Sie zu leisten vermögen. Das bedeutet, dass Sie Ihrem Team Zeit geben müssen, um Informationen zu verarbeiten und kritisch über deren Auswirkungen nachzudenken. Teams, die unter extremem Druck stehen oder ständig arbeiten, machen Fehler und übersehen Dinge.

Beides kann sich Ihr SOC nicht leisten, vor allem nicht in der Anfangsphase. Aber neue Systeme und Arbeitsabläufe brauchen Zeit, um verstanden, angepasst und optimiert zu werden. Planen Sie genügend betriebliche Redundanz ein, um Ihrem Team die Zeit zu geben, die es braucht, um die Kapazität mit um die Kapazität an die stark fluktuierende Arbeitslast anzupassen zu variieren. Das Team wird dann in der Lage sein, das Betriebstempo des SOC umzustellen oder zu beschleunigen, wenn sich eine Krise anbahnt.

## #6: Schaffen Sie ein SOC, das für die Zukunft gerüstet ist

Es gibt viele laufende Debatten und Gespräche darüber, ob SOC für Cybersicherheit und physische Sicherheit zusammengelegt werden sollten. Ich habe an mehreren solchen Gesprächen teilgenommen und weiß aus erster Hand, wie kompliziert es sein kann, zwei getrennte SOC zusammenzuführen. Sie basieren auf unterschiedlichen Prinzipien, sind nach unterschiedlichen Funktionen segmentiert und können sich an verschiedenen Standorten mit unterschiedlichen Betriebsmodellen befinden.

Berücksichtigen Sie beim Aufbau Ihres SOC, wie es zukünftigen Anforderungen gerecht werden kann. Technologie, die heute für einen bestimmten Zweck geeignet ist, kann es schon morgen nicht mehr sein. Geld, das Sie durch Investitionen in eine Technologie sparen, die „für den Moment gut genug“ ist, kann schon bald unzureichend sein und Sie dazu veranlassen, Ihre Sicherheitsstrategie zu überdenken.

Erstellen Sie eine Roadmap für Ihr SOC und überprüfen Sie die Roadmaps Ihrer Partner und Lieferanten. Dann fragen Sie sich selbst:

- Ist es wahrscheinlich, dass mein Unternehmen in naher Zukunft die Bereiche Cybersicherheit und physische Sicherheit zusammenführen wird?
- Was kann ich tun, um die Konvergenzdiskussion voranzutreiben?
- Wie kann ich den Wandel vorantreiben, statt ihn nur zu empfangen?

Und vor allem: Wie kann ich mein SOC gegen das nächste große Risiko oder die nächste Störung absichern?

**Al Bowman** ist ein Enterprise Account Manager bei Dataminr. Bevor er zu Dataminr kam, entwickelte, etablierte und leitete er das Intelligence Services Center von Deloitte in London. Davor diente er in der britischen Armee, wo er zuletzt als Direktor des globalen Risiko- und Aufklärungszentrums tätig war.





Dataminr