ソリューションノート

MICROSOFT TEAMS 上のリアルタイムセキュリティアラートでSOC の生産性を向上

相関付けおよび優先順位付けされた DNS ベースのセキュリティデータを含む Microsoft Teams のメッセージを自動送信

現代のセキュリティ環境は非常に複雑で、常に進化しています。サイバー犯罪者は、フィッシングキャンペーン、マルウェアの拡散、データ窃取といった高度な攻撃手段として、DNS インフラストラクチャをターゲットにするケースが増加しています。セキュリティアナリストは、こうした脅威に迅速に対処するためのプレッシャーにさらされながら、複数のアプリケーションを監視し、検索するためのリソースの確保が難しいのが現状です。「スイベルチェア型」の作業（複数のツールを切り替えて行う作業）は非常に非効率であり、セキュリティチームは、使い慣れた単一のツールを用いて、より効率的なコミュニケーションとコラボレーションを行う必要性が高まっています。このような状況では、平均検出時間（MTTD）と平均対応時間（MTTR）を短縮することが重要です。Microsoft Teams を活用している企業向けに、Infoblox は、Microsoft Teams 上で優先度に応じたセキュリティ通知を即座に受け取れる認定統合機能を開発しました。この統合機能により、SOC チームはより迅速かつ的確に意思決定を行い、対応を進めることができるようになります。

課題

セキュリティチームは、今日の複雑化した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。
- **可視性の欠如：**従来のセキュリティソリューションでは、脅威の背景や影響範囲を簡単に分析し、次に取るべき対応を判断する能力が十分でない場合があります。
- **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。

簡単な統合による迅速な価値実現：INFOBLOX + MICROSOFT TEAMS

Infoblox の DNS 検出および対応（DNSDR）ソリューションである BloxOne Threat Defense は、SOC Insights によって強化され、自動的に大量の DNS Threat Intel とアセットデータを分析し、脅威に対する実行可能な対応策を関連付けて優先順位を付けます。このソリューションは、膨大なイベント、ネットワーク、エコシステム、DNS インテリジェンスデータを実行可能なインサイトに変換し、SecOps の効率を向上させます。BloxOne Threat Defense と SOC Insights によって生成される豊富なセキュリティデータにより、盲点が排除され、DNS ベースの攻撃に対する理解力が向上します。

さらに、SOC の効率を向上させるために、Infoblox は Microsoft Teams へのローコード統合を提供し、各ソリューションの利点を強化し、総所有コストの削減を実現します。この強力な組み合わせにより、脅威の検出と対応機能が効率化され、セキュリティチームに必要な重要な洞察が即時に通知されることで、組織の保護が強化されます。

主なメリット

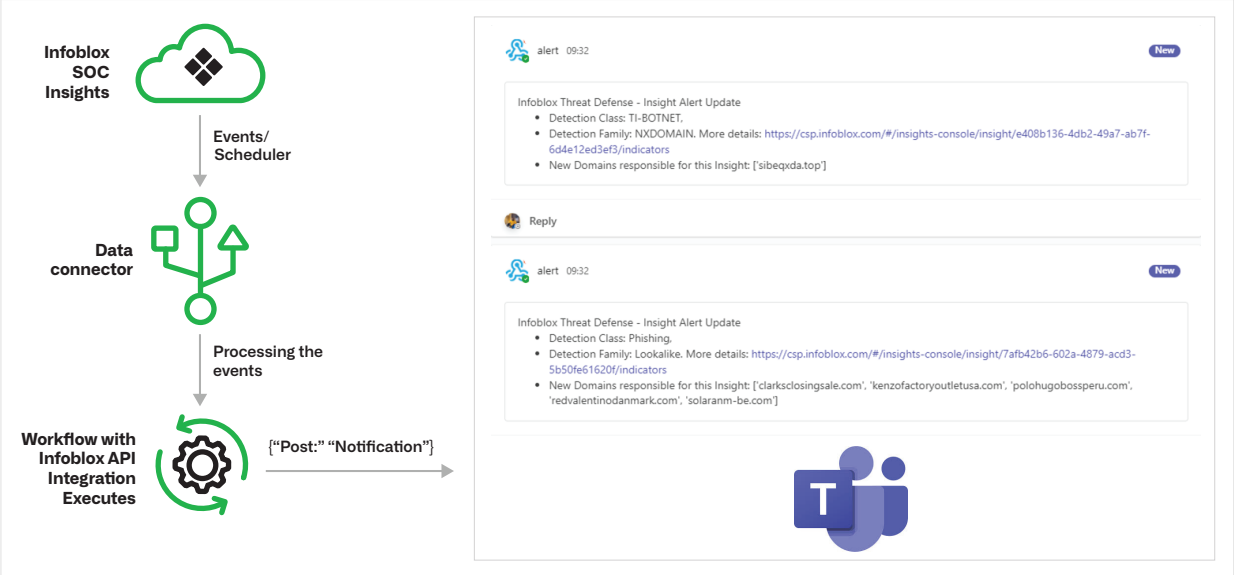
- **一元管理されたコミュニケーションとコラボレーション：**優先度の高いセキュリティアラートを Microsoft Teams 内で直接自動的に受け取ることができ、複数のツールを手動で監視する手間を省きます。
- **迅速な対応：**脅威のコンテキストと詳細に直接アクセスすることで、インシデント対応が加速し、次のステップを素早く決定できます。
- **アラート疲労の軽減：**重大な脅威のみが通知されるため、セキュリティアナリストの負担とノイズが減少します。
- **ROI の最大化：**セキュリティワークフローを効率化し、アプリの切り替えを減らすことで、Microsoft Teams への投資価値を最大化します。

Infoblox と Microsoft Teams は、セキュリティチームに次のようなメリットを提供します：

- **脅威アラートの統合：**Infoblox は、セキュリティアナリストに優先度の高い脅威を通知する Microsoft Teams メッセージをリアルタイムでトリガーし、複数のツールを手動で監視する手間を即座に排除します。アラートはカスタマイズされた Microsoft Teams チャンネルに送信され、アナリストは過去の記録や追跡も含めたアラートの一元管理が可能になります。
- **調査の簡素化：**Infoblox によって送信される Microsoft Teams メッセージは、トリアージや次のステップでのコラボレーションに必要となる重要なコンテンツとコンテキストを提供します。メッセージ内のリンクをクリックするだけで、Infoblox ポータルに直接アクセスし、さらに調査を進めることができます。
- **的確な対応を実行：**Infoblox が提供する適切なコンテンツとコンテキストを活用して、セキュリティアナリストは最も重要な脅威に効率的かつ効果的に対応し、Microsoft Teams のメッセージスレッドでステータスを更新することで、チームに最新情報を提供します。

Microsoft Teams 用の Infoblox を実装することで、セキュリティチームは重要なアラートを一元的に把握し、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。

仕組み



INFOBLOX と MICROSOFT TEAMS の統合による卓越した SOC パフォーマンス

Infoblox と Microsoft Teams を統合することで、既存のインフラストラクチャを強化し、共同で対応できるセキュリティソリューションが提供されます。この相乗効果により、次のことが実現できます：

- **SOC の効率化：**優先度の高い脅威アラートを Microsoft Teams の一元管理されたチャンネルに即座に送信することで、最適なパフォーマンスを維持します。これにより、コミュニケーションが強化され、過去のデータの追跡も可能になります。
- **SOC の有効性：**Microsoft Teams のメッセージアラート内で脅威に関するコンテンツとコンテキストを直接提供することにより、セキュリティアナリストは迅速かつ適切な対応ができるようになります。
- **業務の生産性／ROI：**ワークフローを効率化し、アプリの切り替えを減らすことで、SecOps チームの効率が向上し、時間とコストの節約が実現できます。
- **統合の容易さ：**簡単でテスト済み、認定されたローコード統合により、迅速に導入し、価値を実現するまでの時間を短縮できます。

結論

セキュリティ業務の自動化、検出および対応時間の短縮、そして効果的な脅威対応のためのコミュニケーションとコラボレーションの維持は、SecOps チームにとって重要な課題です。Infoblox と Microsoft Teams メッセージングの統合により、強化された脅威インテリジェンス通信のための統一プラットフォームが提供され、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。Infoblox for Microsoft Teams を活用することで、貴社のセキュリティ機能を強化し、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：20240724v1