LÖSUNGSHINWEIS

ERWEITERN SIE IHR QRADAR SIEM MIT INFOBLOX DDI UND BLOXONE THREAT DEFENSE

Erleben Sie mehr mit Ihrem IBM Security QRadar durch die unvergleichliche DNS-Transparenz von Infoblox

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. Jedoch mangelt es herkömmlichen Security Information and Event Management (SIEM)-Lösungen oft an der notwendigen Integrationstiefe mit DNS-Sicherheitsdaten, die für eine effektive Untersuchung und Reaktion erforderlich ist.

HERAUSFORDERUNGEN

Sicherheitsteams stehen in der heutigen komplexen Bedrohungslandschaft vor zahlreichen Herausforderungen:

- **Warnungsüberlastung:** Sicherheitsanalysten werden mit einem ständigen Strom von Warnungen aus verschiedenen Sicherheitstools überschwemmt, was es schwierig macht, die kritischsten Bedrohungen zu identifizieren und zu priorisieren.
- **Eingeschränkte Sichtbarkeit:** Traditionelle SIEM-Lösungen haben oft nicht die Fähigkeit, die umfangreichen Sicherheitsdaten zu erfassen und zu analysieren, die von der Infoblox DDI-Infrastruktur und BloxOne Threat Defense generiert werden. Dies schafft blinde Flecken und behindert das vollständige Verständnis von DNS-basierten Angriffen.
- **Ineffiziente Arbeitsabläufe:** Die Untersuchung von Bedrohungen erfordert häufig das Wechseln zwischen verschiedenen Sicherheitstools, was wertvolle Zeit und Mühe kostet.

SCHNELLE TIME-TO-VALUE DURCH EINFACHE INTEGRATION

Infoblox, der führende Anbieter im Bereich DNS, DHCP und IP-Adressverwaltung (DDI) sowie DNS-Sicherheit, bietet zusammen mit IBM Security QRadar, einem führenden Anbieter von SIEM- und SOAR-Lösungen, eine einfache Integration, die die Fähigkeiten jeder Lösung verbessern und die Gesamteffizienz von SecOps steigern kann. Diese leistungsstarke Kombination verbessert die Fähigkeiten zur Erkennung und Reaktion auf Bedrohungen und bietet Ihrem Sicherheitsteam die kritischen Erkenntnisse, die es benötigt, um Ihr Unternehmen effektiver zu schützen.

Diese leistungsstarke Kombination ermöglicht Sicherheitsteams Folgendes:

- **Untersuchungen vereinfachen:** Optimieren Sie Ihre Sicherheitsworkflows, indem Sie vorgefertigte Dashboards und Benutzeraktionen in QRadar nutzen. Diese Funktionen bieten schnellen Zugriff auf wichtige Informationen über DNS-Aktivitäten, Threat Intelligence und kontextbezogene Netzwerkdaten und reduzieren so die Zeit, die für die Untersuchung und Reaktion auf Vorfälle benötigt wird.

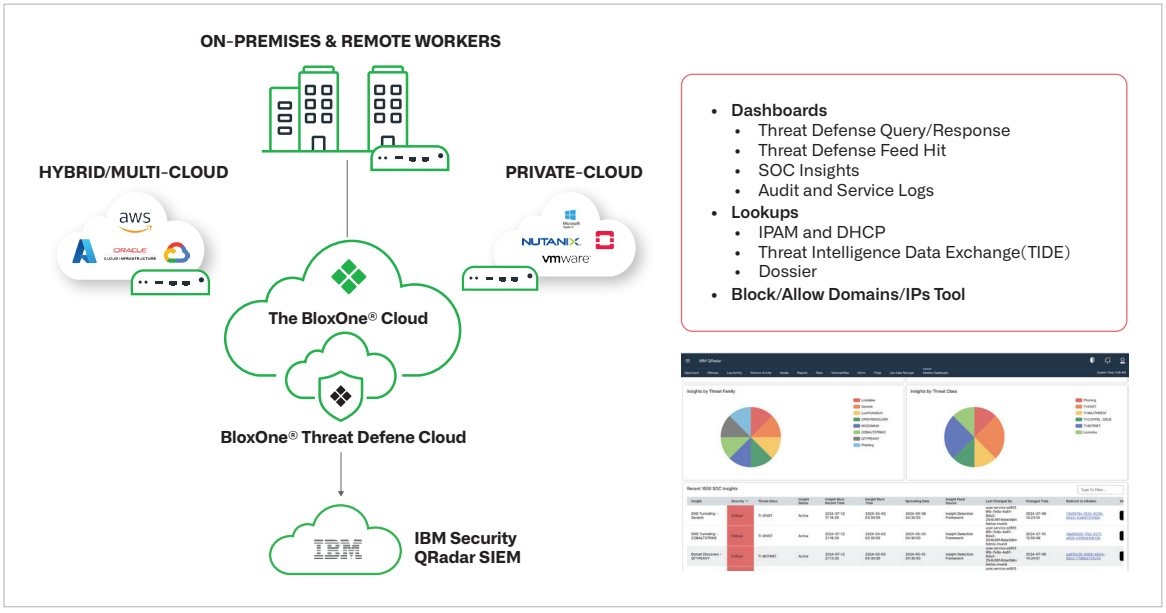
WICHTIGE VORTEILE

- **Verbesserte Sichtbarkeit:** Gewinnen Sie tiefgehende Einblicke in die DNS-, DHCP- und IPAM-Aktivitäten Ihres Netzwerks, um eine umfassende Netzwerktransparenz sicherzustellen.
- **Beschleunigte Reaktion:** Beschleunigen Sie die Reaktion auf Vorfälle mit direktem Zugriff auf die Threat Intelligence von Infoblox und Kontextdaten innerhalb von QRadar.
- **Reduzierte Warnungsermüdung:** Konzentrieren Sie sich auf kritische Bedrohungen, indem Sie nicht wesentliche Warnungen herausfiltern und so die Belastung Ihrer Sicherheitsanalysten verringern.
- **Maximierter ROI:** Steigern Sie den Wert Ihrer QRadar-Investition, indem Sie die fortschrittliche Threat Intelligence von Infoblox nutzen.

- **Die Threat Intelligence vereinheitlichen:** Verschaffen Sie sich einen umfassenden Überblick über Ihre Netzwerkaktivitäten, indem Sie Infoblox-Daten wie DNS-Ereignisse, DHCP-Leases, Audit-Protokolle und Threat Intelligence-Feeds mit anderen von QRadar erfassten Sicherheitsereignissen korrelieren. Diese ganzheitliche Sicht ermöglicht es Analysten, das gesamte Ausmaß potenzieller Bedrohungen zu identifizieren und zu verstehen.
- **Entschlossene Maßnahmen ergreifen:** Ermöglichen Sie Ihren Sicherheitsanalysten, direkt von QRadar aus sofort gegen Bedrohungen vorzugehen. Die Infoblox-App erlaubt es, bösartige Domains und IPs mit einem einzigen Klick zu blockieren, wodurch der potenzielle Schaden eines Angriffs minimiert wird.

Durch die Implementierung der Infoblox-App für QRadar können Sicherheitsteams ihre Sicherheitslage transformieren, indem sie eine zentrale Übersicht über die Netzwerkaktivitäten gewinnen, Untersuchungen optimieren und ihre Reaktion auf Bedrohungen beschleunigen.

WICHTIGE FÄHIGKEITEN



App-Konfiguration

- **Reibungslose Konfiguration:** Einfache Einrichtung innerhalb von QRadar, um eine Verbindung zu den fortschrittlichen Sicherheitsdiensten von Infoblox herzustellen.

Dashboards

- **DNS-Ereignisübersicht:** Bietet eine klare Visualisierung der DNS-Aktivitäten, um potenzielle Bedrohungen schnell zu identifizieren.
- **DHCP-Lease-Übersicht:** Überwacht DHCP-Zuweisungen, um ungewöhnliches Verhalten und potenzielle Sicherheitsprobleme zu erkennen.
- **Übersicht über Audit-Protokolle:** Verfolgt Änderungen an der Netzwerkkonfiguration, um die Einhaltung von Vorschriften und die Sicherheit zu gewährleisten.
- **Übersicht über blockierte DNS-Anfragen:** Analysiert blockierte Anfragen, um Bedrohungen zu verhindern und darauf zu reagieren.
- **SOC Insights-Übersicht:** Fasst kritische Sicherheitseinblicke und Warnungen zusammen.

Benutzeraktionen

- **Dossier-Suche:** Untersuchen Sie mit Infoblox Dossier schnell Domains, IPs und andere Indikatoren für Kompromittierungen.
- **TIDE-Suche:** Greifen Sie auf detaillierte Threat Intelligence zu, um fundierte Sicherheitsentscheidungen zu treffen.
- **IPAM-Suche:** Rufen Sie IP-Adressdaten ab, um Netzwerkaktivitäten mit potenziellen Bedrohungen zu korrelieren.
- **DHCP-Lease-Suche:** Verfolgen Sie Geräteaktivitäten anhand von DHCP-Lease-Datensätzen.
- **Domain-/IP-Blockierung:** Blockieren oder erlauben Sie Domains und IPs direkt in QRadar, um die Bedrohungsabwehr zu optimieren.

Die Infoblox-App für QRadar stärkt Ihre Sicherheitsoperationen mit erweiterter Sichtbarkeit, verbesserten Reaktionszeiten und gesteigerter Effizienz, wodurch Ihr Unternehmen besser gegen aufkommende Bedrohungen geschützt ist.

GESAMTINTEGRATION VON QRADAR UND INFOBLOX

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

- **SIEM-Effizienz:** Sorgen Sie für optimale Leistung, indem Sie nur auf die relevanten Threat Intelligence und Netzwerkdaten zugreifen.
- **SOAR-Effektivität:** Verbessern Sie Ihre Sicherheitsorchestrierung und -automatisierung mit angereicherten Daten und erweiterten Filterfunktionen.
- **Einfache Integration:** Die schnelle und einfache Integration mit bewährten Methoden beschleunigt die Wertschöpfung.
- **Betriebliche Produktivität:** Verbessern Sie die Effizienz Ihrer Sicherheitsoperationen, indem Sie erweiterte Sichtbarkeits- und Filterfunktionen bereitstellen.
- **ROI der Investition:** Steigern Sie die Rendite Ihrer SIEM- und SOAR-Investitionen mit den zusätzlichen Sicherheitsvorteilen von BloxOne Threat Defense.

ZUSAMMENFASSUNG

Die Verwaltung von Sicherheits-Workloads, die Kontrolle der Speicherkosten und die Aufrechterhaltung einer effektiven Bedrohungsabwehr stellen erhebliche Herausforderungen für SecOps-Teams dar. Die Integration von Infoblox mit QRadar steigert den Wert Ihres gesamten Sicherheits-Stacks, indem sie erweiterte Threat Intelligence und umfassende Netzwerkdaten bereitstellt. Diese Kombination steigert die Produktivität von SecOps, verbessert die Effizienz und gewährleistet ein robusteres und reaktionsfähigeres Sicherheitsprogramm. Durch die Nutzung der Infoblox-App für QRadar steigern Sie die Sicherheitsfähigkeiten Ihres Unternehmens und maximieren die Rendite Ihrer Sicherheitsinvestitionen.

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

+1 408 986 4000
www.infoblox.com

Version: 20240703v1