LÖSUNGSHINWEIS

BEREICHERN SIE IHR SPLUNK-SIEM UND SOAR MIT INFOBLOX

Maximieren Sie den Nutzen Ihrer Splunk Enterprise SIEM- und SOAR-Investitionen durch aufschlussreiche DNS-Transparenz.

HERAUSFORDERUNGEN

Sicherheitsteams verlassen sich auf SIEM- und SOAR-Tools, um Sicherheitsvorfälle effizient zu untersuchen und darauf zu reagieren. Da Angriffe immer unauffälliger und schwieriger zu erkennen sind, sind Organisationen gezwungen, die Überwachung zu verstärken, was bedeutet, dass sie immer mehr Protokolle in ihre Sicherheitsüberwachungsplattformen einspeisen müssen. Dieser Prozess erhöht die Speicheranforderungen und die Anzahl der ausgegebenen Warnungen und durchgeführten Untersuchungen, was häufig zur Ermüdung und zum Burnout von Sicherheitsanalysten führt.

Es kann schwierig sein, auf Threat Intelligence und relevante Geräte- und Netzwerkdaten zuzugreifen und diese zu korrelieren, um Erkenntnisse für Untersuchungen zu gewinnen und eine effektive Automatisierung zu ermöglichen. Ohne diese wertvollen Kontextinformationen sind die Fähigkeiten von Playbooks eingeschränkt.

SCHNELLE WERTSCHÖPFUNG DURCH EINFACHE INTEGRATION

Infoblox, ein führender Anbieter von DNS-Infrastruktur und Sicherheit, und Splunk, ein führender SIEM- und SOAR-Lösungsanbieter, bieten einfache Integrationen, die die Fähigkeiten jeder Lösung verbessern und die Gesamteffizienz von SecOps steigern können.

Splunk Cloud Platform und Splunk Enterprise Security bieten Hybrid-Cloud-Dienste mit proaktiven und reaktiven Mechanismen zur Nutzung externer Daten. Auf der Grundlage dieser Daten ermöglichen sie den Sicherheitsteams, zu suchen, zu analysieren, zu visualisieren und zu handeln.

Infoblox BloxOne® Threat Defense mit SOC Insights integriert sich in Splunk-Lösungen, um einzigartige, priorisierte Einblicke und ereignisbezogene Daten bereitzustellen, durch Tools wie den Infoblox Threat Intelligence Data Exchange (TIDE) und Infoblox Dossier. Jede Funktion kann priorisierte Daten an Splunk liefern, um den Speicherbedarf zu minimieren und die Untersuchung, Automatisierung und andere Bemühungen der Sicherheitsanalysten zu optimieren.

VISUALISIEREN SIE INFOBLOX THREAT INTELLIGENCE-DATEN IN SPLUNK ENTERPRISE SECURITY UND DER CLOUD-PLATTFORM

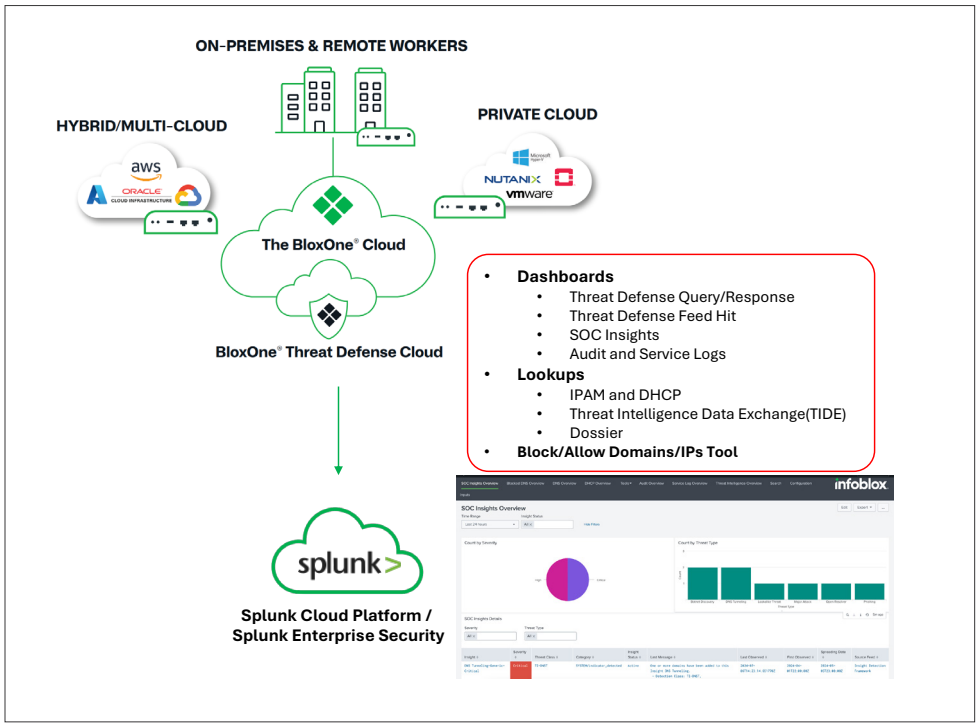
Infoblox TIDE bietet hochpräzise, maschinenlesbare Threat Intelligence an Splunk, um Sicherheitsteams dabei zu unterstützen, Bedrohungsaktivitäten zu erkennen und die Verweilzeit zu reduzieren. Die integrierte Lösung von Infoblox und Splunk unterstützt Sicherheitsteams dabei, die Untersuchungszeiten zu verkürzen und die Transparenz zu erhöhen, um das moderne hybride Netzwerk zu fördern.

WICHTIGE FÄHIGKEITEN

Die Integration von Infoblox mit der Splunk Cloud Platform, Splunk Enterprise Security und Splunk SOAR verbessert die Leistung von Splunk und erhöht die Sichtbarkeit von Ereignissen und Bedrohungsdaten, was zu schnelleren Untersuchungen und effizienteren Reaktionen führt. Die Integration ermöglicht es Sicherheits- und Incident-Response-Teams, die Leistungsfähigkeit von SIEM und SOAR vor Ort oder in der Splunk Cloud Platform besser zu nutzen, indem sie diese mit DNS-Sicherheitsereignissen, IP-Adressverwaltungs-Metadaten (IPAM) und Bedrohungsinformationen von Infoblox verknüpfen.

Die durch Infoblox TIDE erweiterten SIEM-Funktionen von Splunk ermöglichen Sicherheitsteams:

- Zugriff auf umfangreiche Geräte- und Netzwerkdaten im Kontext
- Optimieren Sie die Speicheranforderungen durch intelligente Filterung.
- Korrelieren Sie priorisierte, umfassende Threat Intelligence zu Ereignissen



WICHTIGE FÄHIGKEITEN

- Greifen Sie auf umfangreiche Geräte- und Netzwerkdaten zu (einschließlich Domains, IPs und anderer DNS-Anfragedaten), die einen unschätzbaren Kontext zu Ereignissen bieten, um fundierte Entscheidungen zu treffen.
- Korrelieren Sie priorisierte, umfassende Threat Intelligence mit Ereignissen, um Analysten Einblicke in bösartige Aktivitäten zu geben und die Untersuchung und Reaktion zu beschleunigen.
- Optimieren Sie die Speicheranforderungen durch intelligente Filterung, um die Leistung von Splunk zu maximieren und gleichzeitig sicherzustellen, dass Analysten alle „richtigen“ Daten auf Abruf zur Verfügung haben.
- Fassen Sie Sicherheitstreffer nach Indikatoren für Kompromittierungen (IoCs) zusammen und verfolgen Sie die Treffer in der Bedrohungslandschaft im Laufe der Zeit basierend auf der Bedrohungsschwere mit Zugriff auf die Infoblox Dossier-Daten.
- Beschleunigen Sie die Reaktion, indem Sie Sicherheitsereignissen mit höherem Risiko Priorität einräumen und auf Dutzende von Threat Intelligence-Feeds zugreifen.
- Überwachen Sie Geräteaktivitäten und Trends auf der gesamten Plattform mit konsolidierter Sichtbarkeit.

STEIGERN SIE DIE PRODUKTIVITÄT MIT INFOBLOX DOSSIER

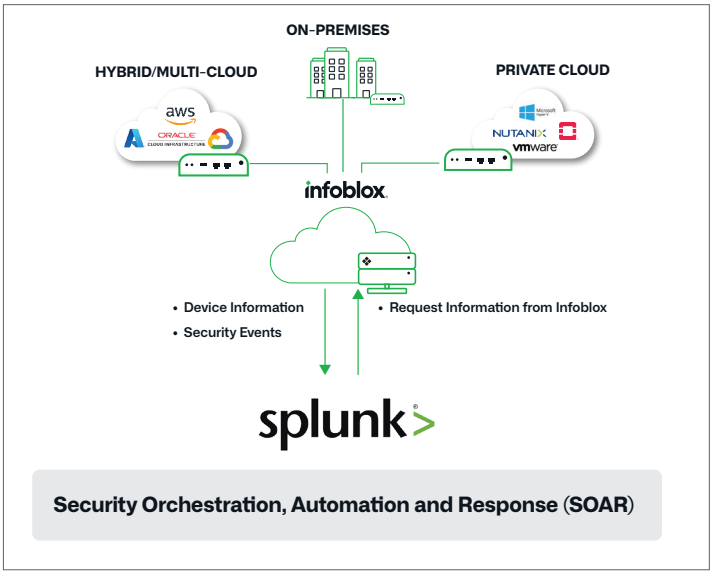
Zusätzlich zu Ereignissen, Kontext sowie Geräte- und Netzwerkmetadaten bietet Infoblox Dossier Zugriff auf umfassende Threat Intelligence. Dies kann Analysten dabei helfen, Risiken zu untersuchen und zu bewerten sowie automatisierte Reaktionen auszulösen und die Playbook-Funktionen zu verbessern.

Die durch Infoblox Dossier erweiterten Splunk SOAR-Funktionen ermöglichen es Sicherheitsanalysten:

- Erhalten Sie direkten Zugriff auf die Infoblox Threat Intelligence, um Bedrohungsaktivitäten zu erkennen.
- Automatisieren Sie eine effektive Bedrohungsreaktion mit vollständigen Gerätemetadaten
- Erweitern Sie Playbooks um umfassende Bedrohungs- und Network Insights

WICHTIGE FÄHIGKEITEN

- Erhalten Sie direkten Zugriff auf IoCs in Infoblox Threat Intelligence, um Bedrohungen und verdächtige Aktivitäten zu erkennen und zu blockieren
- Automatisieren Sie eine effektive Geräteisolierung und andere Bedrohungsreaktionen mit umfassender Sichtbarkeit und Geräte-Metadaten.
- Ermöglichen Sie Administratoren den Zugriff auf zusätzliche Bedrohungs- und Network Insight-Daten, um Ihre SOAR-Playbooks zu verbessern.
- Automatisieren/beschleunigen Sie die Reaktion mit einem vollständigen Satz von Threat Intelligence APIs
- Beschleunigen Sie die Reaktion mit besserer Threat Intelligence und durch Priorisierung von Sicherheitsereignissen mit höherem Risiko.



GESAMTVORTEILE DER SPLUNK- UND INFOBLOX-INTEGRATION

- **SIEM-Effizienz:** Sorgen Sie für optimale Leistung, indem Sie nur auf die relevanten Threat Intelligence und Netzwerkdaten zugreifen.
- **SOAR-Effektivität**: Verbessern Sie Ihre Playbooks durch zusätzlichen Zugriff auf aggregierte und kuratierte Threat Intelligence und Gerätedaten.
- **Integration Einfachheit:** Nutzen Sie bewährte Splunk-Apps, um die Wertschöpfung zu beschleunigen.
- **SecOps-Produktivität:** Verbessern Sie die Sichtbarkeit und bieten Sie erweiterte Filterfunktionen, wodurch die Effizienz von SecOps verbessert wird.
- **ROI der Investition:** Holen Sie mehr aus Ihrer SIEM- und SOAR-Investition heraus, zusätzlich zu den einzigartigen Sicherheitsvorteilen von BloxOne Threat Defense.

ZUSAMMENFASSUNG

SecOps-Teams haben Schwierigkeiten bei der Verwaltung von Workloads, der Kontrolle der Speicherkosten und dem Schritt halten mit allen vorhandenen Tools zur Untersuchung und Reaktion auf Sicherheitsvorfälle. Durch die Integration von Splunk Enterprise SIEM und SOAR mit kuratierter Threat Intelligence sowie Geräte- und Netzwerkmetadaten wird die Effektivität dieser Tools sowie die Effizienz Ihrer Sicherheitsteams verbessert. Infoblox mit Splunk steigert den Wert Ihres gesamten Sicherheits-Stacks, steigert die Produktivität und Effizienz von SecOps und macht Ihr gesamtes Sicherheitsprogramm robuster und reaktionsfähiger.

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: 20240724v4