LÖSUNGSHINWEIS

SOC INSIGHTS

Wenden Sie KI-gesteuerte Analysen an, um riesige Mengen an Ereignis-, Netzwerk-, Ökosystem- und DNS-Informationsdaten in verwertbare Insights umzuwandeln und die SecOps-Effizienz zu steigern.

HINDERNISSE FÜR DIE EFFIZIENZ VON SECOPS

Wie bei anderen Funktionen von Unternehmen oder Regierungsorganisationen hat das moderne SOC heute Schwierigkeiten, mit den verfügbaren Ressourcen mehr zu erreichen. Laut der SANS 2023 SOC-Umfrage[1] fallen 80 % der zehn größten SOC-Hürden bei der vollständigen Nutzung der SOC-Funktionen in drei Bereiche:

- Warnungen verstehen und damit umgehen
- Eingeschränkte Integration oder Automatisierung zwischen Tools
- Wichtige Aufgaben mit dem verfügbaren Personal und den verfügbaren Fähigkeiten ausführen

Aber die wirklich tragischste Statistik könnte sein, dass all diese Hindernisse das SOC seit über einem Jahrzehnt herausfordern. Die schrittweisen Verbesserungen durch die einfache automatische Priorisierung von Vorfällen auf der Grundlage von Malware-Rankings und anderen grundlegenden Filtern konnten mit der Zunahme von Warnungen und anderen Ereignissen, die möglicherweise die Aufmerksamkeit der SOC-Analysten erfordern, nicht Schritt halten. Es ist also nur noch schlimmer geworden.

KI-GESTEUERTE SOC INSIGHTS

Moderne hartnäckige Bedrohungen sind auf eine flexible Angreifer-Infrastruktur und dynamische C2-Systeme angewiesen, um die zahlreichen Pentest-, Exploit-, Verschlüsselungs- und anderen Tools zu hosten und bereitzustellen, die an einem einzelnen Angriff beteiligt sind. Das macht sie extrem abhängig von DNS und unterstreicht eine wichtige Schwäche, die Verteidiger ausnutzen können, um diese Bedrohungen zu erkennen und abzuwehren.

DNS sieht legitime und bösartige Aktivitäten unabhängig von Protokoll, Plattform, Betriebssystem, Anwendung oder sogar Standort. Mit dieser einzigartigen Transparenz stellte ein Pilotprogramm unter dem Director of the Cybersecurity Directorate bei der NSA fest, dass die Absicherung von DNS Malware-Angriffe um 92 % reduzieren kann[2]!

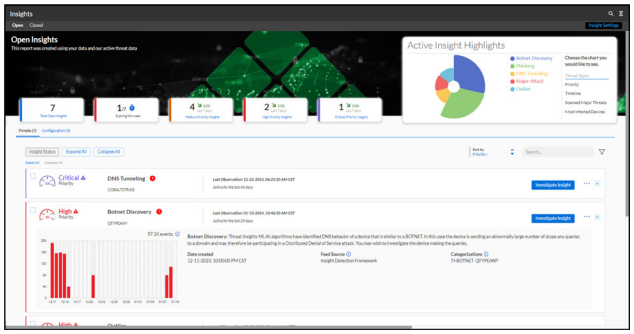

Abbildung 1: Die SOC Insights-Zusammenfassungsseite bietet Analysten mit einem Klick Zugriff auf das Wichtigste.

ZAHLEN UND FAKTEN

- 60 % der SOC-Analysten geben an, dass ihre **Arbeitsbelastung zunimmt**, und 65 % werden **wahrscheinlich im nächsten Jahr** den Job wechseln[4].
- 55 % der Befragten gaben an, dass **kritische Warnungen** häufig wöchentlich und sogar täglich verpasst werden[5].
- 64 % der Analysten geben an, dass **manuelle Arbeit mehr als die Hälfte ihrer Zeit kostet**[6].
- Fehlkonfigurationen gehören zu den **drei häufigsten Faktoren bei fehlerbedingten Verstößen**[3].
- 8 der 10 größten **Hindernisse, die eine vollständige SOC-Nutzung verhindern**, sind Warnungen, Tool-Integration und Fachkräftemangel[1].
- 77 % der CEOs machen sich Sorgen über die **Verfügbarkeit wichtiger Fähigkeiten**[7].
- **92 % der Malware- und C2-Aktivitäten können auf der DNS-Ebene** mit der richtigen DNS-Intelligenz und -Sichtbarkeit gesteuert werden[2].

SOC Insights arbeitet mit BloxOne, der DNS Detection and Response (DNSDR)-Lösung von Infoblox Threat Defense, um einzigartige KI-gesteuerte Analysen zur Erkennung unbekannter Bedrohungen zu bieten, die von anderen Tools übersehen werden, um die SOC-Effizienz zu steigern und den Gesamt-ROI der aktuellen Sicherheitsinvestitionen zu verbessern.

LÖSUNG MEHRERER PROBLEME MIT UNTERSCHIEDLICHEN INSIGHTS

Untersuchungen nach einem Vorfall oder einer Sicherheitsverletzung zeigen oft, dass Frühindikatoren für böswillige Aktivitäten aufgrund von Fehlkonfigurationen, Problemen bei der Integration von Sicherheitstools oder einer einfachen Überlastung mit Warnmeldungen übersehen wurden. SOC Insights wendet KI-gesteuerte Analysen auf eine große Datenmenge an, um diese Risiken zu bewältigen.

Einblicke in die Sicherheit

Das Sicherheits-Add-on für SOC Insights ist für BloxOne Threat Defense 'Business Cloud' oder 'Advanced' erhältlich. Es nutzt KI, um riesige Mengen an Ereignis-, Netzwerk-, Ökosystem- und DNS-Transparenz und -Intelligenz in eine überschaubare Menge an umsetzbaren Sicherheitsinformationen zu destillieren.

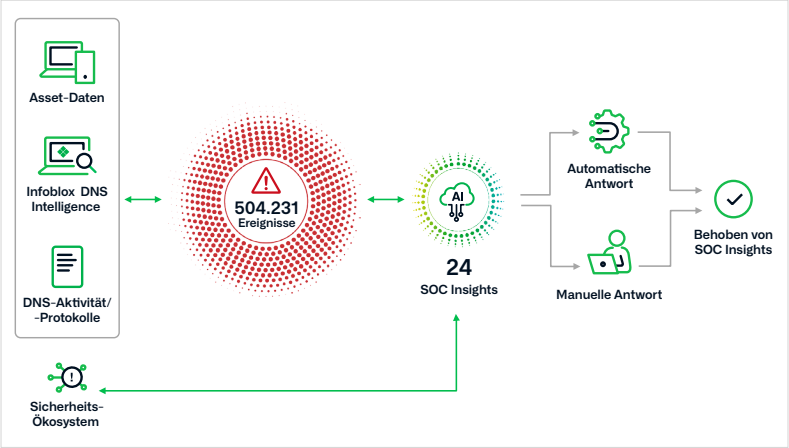

Abbildung 2: Lassen Sie SOC Insights die Überlastung durch Warnungen beseitigen und Berge von Ereignissen in einen besser verwaltbaren Satz aussagekräftiger, umsetzbarer Erkenntnisse zusammenfassen.

- Anhaltende Bedrohung
- Aktive Ausbreitung der Bedrohung
- Großangriff
- Botnet-Erkennung
- Ausreißer-Kommunikation
- Phishing
- Malware
- Offener DNS-Resolver
- DNS-Tunneling
- Aktivität bei Datenverlust
- Gezielter Angriff
- Übermäßige DNS-Fehler
- Überwachte Lookalike-Domain

Einblicke in die Konfiguration

Die Konfigurationsfunktion von SOC Insights ist in BloxOne Threat Defense 'Business Cloud' und 'Advanced' enthalten, damit die Benutzer sicherstellen können, dass sie die aktuellen Best Practices in vollem Umfang nutzen und häufige Fehler vermeiden. Folgen Sie Videos und anderen Anleitungen, um Fehler und Schwächen zu beheben, oder deaktivieren Sie unnötige Warnungen für erlaubte Ausnahmen.

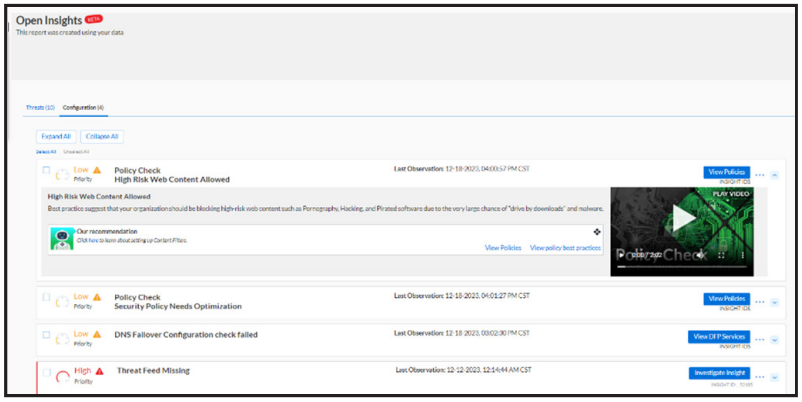

Abbildung 3: Erkennen Sie proaktiv schwache oder gefährliche Konfigurationsfehler, um optimale Abwehr-, Untersuchungs- und Reaktionsmöglichkeiten zu gewährleisten.

- DNS-Bedrohungs-Feed fehlt
- VirusTotal Free Key fehlt
- Sicherheitsrichtlinien müssen optimiert werden
- Fehler bei der DNS-Failover-Prüfung
- Nicht übereinstimmende Feed-Aktion
- DFP-Ausblenden von Asset-Details
- Sicherheitsrichtlinie im Protokollierungsmodus
- Webinhalts-Filer AUS
- Hochriskante Webinhalte erlaubt

EINE POSITIVE FINANZIELLE, OPERATIVE UND GESCHÄFTLICHE AUSWIRKUNG

Während die meisten Sicherheitstools kaum mehr als „Benutzerfreundlichkeit“ und „weniger Sicherheitsverletzungen“ versprechen, kann SOC Insights noch viel mehr – angefangen von der Reduzierung von Analystenstress und Fluktuation bis hin zur Reduzierung vieler Sicherheitsbedenken aufgrund von Expansion, M&A und anderen Geschäftsinitiativen. Zum Beispiel:

- Die Natur des DNS macht es einfach, einen neuen Standort oder Geschäftspartner innerhalb von Minuten statt Monaten in eine gemeinsame DNS-Infrastruktur einzubinden.
- Configuration Insights ist äußerst proaktiv und trägt dazu bei, Verstöße oder Datenverluste aufgrund von „Fehlkonfigurationen“ zu mindern, einem der drei häufigsten Faktoren, die bei fehlerbedingten Verstößen gemeldet werden[3].
- Die Autokorrelation von „Malware“, „Phishing“, „Botnet“ und anderen „großen“ oder „sich verbreitenden“ Aktivitäten ermöglicht es den Einsatzkräften, viele Bedrohungen gleichzeitig zu bekämpfen und so ihre Effizienz zu steigern.
- Gehen Sie zu einem proaktiveren Sicherheitsstatus mit der Möglichkeit, Einblickskategorien wie „Ausreißer“, „DNS-Tunneling“ und „Open Resolver“ sowie die einzigartigen Lookalike- und Anwendungssichtbarkeitsfunktionen von BloxOne Threat Defense zu überwachen.
- Die intelligente Integration des Sicherheitsökosystems verbessert den ROI des gesamten Sicherheits-Stacks, indem es umsetzbare „Insights“ statt nur Rohprotokolle und Ereignisse bietet.
- SOC Insights sammelt automatisch relevante Daten und ermöglicht es Analysten, diese Daten zu sehen und zu nutzen, um schneller und zuverlässiger zu Ergebnissen zu gelangen. Dies trägt zu weniger Stress und einer höheren Bindung qualifizierter und erfahrener Sicherheitsexperten bei.

VERBESSERN SIE SIEM, SOAR UND ANDERE TEILE DES ÖKOSYSTEMS MIT INSIGHTS

SecOps kennt den Wert und die Grenzen des Austauschs von Rohdaten rund um das Sicherheitsökosystem. Dies hat dazu geführt, dass SIEM- und SOAR-Kenntnisse für die meisten Unternehmen eine der größten Herausforderungen darstellen. SOC Insights entlastet diese anderen Tools und kann die daraus resultierenden Insights über den gesamten Sicherheits-Stack hinweg teilen, um andere Tools effektiver zu machen und die Gesamteffizienz von SecOps weiter zu steigern.

1 „SANS 2023 SOC Survey“, Juni 2023, von Chris Crowley, Barbara Filkins, John Pescatore

2 „NSA launches pilot program to secure defense contractors“, 18. Juni 2020, von Lauren C. Williams, NEXTGOV/FCW

3 „Verizon 2023 DBIR Report“

4 Stimme des SOC-Analysten

5 Der Orca Security 2022 Cloud Security Alert Fatigue Report

6 Stimme des SOC-Analysten

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240104v1