Press Release

2024 年 2 月 15 日（木）

Infoblox 株式会社

Infoblox の AI 搭載「SOC Insights」が 重要なセキュリティ運用の課題を軽減

- **BloxOne® Threat Defense SOC Insights は、セキュリティ人材不足、アラート疲れ、スキル不足によって深刻化するセキュリティチームの課題を解決します。**
- **SOC Insights は、BloxOne Threat Defesnse を強化し、より迅速なインシデント調査と対応時間短縮を実現します。**
- **SOC Insights は、AI を活用して膨大な量の脅威とネットワークデータを分析して最も重要なものを特定し、迅速な修復と封じ込めのために広範なセキュリティ・エコシステムとの自動化を推進します。**

2024 年 2 月 15 日（木）―クラウドネットワーキングおよびセキュリティサービスのリーダーである Infoblox Inc. は本日、DNS Detection and Response ソリューションである BloxOne® Threat Defense を強化する、業界初の AI 主導型セキュリティオペレーションソリューション「SOC Insights」を発表しました。 SOC Insights は、膨大なセキュリティイベント、ネットワーク、エコシステム、独自の DNS インテリジェンスデータを AI で即座にアクション可能なインサイトとして提供することで、セキュリティアナリストは重要な調査を迅速に開始でき、インシデント対応時間を劇的に短縮することができます。

SOC Insights は、単純なマルウェアリスクベースのダッシュボードの枠を超え、サイバーセキュリティチームが個々のアラートを独自のインサイトとして統合することで無駄な調査時間を排除し、平均対応時間（MTTR）の短縮を可能にします。各インサイトから、デバイス、イベント、攻撃者のインフラの詳細と Infoblox 独自の DNS インテリジェンスデータに簡単にアクセス可能になります。これにより、SecOps チームが個々のアラートの追跡に時間をかけたり、脅威情報に関するコンテキスト収集のために NetOps チームからユーザーやデバイスの情報を待つ必要がなくなります。

SOC Insights は SecOps にとって 1 つのブレイクスルーになるもので、特に予算やリソースが限られている場合に、本当に重要なことに集中することができます。Infoblox では、AI 主導の分析と DNS 主導のインテリジェンスである SOC Insights が業界標準となることで、SecOps の効率を劇的に向上させる未来を描いています。

生成 AI やクラウドのようなテクノロジーの進化にともない、サイバーセキュリティのスキル不足が続く中、高度な攻撃の増加は、これまで以上にビジネスリスクを高める結果となっています。 SOC Insights により、Infoblox BloxOne Threat Defense は以下のような SecOps チームの重要な課題の解消を支援します。

- 複雑化するサイバー攻撃: 独自の DNS 脅威インテリジェンスを適用することで、他のツールでは見過ごされる脅威を特定し、脅威が発生する前に阻止します。

- アラート疲れ: 何十万ものアラートを、行動可能なガイダンスとともに、より管理しやすいインサイトのセットに絞り込むことで、最も重要なイベントを迅速に特定し、調査と修復のプロセスを加速します。

- インシデント対応時間の長期化: 膨大な量のイベント、ネットワーク、固有の DNS インテリジェンスデータの収集、フィルタリング、解釈にかかる無駄な時間を排除し、SecOps が迅速かつ自動的に対処を開始できるようにします。

- 活用されていない既存のセキュリティエコシステム: AI 主導のインサイトを相関・フィルタリングされたデータと共有し、自動応答をトリガーにすることで、セキュリティスタックの他のツールをより効果的にし、SOC ツールとチームの効率をさらに向上させます。

「DNS は、組織のセキュリティ体制を改善し、侵害を未然に防ぐためのプロアクティブなアプローチを取るだけでなく、侵害が発生した場合の修復までの時間を短縮するのに役立ちます。悪質な攻撃者は、AI を駆使してより巧妙な攻撃を仕掛けてきます。SOC Insights は、防御者が推測することなく攻撃者の一歩先を行くことを可能にする可能性を秘めています。」 と、Moor Insights & Strategy の副社長兼主席アナリスト、ウィル・タウンゼント（Will Townsend） 氏は述べています。「膨大な量の DNS クエリとネットワークデータに AI を適用することで、Infoblox はセキュリティチームにプロアクティブな脅威の阻止、インサイトに満ちた分析、インテリジェントなエコシステムの統合を提供することができます。」

SOC Insights により、マネージド・セキュリティ・サービス・プロバイダーは、顧客のセキュリティ体制の改善、セキュリティ投資の最適化、運用の合理化を支援することができます。また、IT チャネルパートナーは、Infoblox セキュリティエコシステムの他のソリューションを販売したり、アップリフトしたりする新たな機会を得ることができます。

「Infoblox の SOC Insights は、セキュリティオペレーションセンターが AI を活用して膨大な量のデータを正確で実用的なインテリジェンスに変換する方法の転換を象徴しています。」と、Futurum Group の副社長兼プラクティスリーダーであるスティーブン・ディケンズ（Steven Dickens） 氏は述べています。「独自の DNS インテリジェンスと AI 主導の分析を統合することで、SOC Insights は SecOps のワークフローを合理化するだけでなく、プロアクティブな脅威の検知と対応に新たな業界基準を設定し、セキュリティチームが高度化するサイバー脅威に先手を打てるようになります。」

SOC Insights と BloxOne Threat Defense 機能の詳細については、下記の URL をクリックするか、Infoblox の担当者にお問い合わせください。

詳細：https://www.infoblox.com/products/bloxone-threat-defense/　（英語）

Infoblox について

Infoblox はネットワークとセキュリティを統合し、比類のないパフォーマンスと保護を提供します。フォーチュン 100 の企業や新興のイノベーターに信頼され、ネットワークに接続するユーザー、デバイスおよびその接続先をリアルタイムで可視化し制御することで、組織の迅速な稼動と脅威の早期防御を実現します。Infoblox.com をご覧いただくか、LinkedIn または Twitter でフォローしてください。

【本プレスリリースに関するお問合せ】

Infoblox 株式会社

〒107-0062 東京都港区南青山 2-26-37 VORT 外苑前Ⅰ 3 階

Infoblox: 岡田 琢央 SalesJapan@infoblox.com

PR エージェント: 佐藤 郁子 infoblox_pr@mlrev.co.jp