LÖSUNGSHINWEIS

STEIGERUNG DER SOC-PRODUKTIVITÄT MIT ECHTZEIT-SICHERHEITSWARNUNGEN AUF SLACK

Senden Sie automatisch Slack-Nachrichten, die korrelierte und priorisierte DNS-basierte Sicherheitsdaten enthalten.

Die heutige Sicherheitslandschaft ist komplex und entwickelt sich ständig weiter. Cyberkriminelle zielen zunehmend auf die DNS-Infrastruktur ab, um ausgeklügelte Angriffe wie Phishing-Kampagnen, Malware-Verbreitung und Datenexfiltration zu starten. Sicherheitsanalysten stehen unter enormem Druck, diese Bedrohungen zeitnah zu erkennen und darauf zu reagieren. Sie haben nicht die Kapazitäten, um die zahlreichen Anwendungen, für die sie zuständig sind, proaktiv zu überwachen und zu durchsuchen. Eine solche „Drehstuhl"-Routine ist höchst ineffizient und verstärkt die Notwendigkeit, über ein einziges, vertrautes Tool zu kommunizieren und zusammenzuarbeiten, wodurch sich sowohl die mittlere Zeit bis zur Erkennung (Mean Time to Detect, MTTD) als auch die mittlere Zeit bis zur Reaktion (Mean Time to Respond, MTTR) verkürzt. Für Unternehmen, die die Möglichkeiten von Slack nutzen, hat Infoblox eine zertifizierte Integration entwickelt, die sofortige, nach Prioritäten geordnete Sicherheitsbenachrichtigungen direkt auf Slack bereitstellt und so schnelle Entscheidungen und Maßnahmen des SOC ermöglicht.

HERAUSFORDERUNGEN

Sicherheitsteams stehen in der heutigen komplexen Bedrohungslandschaft vor zahlreichen Herausforderungen:

- **Warnungsüberlastung:** Sicherheitsanalysten werden ständig mit Warnungen von verschiedenen Sicherheitstools überschwemmt, was die Identifizierung und Priorisierung der kritischsten Bedrohungen erschwert.
- **Eingeschränkte Sichtbarkeit:** Traditionelle Sicherheitslösungen sind oft nicht in der Lage, den Kontext und das Ausmaß von Bedrohungen einfach zu analysieren und die nächsten Schritte zu bestimmen.
- **Ineffiziente Arbeitsabläufe:** Die Untersuchung von Bedrohungen erfordert häufig das Wechseln zwischen verschiedenen Sicherheitstools, was wertvolle Zeit kostet und umständlich ist.

SCHNELLER NUTZEN DURCH EINFACHE INTEGRATION: INFOBLOX + SLACK

Die DNSDR-Lösung (DNS Detection and Response) von Infoblox, BloxOne Threat Defense, erweitert um SOC Insights, durchsucht automatisch riesige Mengen an DNS-Bedrohungsinformationen und Asset-Daten, um umsetzbare Reaktionen auf Bedrohungen zu korrelieren und zu priorisieren. Die Lösung verwandelt riesige Mengen von Ereignis-, Netzwerk-, Ökosystem- und DNS-Intelligenzdaten in verwertbare Erkenntnisse, um die SecOps-Effizienz zu steigern. Die umfangreichen Sicherheitsdaten, die BloxOne Threat Defense mit SOC Insights generiert, beseitigen blinde Flecken und ermöglichen ein umfassendes Verständnis DNS-basierter Angriffe.

DIE WICHTIGSTEN VORTEILE

- **Zentralisierte Kommunikation und Zusammenarbeit:** Lassen Sie sich automatisch über priorisierte Sicherheitswarnungen direkt in Slack benachrichtigen und reduzieren Sie die Notwendigkeit der manuellen Überwachung mehrerer Tools.
- **Beschleunigte Reaktion:** Beschleunigen Sie die Reaktion auf Vorfälle durch direkten Zugriff auf den Bedrohungskontext und alle Details, um schnell die nächsten Schritte festzulegen.
- **Reduzierte Alarmmüdigkeit:** Lassen Sie sich nur über die kritischen Bedrohungen benachrichtigen und reduzieren Sie so die Belastung der Sicherheitsanalysten.
- **Maximierter ROI:** Erhöhen Sie den Wert Ihrer Slack-Investition, indem Sie Sicherheits-Workflows optimieren und den Wechsel zwischen Apps reduzieren.

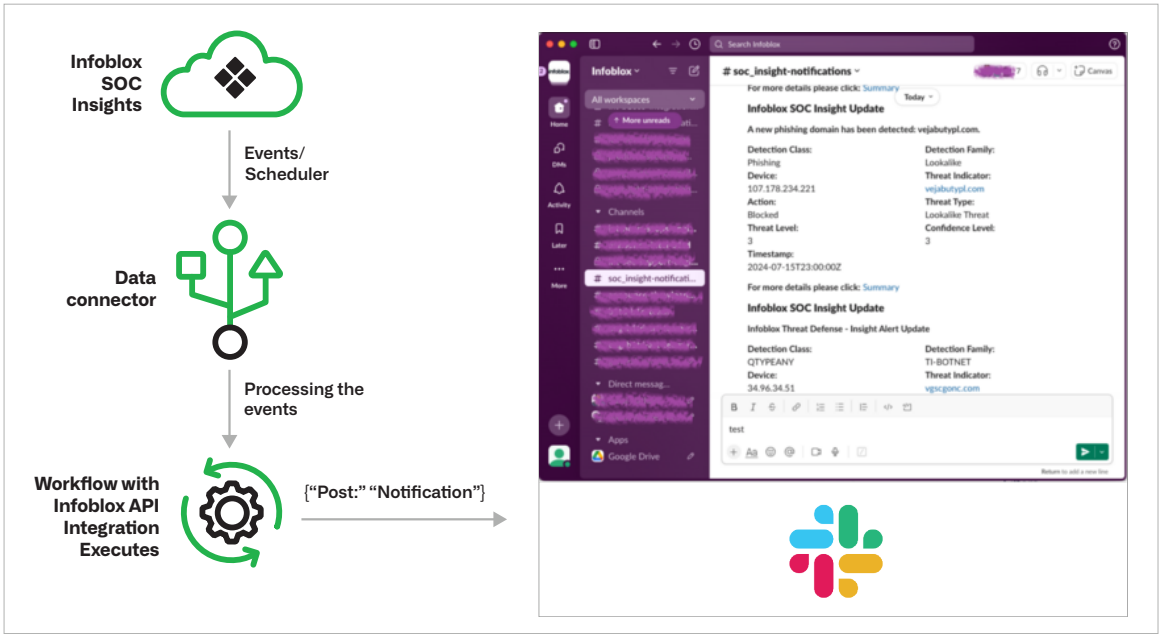
Um die Gesamteffizienz des SOC weiter zu steigern, bietet Infoblox eine Low-Code-Integration in Slack, mit der die Vorteile jeder Lösung gesteigert und die Gesamtbetriebskosten gesenkt werden können. Diese leistungsstarke Kombination rationalisiert die Erkennung von und Reaktion auf Bedrohungen und liefert Sicherheitsteams sofortige Benachrichtigungen über wichtige Erkenntnisse, die zum Schutz Ihres Unternehmens erforderlich sind.

Infoblox und Slack unterstützt und Sicherheits-Teams bei Folgendem:

- **Vereinheitlichung von Bedrohungswarnungen:** Infoblox löst Slack-Nachrichten in Echtzeit aus, die Sicherheitsanalysten über priorisierte Bedrohungen informieren, wodurch manuelle Überwachungsaufgaben mit mehreren Werkzeugen sofort überflüssig werden. Die Warnungen werden an einen benutzerdefinierten Slack-Kanal gesendet, der den Analysten eine zentrale Verwaltung der Warnungen ermöglicht, einschließlich historischer Dokumentation und Nachverfolgung.
- **Vereinfachung von Untersuchungen:** Die durch Infoblox ausgelösten Slack-Nachrichten bieten einen Einblick in den entscheidenden Inhalt und Kontext, der für die Triage und die Zusammenarbeit bei den nächsten Schritten erforderlich ist. Mit einem Klick auf den in der Nachricht enthaltenen Link werden Sie direkt zum Infoblox-Portal weitergeleitet, wo Sie weitere Untersuchungen durchführen können.
- **Ergreifung entschlossener Maßnahmen:** Ausgestattet mit den passenden Inhalten und dem Kontext, den Infoblox bereitstellt, können Sicherheitsanalysten effizient und effektiv auf die wichtigsten Bedrohungen reagieren und den Status im Nachrichten-Thread in Slack aktualisieren, um das Team auf dem neuesten Stand zu halten.

Durch die Implementierung von Infoblox für Slack können Sicherheitsteams ihre Sicherheitslage verbessern, indem sie einen zentralen Überblick über kritische Warnmeldungen erhalten, Untersuchungen rationalisieren und schneller auf Bedrohungen reagieren können.

WIE ES FUNKTIONIERT



ÜBERLEGENE SOC-LEISTUNG MIT DER INTEGRATION VON INFOBLOX UND SLACK

Die Integration von Infoblox mit Slack bietet eine kollaborative Sicherheitslösung, die Ihre bestehende Infrastruktur verbessert. Diese Synergie gewährleistet:

- **SOC-Effizienz:** Sorgen Sie für optimale Leistung, indem Sie priorisierte Bedrohungsmeldungen sofort an einen zentralen Slack-Kanal senden. Dies verbessert die Kommunikation und bietet gleichzeitig eine chronologische Nachverfolgung.
- **SOC-Effektivität:** Ermöglichen Sie es Sicherheitsanalysten, Bedrohungsinhalte und -kontext direkt in der Slack-Nachricht einzusehen, um schnell und angemessen handeln zu können.
- **Betriebliche Produktivität/ROI:** Die Optimierung von Arbeitsabläufen und die Reduzierung von App-Wechseln kann die Effizienz Ihres SecOps-Teams verbessern und zu Zeit- und Kosteneinsparungen führen.
- **Einfache Integration:** Einfache, getestete und zertifizierte Low-Code-Integration verkürzt die Zeit bis zur Wertschöpfung.

ZUSAMMENFASSUNG

Die Automatisierung von Sicherheitsaufgaben, die Verkürzung von Erkennungs- und Reaktionszeiten und die Aufrechterhaltung einer effektiven Kommunikation und Zusammenarbeit bei der Reaktion auf Bedrohungen sind große Herausforderungen für SecOps-Teams. Die Integration von Infoblox mit Slack steigert den Wert Ihres gesamten Sicherheits-Stacks, indem es eine einheitliche Plattform für eine angereicherte Threat-Intelligence-Kommunikation bietet. Diese Kombination steigert die Produktivität von SecOps, verbessert die Effizienz und sorgt für ein robusteres und reaktionsschnelleres Sicherheitsprogramm. Indem Sie Infoblox für Slack nutzen, verbessern Sie die Sicherheitskapazitäten Ihres Unternehmens und maximieren die Rendite Ihrer Sicherheitsinvestitionen.

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.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com

Version: 20240724v1