ソリューションノート

INFOBLOX DDI と BLOXONE THREAT DEFENSE で QRADAR SIEM を強化

Infoblox のこれまでにない DNS の可視性で、IBM Security QRadar からより多くの情報を収集

今日のセキュリティの状況は複雑で、絶えず進化しています。サイバー犯罪者は、フィッシングキャンペーン、マルウェア配布、データ流出などの高度な攻撃を仕掛けるために、DNS インフラを標的にするケースが増えています。セキュリティアナリストは、こうした脅威を特定し、迅速に対応しなければならないという大きなプレッシャーにさらされています。しかし、従来のセキュリティ情報とイベント管理（SIEM）ソリューションは、効果的な調査と対応に必要な DNS セキュリティデータと十分に統合されていないことが珍しくありません。

課題

セキュリティチームは、今日の複雑な脅威環境の中で多くの課題に直面しています。

- **アラートの過多：**セキュリティアナリストは、複数のセキュリティツールから絶え間なく届くアラートの波に圧倒され、最も重要な脅威を特定して優先順位を付けることが非常に難しくなっています。
- **限られた可視性：**従来の SIEM ソリューションは、Infoblox DDI インフラと BloxOne Threat Defense が生成する豊富なセキュリティデータを取得し分析する能力に欠けていることがよくあります。そのため、盲点が生じ、DNSベースの攻撃を完全に理解することが妨げられています。
- **非効率的なワークフロー：**脅威の調査には、異なるセキュリティツールを行き来する必要があり、貴重な時間と労力が無駄になることが多くあります。

容易な統合による迅速な価値実現

DNS、DHCP、IP アドレス管理（DDI）および DNS セキュリティのリーダーである Infoblox は、主要な SIEM およびSOARプロバイダーである IBM Security QRadar と共に、各ソリューションの機能を向上させ、SecOps 全体の効率を高める簡単な統合を提供します。この強力な組み合わせにより、脅威の検出と対応能力が強化され、セキュリティチームに組織をより効果的に保護するために必要な重要な洞察が提供されます。

この強力な組み合わせにより、セキュリティチームは次のことを実現できます。

- **調査の簡素化：**QRadar にあらかじめ組み込まれたダッシュボードとユーザーアクションを活用して、セキュリティワークフローを効率化できます。これらの機能により、DNS アクティビティ、threat intelligence、コンテキストに基づくネットワークデータに関する重要な情報に迅速にアクセスでき、インシデントの調査と対応にかかる時間を短縮できます。
- **Threat Intelligence の統合：**DNS イベント、DHCP リース、監査ログ、Threat Intelligence フィードなどの Infoblox データを、QRadar が収集する他のセキュリティイベントと関連付けることで、ネットワーク活動の全体像を得ることができます。この全体像により、アナリストは潜在的な脅威の全範囲を特定し、理解することが可能になります。

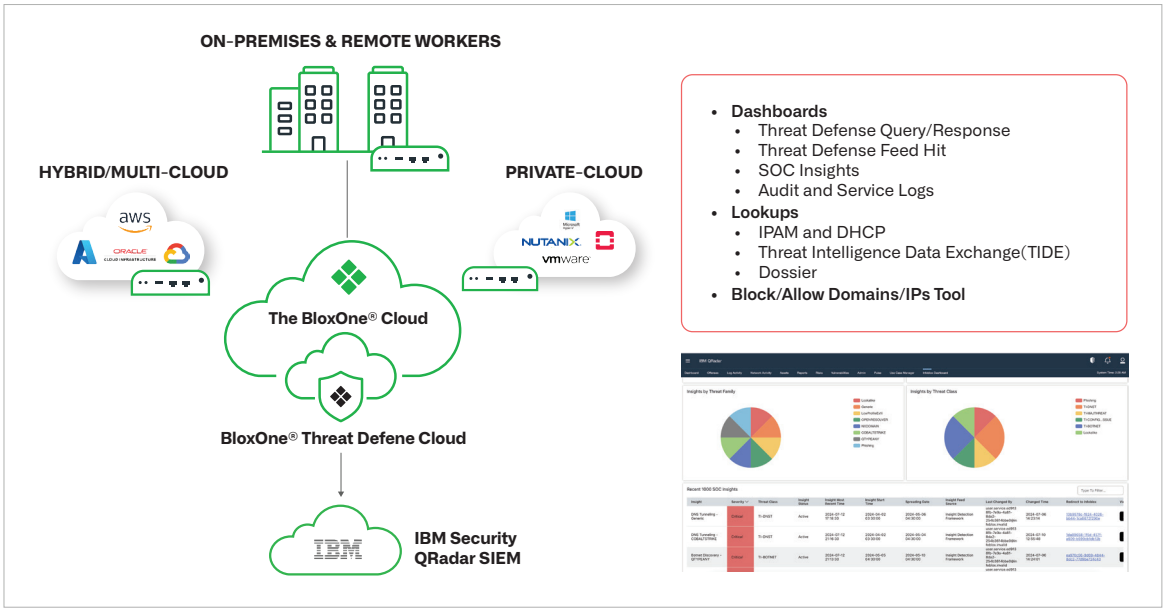
主なメリット

- **可視性の向上：**ネットワークの DNS、DHCP、および IPAM アクティビティに関する深い洞察を得て、包括的なネットワークの可視性を確保します。
- **迅速な対応：**QRadar 内で Infoblox の脅威インテリジェンスとコンテキストデータに直接アクセスすることで、インシデント対応を高速化します。
- **アラート疲れの軽減：**重要でないアラートを除外することで重大な脅威に焦点を当て、セキュリティアナリストの負担を軽減します。
- **ROI の最大化：**Infoblox の高度な脅威インテリジェンスを活用して、QRadar への投資価値を高めます。

- **対応策の決定：**セキュリティアナリストが QRadar から直接脅威に対して即座に行動を起こせるようにします。Infoblox アプリを使用すると、悪意のあるドメインや IP をワンクリックでブロックでき、攻撃による潜在的な被害を最小限に抑えることができます。

QRadar 用の Infoblox アプリを実装することにより、セキュリティチームはネットワーク活動の集中ビューを得て、調査を効率化し、脅威への対応を迅速化することで、セキュリティ体制を変革できます。

主な機能



アプリケーション構成

- **シームレスな構成：**QRadar 内で簡単にセットアップし、Infoblox の高度なセキュリティサービスに接続します。

ダッシュボード

- **DNS イベントの概要：**DNS の活動を明確に視覚化できるため、潜在的な脅威を迅速に特定するのに役立ちます。
- **DHCP リースの概要：**DHCP の割り当てをモニターし、異常な動作や潜在的なセキュリティ問題を検出します。
- **監査ログの概要：**ネットワーク構成の変更を追跡し、コンプライアンスとセキュリティを確保します。
- **ブロックされた DNS リクエストの概要：**ブロックされたリクエストを分析し、脅威を防止し、脅威に対応します。
- **SOC Insights の概要：**重要なセキュリティインサイトとアラートを要約します。

ユーザーアクション

- **Dossier ルックアップ：**Infoblox Dossier を使用して、ドメイン、IP、その他の侵害の兆候を迅速に調査します。
- **TIDE ルックアップ：**詳細な threat intelligence にアクセスし、情報に基づいたセキュリティ上の判断を行います。
- **IPAM ルックアップ：**IPアドレスデータを取得し、ネットワーク活動を潜在的な脅威と関連付けます。
- **DHCP リースルックアップ：**DHCP リースの記録を通じてデバイスの活動を追跡します。
- **ドメイン / IPブロック：**QRadar 内でドメインと IP を直接ブロックまたは許可し、脅威の軽減を効率化します。

QRadar 用の Infoblox アプリは、高度な可視性、応答時間の改善、効率性の向上によってセキュリティ運用を強化し、組織を新たな脅威からより強力に保護します。

QRADAR と INFOBLOX の包括的な統合

QRadar と Infoblox を統合することにより、既存のインフラストラクチャを強化する包括的なセキュリティソリューションを提供します。この相乗効果により、次のことが実現できます：

- **SIEM の効率性：**関連する threat intelligence とネットワークデータのみにアクセスすることで、最適なパフォーマンスを維持します。
- **SOAR の有効性：**強化されたデータと高度なフィルタリング機能を活用して、セキュリティのオーケストレーションと自動化を強化します。
- **統合の容易さ：**実績のある方法を用いた迅速かつ簡単な統合により、価値実現までの時間を短縮します。
- **業務の生産性：**高度な可視性とフィルタリング機能が提供されることで、セキュリティ運用の効率が向上します。
- **投資対効果：**BloxOne Threat Defense の追加セキュリティ機能により、SIEM および SOAR への投資収益率が向上します。

結論

セキュリティワークロードの管理、ストレージコストの制御、効果的な脅威対応の維持は、SecOps チームにとって大きな課題です。Infoblox と QRadar の統合により、強化された threat intelligence と包括的なネットワークデータが提供され、セキュリティスタック全体の価値が向上します。この組み合わせにより、SecOps の生産性が向上し、効率が改善され、より堅牢で応答性の高いセキュリティプログラムを実現できます。QRadar 用の Infoblox アプリを活用することで、組織のセキュリティ機能を向上させ、セキュリティ投資のリターンを最大化することが可能です。

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37 VORT外苑前 I 3F

03-5772-7211
www.infoblox.com

バージョン: 20240703v1