ソリューションノート

INFOBLOX を活用して、SPLUNK SIEM と SOAR を強化

DNS の可視性を明らかにすることで、Splunk Enterprise SIEM および SOAR への投資を最大限に活用できます。

課題

セキュリティイベントを効率的に調査し、対応するために、セキュリティチームは SIEM および SOAR のツールに依存しています。攻撃のステルス化が進み、検出が困難になるにつれて、組織は監視を強化せざるを得なくなっています。そのためには、セキュリティ監視プラットフォームにますます多くのログを取り込む必要があります。このプロセスにより、ストレージ要件と発行されるアラートの数、実施される調査の数が増加し、セキュリティアナリストの疲弊につながることがよくあります。

調査の分析と効果的な自動化のために threat intelligence と関連するデバイスやネットワークデータにアクセスしてそれらを関連付けるのが難しい場合があります。この貴重なコンテキスト情報がなければ、プレイブックの機能は制限されてしまいます。

簡単な統合を通じた迅速な価値提供

DNS インフラストラクチャとセキュリティのリーダーである Infoblox と、大手 SIEM および SOAR ソリューションプロバイダーである Splunk は、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、簡単に導入できる統合を提供します。

Splunk Cloud Platform と Splunk Enterprise Security は、外部データを活用するための能動的および受動的なメカニズムを備えたハイブリッドクラウドサービスを提供します。活用するデータに基づいて、セキュリティチームが検索、分析、視覚化、対応を行えるようにします。

Infoblox BloxOne® Threat Defense with SOC Insights が Splunk ソリューションと統合されると、Infoblox Threat Intelligence Data Exchange（TIDE）や Infoblox Dossier などのツールを介して、独自の優先順位付けされたインサイトとイベント関連データが提供されます。各機能は、優先順位付けされたデータを Splunk に配布し、ストレージ要件を最小限に抑え、セキュリティアナリストによる調査、自動化、その他の作業を最適化できます。

SPLUNK ENTERPRISE SECURITY および CLOUD PLATFORM 内の INFOBLOX THREAT INTELLIGENCE データを視覚化

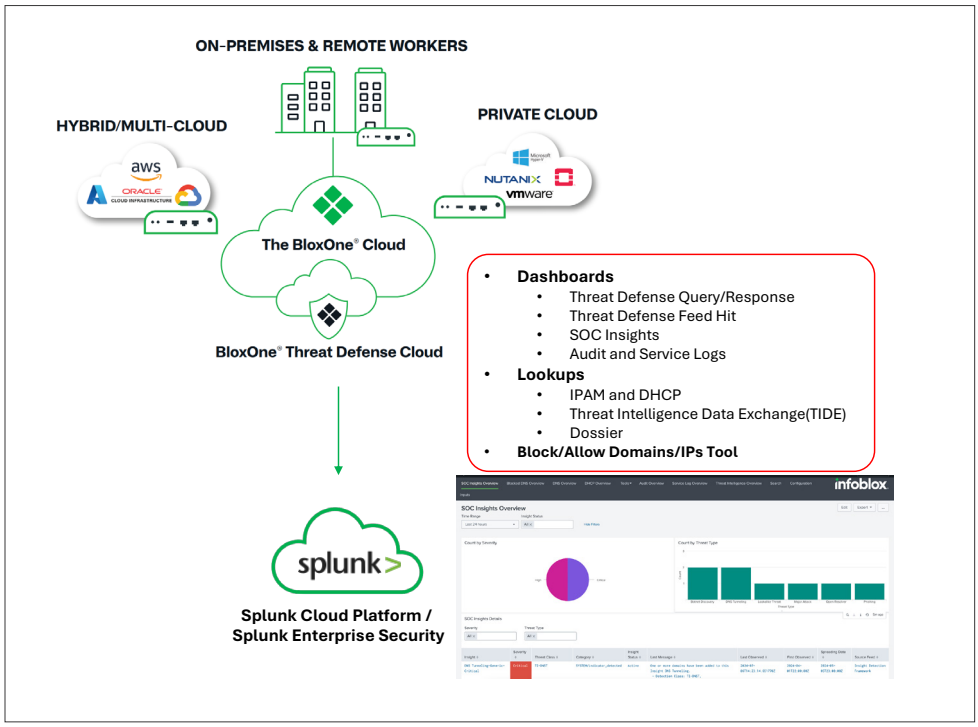
Infoblox TIDE は、Splunk に非常に正確な機械読み取り可能な threat intelligence を提供し、セキュリティチームが脅威の活動を検出し、滞留時間を短縮できるようにします。Infoblox と Splunk の統合ソリューションは、セキュリティチームによる調査時間の短縮、高度な可視性による最新のハイブリッドネットワークのサポートを促進します。

主な機能

Infoblox と Splunk Cloud Platform、Splunk Enterprise Security、Splunk SOAR を統合すると、Splunk のパフォーマンスが強化され、イベントと threat intelligence の可視性が向上し、それに伴い調査のスピードが上がり、対応の効率性が高まります。この統合により、Infoblox からの DNS セキュリティイベント、IP アドレス管理（IPAM）メタデータ、脅威情報がオンプレミスまたは Splunk Cloud Platform に組み合わされ、セキュリティチームとインシデント対応チームは、SIEM と SOAR の能力をより有効に活用できます。

Infoblox TIDE によって強化された Splunk SIEM の機能により、セキュリティチームは以下のことが実現できます。

- コンテキストを得るために、広範なデバイスおよびネットワークデータへのアクセス
- インテリジェンスフィルタリングを介してストレージ要件の最適化
- イベントに関する優先順位付けされた、包括的な threat intelligence の関連付け



主な機能

- 広範なデバイスおよびネットワークデータ（ドメイン、IP、その他の DNS リクエストデータを含む）にアクセスし、イベントに関する貴重なコンテキストを提供して、インテリジェンスに基づく意思決定を促進します。
- 優先順位付けされた包括的な threat intelligence をイベントに関連付け、アナリストに悪意のある活動に関するインサイトを提供し、調査と対応を迅速化します。
- インテリジェンスフィルタリング機能でストレージ要件を最適化し、Splunk のパフォーマンスを最大化すると同時に、アナリストがオンデマンドですべての「正しい」データを入手できるようにします。
- セキュリティ攻撃を侵害指標（IoC）ごとにまとめ、Infoblox Dossier データにアクセスし脅威の深刻度に基づいて時間の経過に伴う脅威状況の変化を追跡します。
- 何十もの脅威情報フィードにアクセスしてリスクの高いセキュリティイベントに優先順位付けし、対応をスピードアップします。
- 統合された可視性を活用して、プラットフォーム全体のデバイスの活動とトレンドをモニターします。

INFOBLOX DOSSIER の活用で生産性を飛躍的に向上させる

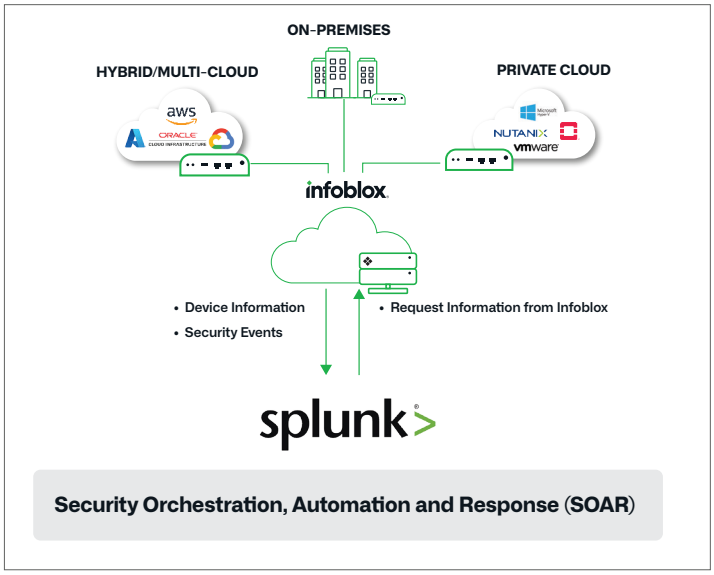
イベント、コンテキスト、デバイスとネットワークのメタデータに加えて、Infoblox Dossier は詳細な threat intelligence にもアクセスできます。これは、アナリストがリスクを調査し評価するのに役立つだけでなく、対応を自動化し、プレイブック機能を向上させるのにも役立ちます。

Infoblox Dossier によって強化された Splunk SOAR の機能により、セキュリティアナリストは以下のことを実行できます。

- 脅威活動を検出するために Infoblox threat intelligence に直接アクセス
- 完全なデバイスメタデータを用いて効果的な脅威対応を自動化
- 包括的な脅威と Network Insight でプレイブック機能を強化

主な機能

- Infoblox Threat Intelligence の IoC に直接アクセスし、脅威や疑わしい活動を検出して阻止
- 広範な可視性とデバイスメタデータを活用し、効果的にデバイスの隔離やその他の脅威への対応を自動化
- SOAR プレイブックを改善するために、脅威とネットワークのインサイトデータへのアクセス権を管理者に付与
- 完全な threat intelligence API セットを使用して、対応を自動化し加速化
- より優れた threat intelligence を使用し、リスクの高いセキュリティイベントを優先することで、対応を迅速化



SPLUNK と INFOBLOX の統合による全体的なメリット

- **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**：集約され、厳選された threat intelligence とデバイスデータにアクセスできることで、プレイブック機能が強化されます。
- **統合の容易さ：**簡単に導入でき、実績のある Splunk アプリを活用して、価値を実現するまでの時間を短縮できます。
- **SecOps の生産性：**可視性の向上、高度なフィルタリング機能で、SecOps の効率性と生産性を向上させます。
- **投資 ROI：**BloxOne Threat Defense の独自のセキュリティ上の利点に加え、SIEM および SOAR への投資からより多くのメリットを得ることができます。

結論

SecOps チームは、ワークロードの管理、ストレージコストの制御、セキュリティイベントの調査と対応を行うための既存のツールすべてに対応することに苦労しています。Splunk Enterprise SIEM と SOAR を、厳選された threat intelligence、デバイスおよびネットワークメタデータと統合することで、これらのツールの有効性とセキュリティチームの効率の両方が向上します。Infoblox と Splunk を組み合わせることで、セキュリティスタック全体の価値が高まり、SecOps の生産性と効率が向上し、セキュリティプログラム全体がより堅牢で応答性が高くなります。

infoblox.

Infobloxはネットワークとセキュリティを統合して、これまでにないパフォーマンスと保護を提供します。Fortune 100企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に検知・対処できます。

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：20240724v4