FIREEYE™

LÖSUNGSÜBERSICHT

Einsatzbereiche für Bedrohungsdaten

SOC-Analysten (Security Operations Center)

HERAUSFORDERUNGEN FÜR SOC-ANALYSTEN

Die Zahl der von Sicherheitstools generierten Warnmeldungen, Alarme und Ereignisse steigt exponentiell an und SOC-Analysten haben Schwierigkeiten zu erkennen, wann es sich um ernstzunehmende Kampagnen und komplexe Angriffe handelt und ob sie sofort eingreifen müssen. Die Analysten müssen die relevanten Informationen aus der Masse herausfiltern und entscheiden, wie die knappen Incident-Response-Ressourcen des Unternehmens am sinnvollsten eingesetzt werden. Hier zwei Beispiele der größten Herausforderungen:

- Es ist nahezu unmöglich, Zehntausende oder sogar Millionen von Warnmeldungen und Alarmen pro Tag zu sichten, um die gefährlichsten Bedrohungen zu identifizieren.
- Die verfügbaren Informationen reichen meist nicht aus, um in der Masse ungültiger, unzuverlässiger und unerheblicher Warnmeldungen und Alarme die wirklich relevanten zu finden, die eine ernste Gefahr für das Unternehmen darstellen.

Tools zum Zusammenfassen von Logdateien und Korrelieren der zugehörigen Alarme verrin-gern zwar die Anzahl der Warnmeldungen, die evaluiert werden müssen, aber Level-1-SOC-Analysten sind immer noch stark überlastet.

So profitieren Level-1-SOC-Analysten von Cyberbedrohungsdaten

In modernen Security Operations Centern (SOC) werden Warnmeldungen mithilfe von Cyberbedrohungsdaten priorisiert und validiert. Auf diese Weise können die Analysten schneller ermitteln, welche Bedrohungen für das Unternehmen tatsächlich relevant sind. Durch die Eingrenzung des Problems und die zusätzlichen Kontextinformationen können Level-1-Analysten schneller und besser entscheiden, welche Warnmeldungen und Alarme zur tief gehenden Analyse an das Incident-Response-Team (IR-Team) weitergeleitet werden sollen.

Tabelle 1: Einsatzbereiche – Level-1-SOC-Analysten

Einsatzbereich	Ziel	Erforderliche Bedrohungsdaten
Maschinelle Priorisierung	Automatisieren der Ersteinschätzung zur Unterstützung der SIEM- und Analysetools bei der Priorisierung von Warnmeldungen und Alarmen (die dann an die SOC-Analysten weitergeleitet werden)	Maschinell lesbare Bedrohungsdaten: Gefahrenindikatoren mit Schweregrad und Tags zu Angriffen, die auf bestimmte Branchen, Regionen, Anwendungen usw. ausgerichtet sind
Ersteinschätzung der Warnmeldung/ des Ereignisses	Schnell entscheiden, welche Warnmeldungen und Ereignisse zuerst untersucht werden sollen	Gefahrenindikatoren in den Bedrohungsdaten, die Kontextinformationen enthalten und einen Überblick über die Bedrohungslage bieten
Analyse und Validierung der Warnmeldung/ des Ereignisses	Validieren der Ereignisse und Auswählen derjenigen, die zur umfassenden Schadensbehebung an das IR-Team weitergeleitet werden	Bedrohungsdaten, die individuelle Indikatoren den Kampagnen, Hackern und Techniken zuordnen, sowie weitereKontextinformationen

Maschinelle Priorisierung: Technologie für umfangreiche Aufgaben
Welche der Tausenden (oder sogar Millionen) Alarme, Warnmeldungen und Ereignisse sind wirklich wichtig? SOC-Teams sehen zahlreiche Fehlalarme für Ereignisse, die den Geschäftsbetrieb gar nicht beeinträchtigen oder die von den vorhandenen Sicherheitslösungen abgewehrt werden. SIEM-, Logdateiverwaltungs- und Sicherheitsanalysetools sind in der Lage, Alarme und Ereignisse mit Bedrohungsdaten abzugleichen und die erste Priorisierung zu übernehmen. Das bringt gleich zwei Vorteile: Zum einen wird damit die Priorisierung beschleunigt und zum anderen müssen Level-1-SOC-Analysten nicht mehr ihre Zeit darauf verwenden, jeden Tag Zehntausende irrelevanter Warnmeldungen durchzusehen.

Stattdessen können sie beispielsweise SIEM-Regeln erstellen, um Gefahrenindikatoren, die im Netzwerk gefunden wurden (z. B. in Domains und IP-Adressen, Ports und Protokollen, Datei-Hashes oder Registry-Einstellungen), mit Bedrohungsdaten abzugleichen. Auf diese Weise können die Gefahrenindikatoren den Hackern und Kampagnen zugeordnet werden, die die Branche, Region, Softwareanwendungen oder Infrastrukturkomponenten des Unternehmens gefährden. Wird eine Übereinstimmung gefunden, erhöht das SIEM-Tool automatisch die Priorität der Warnmeldung oder des Ereignisses, damit das SOC-Team über die relevanten Bedrohungen informiert wird.

Ersteinschätzung von Ereignissen und Warnmeldungen: schnellere menschliche Analysen
Durch die maschinelle Priorisierung wird zwar schon ein Großteil der Arbeit vorweggenommen, aber die SOC-Analysten müssen immer noch ermitteln, welche Warnmeldungen und Alarme tatsächlich relevant sind. Diese Analysen sind recht zeitaufwendig. Mit Cyberbedrohungsdaten kann dieser Prozess beschleunigt werden, da sie SOC-Teams Kontextinformationen und einen Überblick über die Bedrohungslage bieten.

Die Bedrohungsdaten enthalten Tags und zusammenfassende Beschreibungen, die die individuellen Gefahrenindikatoren Hackern und Zielen zuordnen, oder längere Erläuterungen, in denen zu den jeweiligen Indikatoren Kontextinformationen zu Kampagnen und mehrstufigen Angriffen gegeben werden.

Wenn beispielsweise ein Malware-Alarm ausgelöst wird, kann der SOC-Analyst aus den Bedrohungsdaten schnell ablesen, ob diese Malware schon zuvor bei Cyberangriffen oder Cyberspionagekampagnen eingesetzt wurde. Weist eine Warnmeldung auf verdächtige Kommunikation mit einer IP-Adresse im Internet hin, ist aus den verknüpften Bedrohungsdaten rasch erkennbar, ob diese IP-Adresse Hackern gehört, die für Angriffe auf die Branche des Unternehmens oder auf Länder bekannt sind, in denen das Unternehmen tätig ist.

Analyse und Validierung: Zusammentragen von Nachweisen und Priorisieren von Sicherheitsverletzungen
Level-1-SOC-Analysten können Bedrohungsdaten auch nutzen, um Bedrohungen detaillierter zu analysieren und Ereignisse zu validieren. Dadurch lassen sich Fragen beantworten wie: Gehört dieses Ereignis zu einer Bedrohung, die für unser Unternehmen gefährlich werden könnte? Treten diese Ereignisse isoliert oder im Rahmen eines komplexen gezielten Angriffs auf?

Zu den Kontextinformationen gehören beispielsweise Listen verknüpfter Malware-Varianten, Domains und IP-Adressen sowie Angaben zum Verhalten der Malware-Samples, Phishing-Angriffe und anderer Angriffstechniken. Die Daten in Bedrohungsdatenbanken liefern zusätzliche Details und Erläuterungen, zum Beispiel die Zuordnung der Malware oder Phishing-Nachrichten zu einer bestimmten Hackergruppe oder einem speziellen Angreifer, die Analyse der Schritte eines mehrstufigen Angriffs und Empfehlungen für geeignete Abwehrmaßnahmen.

Mithilfe dieser Ressourcen können SOC-Analysten schnell Nachweise zusammenstellen, um zu ermitteln, ob Warnmeldungen und Ereignisse als relevante Bedrohung für das Unternehmen eingestuft und zur tief gehenden Analyse sofort an das Incident-Response-Team weitergeleitet werden sollten.

Das Ergebnis
SOC-Teams erhalten heutzutage riesige Mengen an Rohdaten. Mit den zuverlässigen, praxisrelevanten Bedrohungsdaten und Kontextinformationen von FireEye können Level-1-SOC-Analysten …

- die Masse der Warnmeldungen und Sicherheitsereignisse eingrenzen,
- das ineffiziente Sichten der zahlreichen ungültigen oder unwichtigen Warnmeldungen vermeiden,
- schnell die Warnmeldungen für die tatsächlich relevanten Bedrohungen identifizieren und
- rasch die erforderlichen Nachweise zusammenstellen und dadurch fundierte Entscheidungen dazu treffen, welche Vorfälle eskaliert werden müssen.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™