ソリューション ノート

SOC INSIGHTS

AI 主導の分析を適用して、膨大な量のイベント、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え、SecOps の効率を向上させます。

SECOPS の効率化を阻む障壁

今日の企業や政府組織の他の部署と同様に、現代の SOC は、利用可能なリソースでより多くのことを行うために奮闘しています。SANS 2023 SOC 調査[1] によると、SOC の能力のフル活用を阻む、SOC の障壁トップ 10 のうち 80% は、次の 3 つの分野に分類されています。

- アラートの理解とその対応
- ツール間での限定的な統合または自動化
- 利用可能なスタッフとスキルで重要なタスクを実行すること

しかし、最も本当に悲劇的な統計としては、これらすべての障壁がこの 10 年以上にわたって SOC を悩ませ続けているということかもしれません。マルウェアのランキングやその他の基本的なフィルターに基づいてインシデントの優先順位を単純に自動設定するという漸進的な改善は、SOC アナリストの注意を必要とする可能性のあるアラートやその他のイベントの増加に追いつくことができていません。そのため、事態は悪化の一途をたどっています。

AI を活用した SOC INSIGHTS

最新の持続的な脅威では、柔軟に対応する攻撃者のインフラストラクチャと動的な C2 システムに依存し、たとえ 1 回の攻撃であっても、侵入テスト、エクスプロイト、暗号化、その他のツールを多数ホストして展開します。これにより、DNS への依存度が非常に高くなり、防御者がこれらの脅威を検出して阻止するために利用できる重要な弱点が浮き彫りになります。

DNS は、プロトコル、プラットフォーム、OS、アプリケーション、さらには場所に関係なく、正当な活動と悪意のある活動を監視します。この独自の可視性により、NSA のサイバーセキュリティ局長の下で行われたパイロットプログラムでは、DNS を保護することでマルウェア攻撃を 92% 削減できることが明らかになりました[2]!

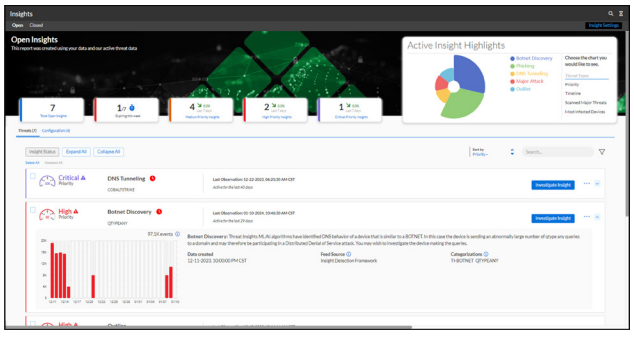

図 1：SOC Insights のサマリーページでは、アナリストは 1 クリックで最も重要な情報にアクセスできます。

事実と数字

- SOC アナリストの 60% は**仕事量が増えている**と答え、65% は今後 1 年間に**転職する可能性がある**と回答しています[4]。
- 調査回答者の 55% が、**重要なアラート**が毎週、あるいは毎日見落とされていることが多いと回答しています[5]。
- アナリストの 64%が、**手作業が自分の勤務時間の半分以上を占めている**と回答しています[6]。
- 構成ミスは、**エラーに関連する違反の上位 3 つの要因**の 1 つです[3]。
- **SOC のフル活用を阻む障壁**トップ 10 のうち 8 つが、アラート、ツール統合、スキル不足に関係しています[1]。
- 77%の CEO が**主要スキルの確保**に不安を抱いています[7]。
- 適切な DNS インテリジェンスと可視性があれば、**マルウェアと C2 活動の 92% を DNS レイヤーで制御できます**[2]。

SOC Insights は、Infoblox の DNS Detection & Response（DNSDR）、BloxOne Threat Defense と連携し、独自のソリューションを提供します。AI 主導の分析により、他のツールが見逃す未知の脅威アクティビティを検出し、SOC の効率を高め、現在のセキュリティ投資への全般的な投資利益率を向上させます。

さまざまなインサイトで複数の問題を解決

インシデントや侵害後の調査では、構成ミス、セキュリティツールの統合の問題、または単純なアラートの過負荷により、悪意のある活動の初期の兆候が見逃されていたことが判明することがよくあります。SOC Insights は、膨大な量のデータに AI 主導の分析を適用して、これらのリスクに対処します。

Security Insights

SOC Insights のセキュリティアドオンは、BloxOne Threat Defense の「Business Cloud」または「Advanced」で利用可能で、AI を使用して、膨大な量のイベント、ネットワーク、エコシステム、DNS の可視性とインテリジェンスを、実行可能なセキュリティインサイトにまとめて管理できるように抽出します。

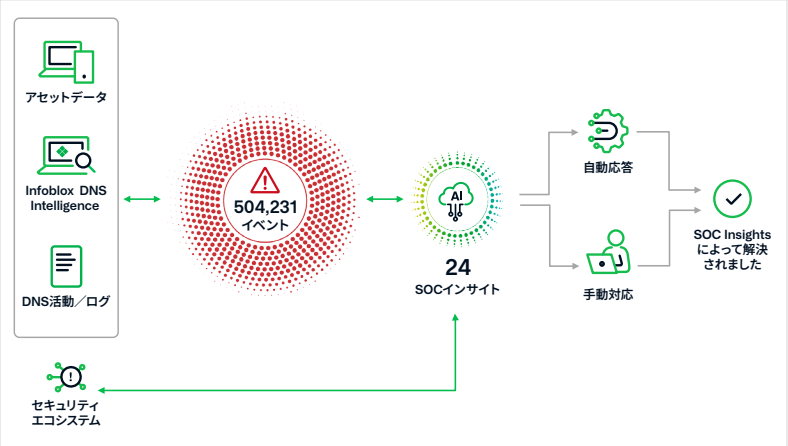

図 2：*SOC Insights* によってアラートの過負荷が解消され、山ほどのイベントがより管理しやすい有意義で実行可能なインサイトとして抽出されます。

- Zero Day DNS™
- 持続的な脅威
- 活発に脅威が拡散中
- 深刻な攻撃
- ボットネットの検出
- 通常とは異なる通信
- フィッシング
- マルウェア
- オープン DNS リゾルバー
- DNS トンネリング
- データ損失活動
- 標的型攻撃
- 過剰な DNS エラー
- 監視対象の類似ドメイン

Configuration Insights

SOC Insights の Configuration Insights 機能は、BloxOne Threat Defense の「Business Cloud」と「Advanced」に標準で含まれています。これにより、ユーザーは現在のベストプラクティスを最大限に活用し、よくあるミスを回避できます。動画やその他のガイドに従って、間違いや弱点に対処したり、許可されている例外に対する不要な警告を無効にしたりしてください。

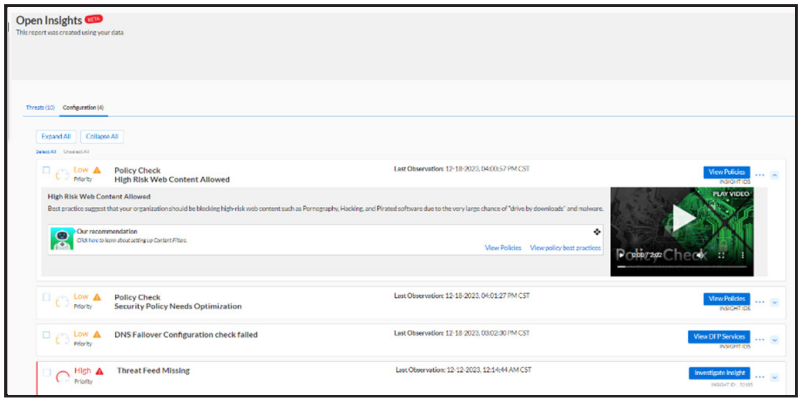

図 3：脆弱または危険な構成エラーを事前に特定し、最適に防御、調査、対応できるようにします。

- DNS 脅威フィードがありません
- VirusTotal Free Key がありません
- 最適化するにはセキュリティポリシーが必要です
- DNS フェイルオーバーチェックが失敗しました
- フィードアクションが一致しません
- DFP 非表示アセットの詳細
- ログモードでのセキュリティポリシー
- Web コンテンツフィルターがオフです
- 高リスクの Web コンテンツが許可されました

財務、運用、ビジネスにプラスの影響

ほとんどのセキュリティツールは、「使いやすさ」と「侵害の減少」くらいしか約束できませんが、SOC Insights では、アナリストのストレスや離職率を軽減することから、事業拡大、M&A、その他のビジネスの取り組みから生じる多くのセキュリティ懸念の軽減に至るまで、もっと多くのことことが可能になります。次がそのいくつかの例です。

- DNS の性質により、新しい拠点やビジネスパートナーを共通の DNS インフラストラクチャに数か月ではなく数分で簡単に統合できます。
- 構成インサイトは、エラー関連の侵害で報告された上位 3 つの要因の 1 つである「構成ミス」による侵害やデータ損失を軽減するために、先回りしたインサイトを提供します [3]。
- 「マルウェア」、「フィッシング」、「ボットネット」、その他の「重大な」または「拡散的」活動を自動的に相関付けるため、対応者が多くの脅威に一度に対処できるようになり、効率が向上します。
- 「異常値」、「DNS トンネリング」、「オープンリゾルバー」などのインサイトのカテゴリーを監視する機能や、BloxOne Threat Defense 独自の類似機能やアプリケーション可視化機能も備えた、より先回りしたセキュリティ体制に移行します。
- セキュリティエコシステムのインテリジェンス統合により、単なる未加工のログやイベントではなく実効性のある「インサイト」が提供されるため、セキュリティスタック全体の投資利益率が向上します。
- SOC Insights が関連データを自動収集し、アナリストはそのデータを確認し、そのデータを中心に分析して、より早く、そして自信を持って結論に達することができるようになります。これにより、アナリストのストレスが軽減され、熟練した経験豊富なセキュリティ専門家の定着率を向上させます。

驚くべき成果

お客様から報告された、BloxOne Threat Defense を使用した SOC Insights の主なメリットは以下の通りです：

- EDR と FW のアラートを 50% 削減
- 1 か月あたり平均 500 時間の SOC アナリストの時間を短縮
- 生産性向上により年間 40 万米ドルのコスト節減を達成

SIEM、SOAR、エコシステムのその他の領域がインサイトで向上

SecOps は、セキュリティエコシステム全体で未加工のデータを共有することの価値と限界を理解しています。そのため、SIEM と SOAR の専門知識は、ほとんどの組織にとって最も困難なスキルセットの 1 つとなっています。SOC Insights は、これらの他のツールの負担を軽減し、セキュリティスタック全体で得られたインサイトを共有して、他のツールをより効果的にし、SecOps 全体の効率をさらに向上させることができます。

1 “SANS 2023 SOC Survey”、2023 年 6 月、Chris Crowley、Barbara Filkins、John Pescatore 著

2 “NSA launches pilot program to secure defense contractors”、2020 年 6 月 18 日、Lauren C. Williams、NEXTGOV/FCW

3 “Verizon 2023 DBIR Report”

4 Voice of the SOC Analyst

5 The Orca Security 2022 Cloud Security Alert Fatigue Report

6 Voice of the SOC Analyst

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

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 : 20250226v2