PLANUNG UND AUFBAU EINES SOC

Best Practices für den Aufbau eines Physical Security Operations Center (SOC)

DATAMINR PULSE

Einleitung

Sie und Ihr Team haben den Auftrag erhalten, das erste physische Security Operations Center Ihres Unternehmens aufzubauen. Das Projekt wird von einer Führungskraft gesponsert, es gibt einen überzeugenden Anwendungsfall und ein entsprechendes Budget. Ihr Ziel ist es nun, ein hochleistungsfähiges SOC aufzubauen, das den immer komplexeren Risiken, mit denen Ihr Unternehmen heute konfrontiert ist, gewachsen ist. Dieses E-Book soll Ihnen dabei helfen, die Mitarbeiter, Prozesse, Technologien und Leistungsmerkmale zu identifizieren, die für den Aufbau eines erstklassigen SOC erforderlich sind.

Risikoereignisse als Trigger

Wenn Unternehmen die Entscheidung treffen, ihr erstes SOC aufzubauen, haben sie oft bereits einen Risikovorfall erlebt – und zwar einen, auf den ihr bestehendes physisches Sicherheitsteam nur mit Mühe effizient reagieren konnte. Solche Vorfälle können das Managementteam eines Unternehmens zum Handeln anspornen und untermauern den Business Case für zusätzliche Investitionen in die Unternehmenssicherheit.

Im Folgenden finden Sie einige Beispiele für Risikoereignisse, die wir bei unseren Kunden beobachtet haben und die diese dazu veranlasst haben, ihr erstes SOC aufzubauen:

- Der CEO eines Unternehmens befand sich in einer Niederlassung seiner Firma in einer Besprechung, als er vor dem Gebäude Schüsse hörte. Die vor Ort tätigen, externen Sicherheitskräfte verriegelten die Bürotüren und forderten die Mitarbeiter auf, drinnen zu bleiben, aber die Krisenintervention war chaotisch und die Mitarbeiter hatten Angst. Der CEO rief später das Sicherheitsteam seines Unternehmens an und musste feststellen, dass die Mitarbeiter keine Ahnung hatten, dass in der Nähe des Büros eine Schießerei stattgefunden hatte.

- 2017 wurde Mexiko-Stadt von einem schweren Erdbeben erschüttert, das Dutzende von Gebäuden zum Einsturz brachte und Hunderte von Menschen tötete. Ein großes amerikanisches Unternehmen unterhielt mehrere Bürostandorte in Mexiko-Stadt und musste sich schnell um seine Mitarbeiter und Führungskräfte kümmern. Nachrichtenmeldungen gingen nur langsam ein und waren nicht so detailliert, wie es das Sicherheitsteam für die Planung von Evakuierungsmaßnahmen gebraucht hätte.

- In den ersten Wochen der COVID-19-Pandemie waren Einzelhändler mit einem sich schnell ändernden Flickenteppich von staatlichen, regionalen und kommunalen Gesundheitsvorschriften konfrontiert. Ein großes amerikanisches Einzelhandelsunternehmen hatte Mühe, sich einen vollständigen Überblick über die behördlichen Beschränkungen zu verschaffen, die seine Standorte im ganzen Land betrafen. Unabhängig davon bat das Management des Einzelhändlers das Sicherheitsteam um tägliche Lageberichte über die Anzahl der COVID-19-Fälle, die sich aus öffentlichen Quellen manuell allerdings nur schwer zusammenstellen ließen.

Wie Sie Ihr Security Operations Center gestalten, hängt vom Budget, dem Risikoprofil und den Zielen Ihres Unternehmens ab. Jedes zentralisierte Sicherheitsteam hat, unabhängig von seiner Größe, der Branche oder dem Zuständigkeitsbereich, vier gemeinsame Merkmale:

- **Echtzeitinformationen** fließen in das Sicherheitsteam ein und dienen als wichtige Grundlage für die Entscheidungsfindung.
- **Analysten** untersuchen Echtzeitinformationen und entscheiden, ob Maßnahmen zur Risikominderung ergriffen werden sollen.
- Maßnahmen zur Risikominderung gehen in **Workflow-Prozesse** ein, die wiederholbar, skalierbar und messbar sind.
- Das Team **meldet die Ergebnisse des SOC** an das Unternehmen zurück, um weitere Investitionen in das Programm zu bewirken.

Trotz dieser ähnlichen Merkmale gibt es keinen Standardansatz für die Entwicklung oder Skalierung einer zentralisierten Sicherheitsabteilung. Deren Umfang und Zuständigkeiten hängen von dem einzigartigen Risikoprofil Ihres Unternehmens, seiner Risikotoleranz, seiner Führung, seiner Unternehmenskultur und anderen Faktoren ab.

Dataminr arbeitet eng mit Hunderten der weltweit leistungsfähigsten SOC zusammen und hat dadurch einen einzigartigen Einblick in die Best Practices der Branche.

Wir haben erlebt, dass Unternehmen ähnlicher Größe, in der gleichen Branche und mit einem ähnlichen.

Risikoprofil ihr zentrales Sicherheitsteam auf vollkommen unterschiedliche Weise aufgebaut haben. In einem Beispiel entschied sich Unternehmen A für ein großes globales Security Operations Center, während sich Unternehmen B für einen dezentralen Ansatz mit kleinen, regionalen Teams entschied, die weitgehend unabhängig voneinander arbeiten.

Trotz dieser gravierenden operativen Unterschiede sind Echtzeitinformationen ein entscheidender Faktor dafür, wie Sicherheitsteams handeln, um ihre Mitarbeiter und Vermögenswerte zu schützen.

Echtzeitinformationen

Echtzeitinformationen aus internen und externen Quellen bilden den Grundstein für ein leistungsstarkes Sicherheitsteam. Echtzeitinformationen sind Angaben zu einem bestimmten Risikoereignis, die so schnell wie möglich nach dessen Eintreten bereitgestellt werden, in vielen Fällen innerhalb von Sekunden.

Die Informationen stammen dabei aus verschiedenen Quellen:

- Interne Tools:
  - Zugangskontrollsysteme
  - Videoüberwachung
  - Netzwerksicherheitstools
- Schnelle Kommunikationswege zum Unternehmen:
  - Dedizierter Sicherheits-E-Mail-Alias
  - Sicherheits-Apps
  - Chat-Tools
  - Rund um die Uhr besetzte Rufnummern
- Externe Nachrichten- und Informationsquellen:
  - Tools zur Überwachung sozialer Medien
  - Nachrichten-Feeds
- Echtzeitinformationsplattformen wie Dataminr Pulse

Zusammen geben diese Echtzeitinformationsquellen den Sicherheitsteams – vom Analysten bis zum Chief Security Officer – ein umfassendes Bild der aktuellen Risiken, denen ihr Unternehmen ausgesetzt ist. Im Krisenfall werden die Sicherheitsteams danach beurteilt, wie gut die ihnen zur Verfügung stehenden Echtzeitinformationen sind und wie schnell sie diese verarbeiten und auf sie reagieren können, um die Geschäftskontinuität zu gewährleisten.

Die Echtzeitinformationen werden innerhalb des SOC in andere Technologieplattformen eingespeist, wie z. B.:

- eine Plattform zur Risikoüberwachung bestimmter Standorte
- eine Lösung für GIS-Mapping und Datenvisualisierung
- ein Ticketing- und Workflow-Managementsystem für die Reaktion auf Ereignisse
- Tools für die Massenkommunikation
- Plattformen für Reiseinformationen
- Cybersecurity-Warnsoftware

Wichtige Überlegungen beim Aufbau eines Security Operations Center – Planung und Aufbau eines SOC

HIER LESEN

Künstliche Intelligenz im SOC

Wie viel Zeit verbringen Ihre Sicherheitsanalysten mit dem Sammeln von Informationen? Dataminr Pulse nutzt künstliche Intelligenz, damit Ihre Analysten weniger Zeit mit der Suche nach Informationen verbringen müssen und mehr Zeit haben, auf diese zu reagieren.

Die KI-Plattform von Dataminr verarbeitet in großem Umfang Nachrichten aus mehr als 150.000 öffentlichen Informationsquellen – Social-Media-Inhalte, mit dem Internet verbundene Sensoren, Nachrichtenseiten, Audio-Feeds sowie das Deep- und Dark-Web – und liefert so die frühesten Hinweise auf sich abzeichnende Risiken für die Geschäftskontinuität.

Die Plattform ist in hohem Maße konfigurierbar: Sie können die physischen Standorte Ihres Unternehmens und die spezifischen Themen, die für Sie von Interesse sind, festlegen, um die für Ihr Unternehmen relevantesten Warnmeldungen zu erhalten.

Hunderte der weltweit führenden Sicherheitszentralen, Regierungsbehörden, humanitäre Organisationen und Journalisten von mehr als 650 führenden Nachrichtenagenturen vertrauen auf Dataminr.
.

Menschen

In Security Operations Centers arbeiten Analysten und Manager zusammen, um Empfehlungen zum Schutz von Mitarbeitern und Führungskräften, Partnern und Kunden sowie Unternehmenswerten zu geben.

SOC können dabei verschieden groß sein. Hier ein paar typische Konfigurationen:

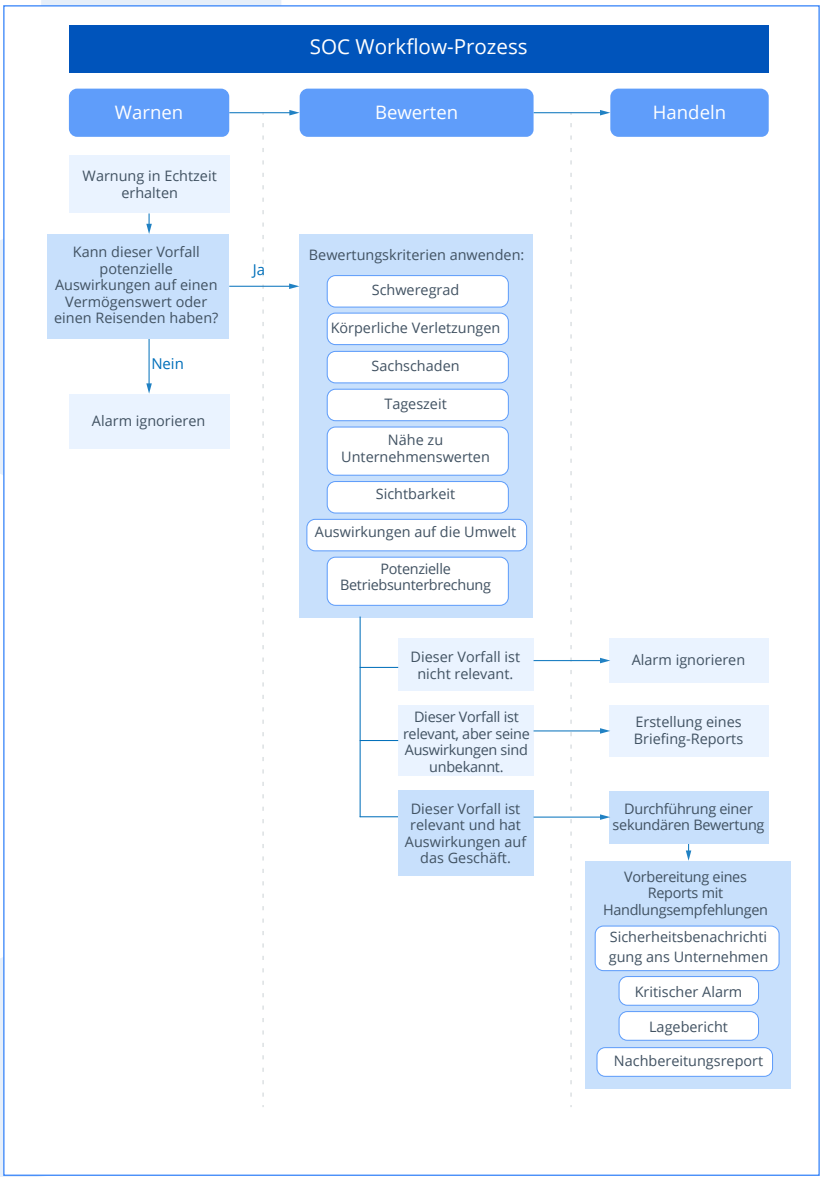
- Kleinere Unternehmen mit einer zentralisierten Sicherheitsabteilung von drei Mitarbeitern, die nur während der normalen Arbeitszeit aktiv sind und sich auf einen Managed Security Service Provider verlassen, um außerhalb der Arbeitszeit oder während einer ernsten Krise abgesichert zu sein.
- Mittelgroße Unternehmen mit einem zentralisierten Team von bis zu fünf Mitarbeitern, die oft ohne ein physisches SOC arbeiten. Diese Teams kümmern sich rund um die Uhr um die Sicherheit des Unternehmens und werden von regionalen Sicherheitsmanagern unterstützt.
- Größere Unternehmen mit einem eigenen globalen Security Operations Center mit bis zu 30 Mitarbeitern, das rund um die Uhr besetzt ist und die Bemühungen regionaler SOC und Sicherheitsmanager koordiniert.

SOC-Manager sind dafür verantwortlich, die Arbeitsabläufe und Prozesse des SOC zu überwachen und zu verbessern und den Erfolg zu messen.
Sie sollten auch unter Druck ruhig und besonnen vorgehen und tragen die zusätzliche Verantwortung, bei einem Risikovorfall auf der Grundlage von Echtzeitinformationen geeignete Maßnahmen zu ergreifen

Workflow-Prozesse

Prinzipiell verwandeln alle zentralisierten Sicherheitsteams Echtzeitinformationen in verwertbare Erkenntnisse. Vordefinierte Workflows formalisieren den Prozess der Umwandlung von Informationen in Maßnahmen und enthalten Tools, mit denen die Leistung des Workflows gemessen werden kan.

SOC-Workflows lassen sich in drei Hauptschritte gliedern: Warnen, Bewerten und Handeln. **Hier ein Beispiel für einen Workflow, den wir bei mehreren SOC im Einsatz gesehen haben:**



Die Arbeitsabläufe werden mit einem Incident Management System abgebildet, das Tools zur Messung der durchschnittlichen Reaktionszeit und Performance eines Teams enthält. Unabhängig davon verwenden einige SOC andere Messinstrumente, um die Effizienz und den Erfolg des Teams zu messen, z. B. Umfragen zur Mitarbeiterzufriedenheit.

5 Stolpersteine, die Sie beim Aufbau Ihres Security Operations Center vermeiden sollten

VIDEO ANSEHEN

Reporting-Auswirkungen

Sicherheitsteams erwirtschaften keine Einnahmen für das Unternehmen. Daher ist es wichtig, Ressourcen für die Messung der positiven Auswirkungen eines SOC bereitzustellen, um weitere Investitionen in das Programm zu rechtfertigen.

SOC-Manager, die mehr in ihr Programm investieren möchten, sollten von Anfang an Maßnahmen zur Messung der Effizienz und Reporting-Tools entwickeln und ihr Führungsteam regelmäßig über die Auswirkungen und die Leistung des SOC auf dem Laufenden halten.

Den Wert eines eingedämmten Risikos zu messen und zu bewerten, ist eine besondere Herausforderung für Sicherheitsteams. Das potenzielle Ausmaß der Auswirkungen lässt sich nie vollständig erfassen, sodass es schwierig ist, die Kosten eines abgewendeten Ereignisses oder eines anderweitig minimierten Risikos abzuschätzen.

Zu den wichtigsten Leistungsindikatoren, die Sie messen sollten, gehören:

- Gesamtzahl der von der SOC im Berichtszeitraum verarbeiteten Echtzeitwarnungen
- Gesamtzahl der Maßnahmen zur Risikominderung, die das SOC im Berichtszeitraum ergriffen hat
- Ausgewählte entscheidende Maßnahmen zur Risikominderung im Berichtszeitraum
- Bewertung der Mitarbeiterzufriedenheit

Für die Zukunft

Bei der Zukunftsplanung gibt es zwei Dinge, die SOC-Manager tun können, um eine kontinuierliche Investition in ihr Team sicherzustellen.

Erstens sollten Sie die Arbeit des Security Operations Center auf ein höheres Niveau heben, weg von der reaktiven Reaktion auf Risiken und hin zum proaktiven Risikomanagement und zur Stärkung der geschäftlichen Resilienz. Nutzen Sie verfügbare Echtzeitinformationen und historische Risikodaten, um der Unternehmensleitung dabei zu helfen, fundiertere Entscheidungen zu treffen.

Geben Sie den Zugang zu Echtzeitinformationen an andere Teams im Unternehmen weiter, die für die Risikominderung zuständig sind, wie z. B. das Cybersicherheitsteam und das Risikomanagementteam, sodass sie diese Informationen nutzen können, um künftige Risiken besser vorherzusehen.

Zweitens sollten Sie Risikomanagement, Business-Resilienz und -Kontinuität, Cybersicherheit und physische Sicherheit ganzheitlich betrachten. Jedes dieser Teams konzentriert sich auf ein ähnliches Ziel: die Vorhersage, Planung und Minderung von Risiken. Wenn diese Teams jedoch in operativen Silos arbeiten, können ungewollt blinde Flecken für Risiken entstehen.

Erfahren Sie mehr

Demo anfordern

Vereinbaren Sie einen Demotermin, um zu sehen, wie Sie früher Einblicke in wichtige Ereignisse und sich abzeichnende Risiken gewinnen können.

DEMOTERMIN VEREINBAREN

Kontakt

Allgemein | info@dataminr.com
Support | support@dataminr.com

Weitere Informationen zum Thema SOC finden Sie auf unserem Security Operations Center Hub.