ソリューションノート

THREAT INTELLIGENCE DATA EXCHANGE（TIDE）

Threat intelligence 管理と自動化で SecOps の効率性を向上

セキュリティの有効性は、多様で正確な THREAT INTELLIGENCE（TI）に依存

数十年にわたり、世界最大手で最高のセキュリティを誇る企業のほとんどは、常に進化する脅威の状況から組織を守るために十分な threat intelligence を単一のベンダーでは提供できないという判断から、「マルチベンダー」によるセキュリティ体制を採用してきました。ですので、少なくとも 1 社のベンダーが、サイバーキルチェーン全域で攻撃の一部を検出するために必要な threat intelligence を持っていることを期待して、複数のベンダーによる複数のソリューションを介して攻撃を強制するように防御を調整していることでしょう。

近年、調査により、ベンダー、オープンソース、コミュニティ、その他のソースからの脅威フィードで重複がほとんどないことが明らかにされ、このアプローチの価値が検証され、強調されました。ある調査では、2 社のセキュリティベンダーが提供した threat intelligence データを比較したところ、重複しているのはわずか 11% で、各ベンダーのデータの 89% が独自のものであることがわかりました。

その結果、組織が全体的なセキュリティ投資を最大限に活用できるように、threat intelligence の最適な組み合わせを求める動きが生まれました。残念ながら、この取り組みにより、SecOps では、入手可能な数十のソースからさまざまな種類の threat intelligence を特定、収集、正規化、配布し、各セキュリティツールに適切な threat intelligence を組み合わせて提供するという負担が増えています。さらに、ある程度の成功感を得るために、API、スクリプト、マクロに関連する商用ツールと自社開発ツールを組み合わせることに悪戦苦闘しています。

INFOBLOX TIDE が THREAT INTELLIGENCE の最適化への取り組みを効率化

Infoblox BloxOne Threat Defense Advanced は、TIDE（Threat Intelligence Data Exchange）と呼ばれる、threat intelligence の収集と管理を効率化する機能を提供します。BloxOne Threat Defense に搭載の最大 30 個の脅威フィードに加えて、TIDE は他のソースから threat intelligence を取り込み、その threat intelligence をセキュリティスタック全体にどのように配布するかを制御し、各ツールを最大限に効果的にする機能を提供します。

事実と数字

2021 年の SANS サイバーセキュリティインテリジェンス（CTI）調査結果：

- **回答者の 3 分の 2 は**CTI 情報をメールや文書で配布することに苦労していると回答
- 回答者の半数以上が**スタッフ、スキル、または資金の不足**を CTI の効果を阻害する要因として回答
- SANS の調査作成者は、**CTI の効率性とスケールをサポートするためには自動化が必要**

TIDE の主なメリット：

- 複数のソースからリアルタイムで厳選された threat intelligence を単一のオープンで柔軟なプラットフォームで収集し、管理
- 300 を超える個別の脅威分類領域のコンテキストを活用し、迅速な脅威の調査と対応を支援
- 簡単に共有できる threat intelligence を活用して、SecOps の効率とセキュリティスタック全体の有効性を向上
- DNS レイヤーで高度に回避的な脅威活動を監視し、制御（それと同じ threat intelligence は BloxOne によって適用）
- バックドア、C2 通信、データトンネリング、DNS 経由のデータ漏洩などのリスクを明らかにする Threat Defense

Infoblox の TIDE は、Infoblox BloxOne Threat Defense などのセキュリティシステムやサイバーセキュリティエコシステム全体を、新しい脅威や進化する脅威に対してリアルタイムで更新するように設計されています。Infoblox が提供する 30 種類の異なる threat intelligence ソースに加え、政府や業界からのソース、オープンソース、独自の社内 TI データセットなど、市販されているあらゆる threat intelligence ソースも組み合わせて利用できます。自動化機能と多様なファイル形式のサポートにより、TIDE は、ファイアウォール、SIEM、SWG、SOAR、脆弱性スキャナーなど、エコシステム内のさまざまなツールに適切な threat intelligence の組み合わせて、お客様が収集および配布できるよう支援します。

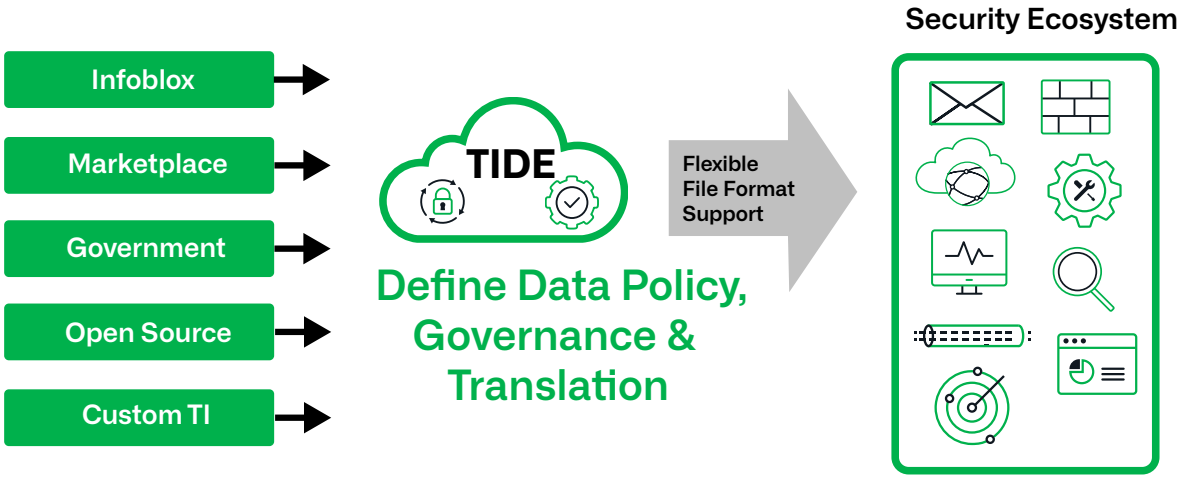

図 1：*TIDE* はセキュリティエコシステム全体での *threat intelligence* の交換を促進し、防御を強化し、レポートを改善します。

BLOXONE THREAT DEFENSE の多くの価値ある機能の一つ

TIDE は BloxOne Threat Defense を構成するいくつかの機能の 1 つです。BloxOne Threat Defense は、最新のマルウェア、ランサムウェア、C&C 通信、データ漏えい、その他の高度な脅威から、DNS を防御の第一線として使用するクラウドネイティブなセキュリティソリューションです。脅威調査を迅速に行い、脅威に対して迅速かつ確実に対応できるようにするなど、セキュリティスタック全体を強化し、SecOps がより効率的に作業できるような機能が含まれています。これは、現代のハイブリッド環境において、BYOD や IOT/OT を含むネットワーク上のすべてのデバイスをあらゆる場所で全域にわたりセキュリティを提供する業界初のセキュリティソリューションです。

脅威のハンティング、調査、対応を最適化

BloxOne Threat Defense Advanced には、アナリストが Dossier と呼ばれる単一のビュー内で threat intelligence の全容にアクセスし、活用できる別の機能が用意されています。Dossier は、脅威の重大度、WHOIS データ、MITRE ATT&CK ガイダンス、ファイルサンプル、関連する IP/URL/ ドメイン、脅威アクターの背景、活動のタイムラインなどにオンデマンドでアクセスを提供します。これにより、アナリストはデータと自分の経験に従って必要な場所に方向転換できるようになり、自信を持ってより迅速に結論を出すことができます。

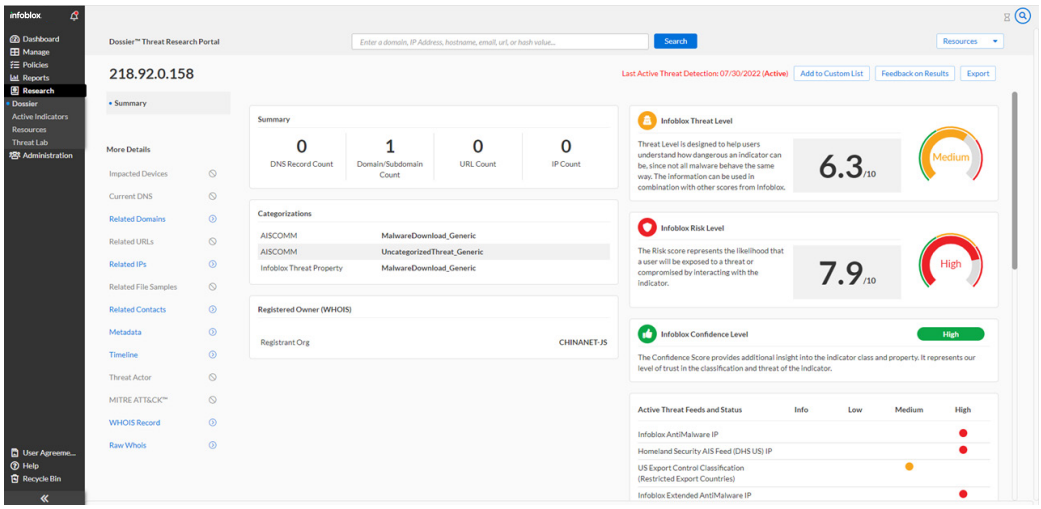

図 2：オンデマンドでドリルダウンおよびピボットできる *Dossier* ダッシュボード。

即時に利用可能な統合：サードパーティの脅威フィード

BloxOne Threat Defense の TIDE 機能は、ほぼすべての threat intelligence フィードとの統合プロセスを簡素化および自動化し、ほぼすべてのセキュリティツールに配置できますが、Infoblox と協力しているパートナーの一部では、顧客のオンボーディングプロセスのサポートを提供しています。

以下のパートナーは、TIDE 機能について即時でサポートを提供しています。

CrowdStrike：CrowdStrike は次世代のエンドポイント保護、threat intelligence、サービスを提供する大手プロバイダーです。CrowdStrike Falcon のホスト名と IP インテリジェンスにより、標的型攻撃による被害を防ぎ、高度なマルウェアや敵対的な活動をリアルタイムで検出して特定し、すべてのエンドポイントを簡単に検索できるため、全体的なインシデント対応時間を短縮できます。お客様は CrowdStrike から直接 CrowdStrike フィードを購入する必要がありますが、Infoblox では TIDE プラットフォームでフィードを簡単に「オン」にできます。

FireEye iSIGHT Threat Intelligence：IP およびホスト名のサイバー脅威インテリジェンスにより、企業は世界規模の専門家チームによって導き出された戦略的、運用的、戦術的な分析を活用できます。ThreatScape サブスクリプションは、セキュリティプログラムをビジネスリスク管理の目標に整合させ、新たなサイバー脅威や出現しつつあるサイバー脅威に対して能動的に防御するために必要なインテリジェンスを提供します。お客様は iSight フィードを FireEye から直接購入する必要がありますが、Infoblox では TIDE プラットフォームでフィードを簡単に「オン」にできます。

さらに、BloxOne Threat Defense Advanced のサブスクリプションの登録者は、次のサードパーティベンダーのフィード（追加のサブスクリプションが必要）を RPZ 形式で（追加費用なしで）活用し、DNS コントロールプレーンでの脅威の守備範囲を拡大できます。

Farsight Security の新しく観測されたドメイン（NOD）フィード：このフィードは、新しく開始されたドメインで発生または終了するマルウェアの引き出し、ブランドの悪用、およびスパムベースの攻撃に対抗するための、防御の増分レイヤーを提供します。

Proofpoint Emerging Threats（ET）IP and Domain Reputation Feed：このフィードは、Proofpoint の ET ラボによる脅威アクターの行動観察および直接的な観察に基づいてスコア化された、実用的な IP とドメインレピュテーションエントリを提供します。世界最大級のアクティブなマルウェア交換、大規模な被害者エミュレーション、独自の検出技術、グローバルなセンサーネットワークを活用した独自のプロセスに基づいて構築された Proofpoint の ETインテリジェンスは、リアルタイムで更新され、今日の新たな脅威に対処するための実用的なインテリジェンスを組織に提供します。

Infoblox はネットワークとセキュリティを統合して、比類の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：20231030v1