

LÖSUNGSHINWEIS

STEIGERN SIE DIE PRODUKTIVITÄT DES SOC MIT ECHTZEIT-SICHERHEITSWARNUNGEN IN MICROSOFT TEAMS

Automatisch Microsoft Teams-Nachrichten senden, 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 immensem Druck, diese Bedrohungen rechtzeitig zu identifizieren und darauf zu reagieren, und haben nicht die Kapazität, die verschiedenen Anwendungen, für die sie verantwortlich sind, proaktiv zu überwachen und zu durchsuchen. Diese „Drehstuhl“-Routine ist höchst ineffizient und verstärkt die Notwendigkeit, über ein einziges, vertrautes Tool zu kommunizieren und zusammenzuarbeiten, wodurch sowohl die mittlere Zeit bis zur Erkennung (MTTD) als auch die mittlere Zeit bis zur Reaktion (MTTR) verkürzt wird. Für Unternehmen, die die Leistungsfähigkeit von Microsoft Teams nutzen, hat Infoblox eine zertifizierte Integration entwickelt, die darauf abzielt, sofortige und priorisierte Sicherheitsbenachrichtigungen direkt in Microsoft Teams bereitzustellen, um eine schnelle Entscheidungsfindung und Maßnahmen im SOC zu ermöglichen.

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 und Mühe kostet.

SCHNELLE WERTSCHÖPFUNG DURCH EINFACHE INTEGRATION: INFOBLOX + MICROSOFT TEAMS

Die DNS Detection and Response (DNSDR)-Lösung 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 wandelt riesige Mengen an Ereignis-, Netzwerk-, Ökosystem- und DNS-Informationsdaten in verwertbare Erkenntnisse um, um die SecOps-Effizienz zu steigern. Die umfangreichen Sicherheitsdaten, die von BloxOne Threat Defense mit SOC Insights generiert werden, beseitigen blinde Flecken und erhöhen die Fähigkeit, DNS-basierte Angriffe vollständig zu verstehen.

WICHTIGE VORTEILE

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

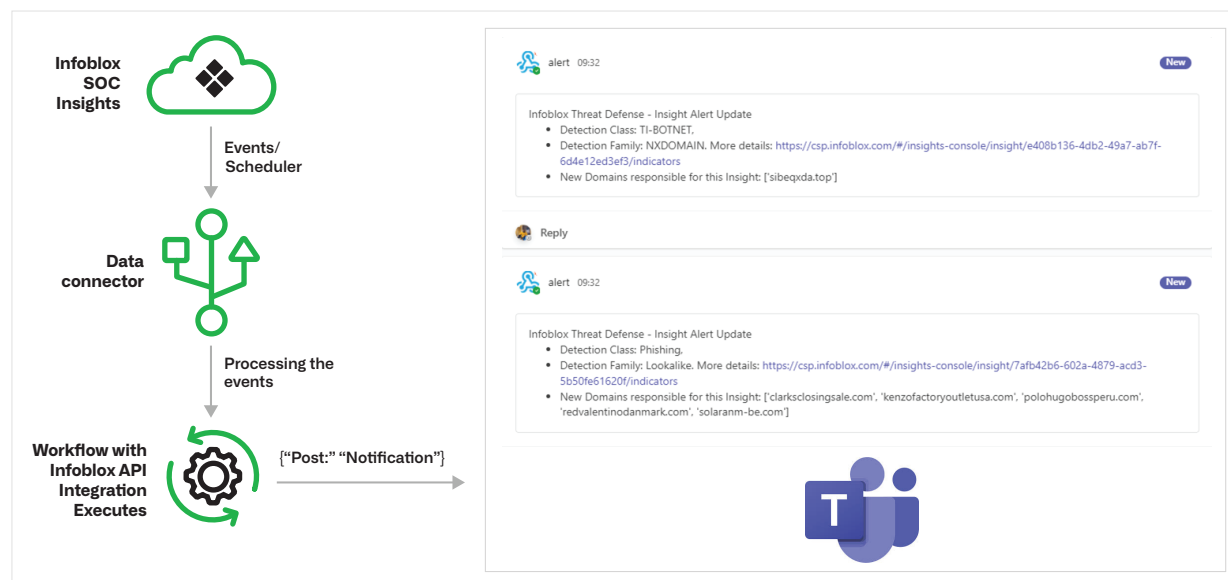
Um die allgemeine SOC-Effizienz weiter zu steigern, bietet Infoblox eine Low-Code-Integration in Microsoft Teams an, die die Vorteile jeder Lösung maximieren und die Gesamtbetriebskosten reduzieren kann. Diese leistungsstarke Kombination optimiert die Bedrohungserkennungs- und Reaktionsfähigkeiten und bietet Sicherheitsteams sofortige Benachrichtigungen über die kritischen Erkenntnisse, die zum Schutz Ihres Unternehmens erforderlich sind.

Infoblox + Microsoft Teams befähigt Sicherheitsteams zu Folgendem:

- **Vereinheitlichung von Bedrohungswarnungen:** Infoblox löst Microsoft Teams-Nachrichten in Echtzeit aus, die Sicherheitsanalysten über priorisierte Bedrohungen informieren, sodass keine manuellen Überwachungsaufgaben mit mehreren Tools mehr erforderlich sind. Warnungen werden an einen angepassten Microsoft Teams-Kanal gesendet, der Analysten eine zentralisierte Warnungsverwaltung bietet, einschließlich Verlaufsdocumentation und Nachverfolgung.
- **Vereinfachung von Ermittlungen:** Die von Infoblox gesteuerten Microsoft Teams-Nachrichten bieten Einblick in die entscheidenden Inhalte und den Kontext, die für die Triage und Zusammenarbeit bei den nächsten Schritten erforderlich sind. Klicken Sie einfach auf den bereitgestellten Link in der Nachricht, um direkt zum Infoblox-Portal zu gelangen und dort weitere Untersuchungen durchzuführen.
- **Ergreifung entschlossener Maßnahmen:** Mit den passenden Inhalten und dem Kontext, den Infoblox bereitstellt, können Sicherheitsanalysten effizient und effektiv auf die wichtigsten Bedrohungen reagieren und den Status im Nachrichtenthread in Microsoft Teams aktualisieren, um das Team informiert zu halten.

Durch die Implementierung von Infoblox für Microsoft Teams können Sicherheitsteams ihre Sicherheitslage transformieren, indem sie einen zentralen Überblick über kritische Warnmeldungen erhalten, Untersuchungen optimieren und ihre Reaktion auf Bedrohungen beschleunigen.

WIE ES FUNKTIONIERT



ÜBERLEGENE SOC-LEISTUNG DURCH DIE INTEGRATION VON INFOBLOX UND MICROSOFT TEAMS.

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

- **SOC-Effizienz:** Sorgen Sie für eine optimale Leistung, indem Sie priorisierte Bedrohungswarnungen sofort an einen zentralen Microsoft Teams-Kanal senden. Das verbessert die Kommunikation und ermöglicht die Nachverfolgung von Verlaufsdaten.
- **SOC-Effektivität:** Ermöglichen Sie Sicherheitsanalysten, Bedrohungsinhalte und -kontext direkt in der Microsoft Teams-Nachrichtenwarnung zu erhalten, um schnell und angemessen handeln zu können.
- **Betriebliche Produktivität/ROI:** Die Rationalisierung von Arbeitsabläufen und die Reduzierung von App-Wechseln können die Effizienz Ihres SecOps-Teams verbessern, was zu Zeit- und Kosteneinsparungen führt.
- **Integrationseinfachheit:** Eine einfache, getestete und zertifizierte Low-Code-Integration beschleunigt die Wertschöpfungszeit.

ZUSAMMENFASSUNG

Die Automatisierung von Sicherheits-Workloads, die Verkürzung der Erkennungs- und Reaktionszeiten sowie die Aufrechterhaltung einer effektiven Kommunikation und Zusammenarbeit bei der Bedrohungsabwehr stellen erhebliche Herausforderungen für SecOps-Teams dar. Die Integration von Infoblox mit Microsoft Teams Messaging steigert den Wert Ihres gesamten Sicherheits-Stacks, indem sie eine einheitliche Plattform für noch bessere Threat-Intelligence-Kommunikationen bietet. Diese Kombination steigert die Produktivität von SecOps, verbessert die Effizienz und gewährleistet ein robusteres und reaktionsfähigeres Sicherheitsprogramm. Durch die Nutzung von Infoblox für Microsoft Teams erhöhen Sie die Sicherheitsfähigkeiten Ihres Unternehmens und maximieren die Rendite Ihrer Sicherheitsinvestitionen.



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