ソリューションノート

DNS DETECTION AND RESPONSE（DNSDR）によるセキュリティ有効性の変革

XDR フレームワークの一部として DNS を使用するプロアクティブなアプローチ

急速に進化する脅威の状況

サイバー脅威の状況は常に変化しており、脅威は前例のないペースで進化し続けています。デジタルトランスフォーメーション（DX）が様々な業界に浸透するにつれ、企業は拡大し続ける攻撃対象領域に悩まされるようになっています。この拡大は、クラウドが持つ無限の領域から、相互に接続されたハイブリッドな労働環境にまで及び、急成長している IoT 環境にまで広がります。新しいタッチポイントが出現するたびに、悪意のある行為者が悪用する新たな経路が生まれます。

DNS は、サイバー攻撃の一部である一連のイベント（「攻撃チェーン」と呼ばれることが多い）において、重要な役割を果たします。サイバー攻撃者は、展開する悪意のあるソフトウェア（マルウェア）とともに、ネットワーク通信における重要な機能を持つ DNS を悪用し、ドメインシャドウイングやファストフラックスなどの危険な手法を使用して悪意のあるドメインを隠し、セキュリティ担当者に気付かれずに陰湿な攻撃を仕掛けます。非常に巧みな類似ドメインを使用したスミッシングや、DNS ビーコンを利用して C2 を確立する持続的な低プロファイルのインフラストラクチャ・マルウェアなどの戦術や手法は、今日の最新のセキュリティ戦略による検出を簡単に逃れることができます。

類似ドメインを取り入れたスミッシングや、低プロファイル・インフラストラクチャのマルウェアが既存の防御を回避しています

平均して、毎日 20 万の新しいドメインが作成されています

現在、 ファイル拡張子（ZIP、MOV） に似たトップレベルドメインが使用されており、エンドユーザーに混乱を招いています

研究者は、6 か月ごとに約 8,000 万のドメインを悪質なドメインとしてフラグ付けしています。

デジタルイニシアチブは問題を悪化させます。

- マルチクラウドの導入は急ピッチで加速しており、調査対象企業の 73% 超が[1]クラウドプラットフォームを導入。
- IoT の導入は増加しており、2030 年までに 2 倍に。
- AI は主流になりつつあり、悪意のあるアクターは AI を使用して高度な攻撃を迅速に設計、拡張、配布しています。

DNS の事実と数字

> セキュアな *DNS* を使用することで、コマンドアンドコントロールの観点から、特定のネットワークへのマルウェア展開を含むマルウェア攻撃の 92% を抑制できます。"

Anne Neuberger、
サイバーセキュリティ担当役員会
取締役
国家安全保障局（NSA）

1 20/20 Visibility Clarifies Network Security, Forrester, June 2022

このように攻撃対象領域が拡大すると、ネットワークに誰と何が接続されているかを可視化して制御するセキュリティチームの負担が増大します。従来のセキュリティソリューションはネットワークの一部にのみ焦点を当てているため、セキュリティチームは脅威を探し出して滞在時間を最小限に抑えるという、非常に困難な課題に直面しています。

DNS はリスク軽減において最前線であり、中心的な存在です

独自の視点による戦略的ソリューション

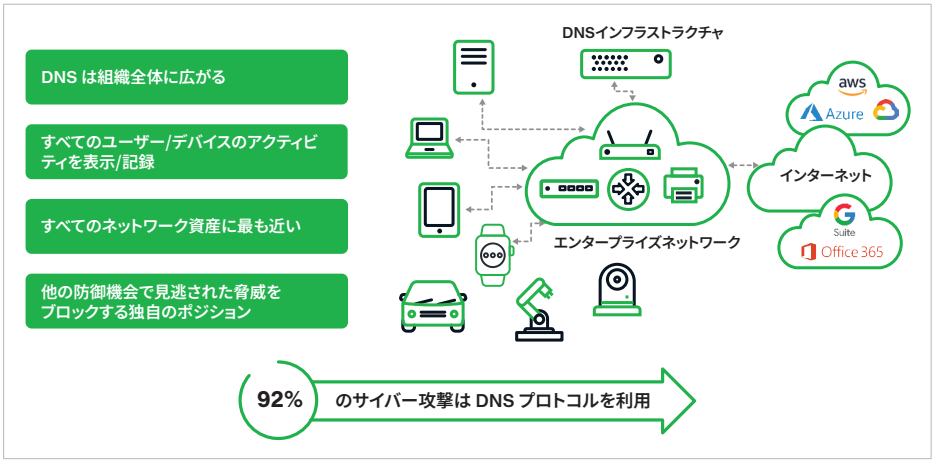

図 1: *DNS* はリスク軽減において最前線であり、中心的存在

サイバーセキュリティの状況は常に進化しており、時代遅れの戦略に頼ると、機密情報の盗難、評判やブランドの信用失墜、経済的損失につながる可能性があります。組織は、脅威の動的な性質を認識し、リアルタイムの保護を中核とするプロアクティブなアプローチを採用する必要があります。ここで、DNSDR の出番です。

リアクティブからプロアクティブへ：DNSDR が持つメリットの活用

数十年にわたって、サイバーセキュリティの防御担当者は反応的でした。彼らは脅威への対応に多くの時間を費やし、パッチが適用される前に脆弱性を悪用した攻撃者への対処に追われていました。この事後対応型のアプローチにより、組織の脆弱性は永続化し、運や時代遅れのツールに依存していました。DNSDR は、見過ごされがちなドメイン名システムの戦場に明るいスポットライトを当てることで、脅威の検出に革命をもたらします。

DNSDR の機能は、情報技術（IT）、ネットワーク・オペレーション・センター（NOC）、セキュリティ・オペレーション・センター（SOC）の各チームが企業を防御するために使用する複合的な戦略へのパラダイム・シフトを形にしたものです。DNSDR を他のXDR（Extended Detection and Response）製品と組み合わせることで、深層防御戦略を強化し、エコシステム全体で対応を自動化することができます。DNSDR のメリットには、データ漏えい、それに伴う潜在的な経済的損失、ブランドへの損害のリスクを減らすことが含まれます。

現場で求められるのは迅速性

> 防御側は攻撃側の先手を取る必要があります。
>
> サイバーセキュリティの観点での目標は、攻撃者よりも迅速に意思決定プロセスを実行することです。つまり、サイバーセキュリティ担当者は、攻撃者が攻撃を開始する前に、彼らのインフラストラクチャを特定する必要があります。
>
> *Infoblox DNSDR の DNS 脅威インテリジェンス、デバイス/ユーザーコンテキスト、自動応答、およびエコシステムの統合は、XDR フレームワークを補完し、サイバー脅威に対応して打ち負かすために必要な、俊敏性と迅速な意思決定を可能にします。"*

Anthony James
プロダクトマーケティング部門副社長
Infoblox, Inc.

DNSDR の主な機能

DNSDR には、サイバー防御エコシステムの回復力と有効性を向上させ、価値を提供するのに役立つ、拡張された強力な機能がいくつか組み込まれています。

DNS DETECTION AND RESPONSE

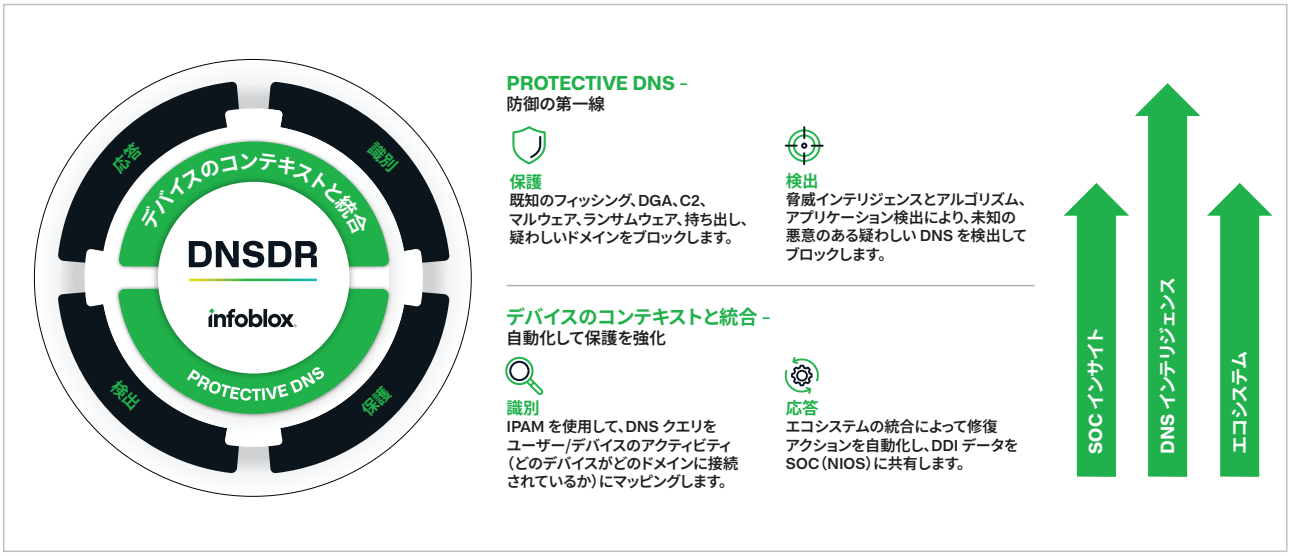

図 2：*INFOBLOX DNS Detection and Response*

DNSDR には、次の5つの基本的な側面があります。

1. **識別：**これにより、IP アドレス管理（IPAM）と DNS ベースのアプリケーション検出を使用して、DNS クエリがユーザーまたはデバイスのアクティビティにマッピングされます。これは、どのユーザーまたはデバイスがどの DNS クエリを実行しているかを特定することにより、ネットワークの全体像を理解するのに役立ちます。その利点は、セキュリティ運用チームが複数のログを経由することなく、ネットワーク内の侵害された資産を簡単に特定できるため、トリアージの迅速化と MTTR の短縮というメリットが得られることです。
2. **Protective DNS（PDNS）：**これは、フィッシング、ランサムウェア、マルウェアのコマンドアンドコントロール（C&C）、ドメイン生成アルゴリズム（DGA）、データの持ち出しなど、さまざまな種類のサイバー脅威をブロックするように設計されています。また、コンテンツフィルタリングと DNSSEC も含まれており、IoT デバイスや OT デバイスなど、あらゆる場所のシステムを保護します。Protective DNS の利点として、悪意のある活動がネットワークに影響を及ぼすのを防ぐ効果が期待できます。
3. **検出:** DNS Threat Intelligence と AI/ML のアルゴリズムを使用して、未知の悪意のある DNS アクティビティを検出してブロックします。高度な技術を使用して、従来のセキュリティ対策では見逃されがちな潜在的な脅威を特定できます。新たな脅威に対して、より強力で能動的な防御が可能になる点が利点です。
4. **対応：**これには、エコシステムの統合による自動修復が含まれます。DDI データを共有し、セキュリティオペレーションセンター（SOC）ツールでイベントへの自動応答をトリガーします。検出された脅威に対してより迅速かつ効果的に対応することで、キルチェーンの実行をより早く停止できる可能性があり、データ侵害のリスクと損害を減らすことができるという利点があります。
5. **DNS Threat Intelligence：**データサイエンス、DNS の専門知識、AI/ML 機能を統合した DNSDR は、**インフラストラクチャ中心の脅威インテリジェンスを使用して**、攻撃者のインフラストラクチャと脅威アクターを特定し、学習しながら追跡します。ドメインを「犯罪予防」モードでブロックする利点は、多くの攻撃を開始される前に阻止できることです。

XDR アーキテクチャ内の DNS

XDR は、エンドポイント、ネットワーク、クラウドなど、さまざまなプラットフォームにわたる制御と可視性を統合することで、セキュリティの効率を高めます。異なるセキュリティ・ソリューションのデータを統合することで、脅威の可視性を高め、脅威の特定と対応のプロセスを加速します。この合理的なアプローチは、攻撃対策に要する時間を短縮するだけでなく、全体的なセキュリティ態勢を強化します。

図 3：*XDR アーキテクチャ内の INFOBLOX DNS*

重要なメリットをもたらす DNSDR のユースケース

DNSDR は、その主要なユースケースを通じて、さまざまなドメインにわたって多数の利点を提供します。これは、機密データの損失、ブランドの評判の失墜、収益と業務の混乱につながる可能性のあるサイバー攻撃のリスクを軽減する上で重要な役割を果たします。DNSDR の中核的機能の 1 つは、DNS を利用したキルチェーンプロセスを迅速に検出して中断し、潜在的な損害を回避する機能です。さらに、DNSDR は、セキュリティオペレーションセンター（SOC）内で新しい脅威を検出、調査、理解するために必要な時間と費用を大幅に削減します。DNSDR のユースケースには、次のようなものがあります。

1. オンプレミス、クラウド、IoT/OT、リモートワーカー、ブランチを含む攻撃対象領域全体をカバーする**単一の企業全体のコントロールポイントとしての DNS**
2. Protective DNS 機能を使用して**既知の不正なトラフィックをブロック**し、脅威を早期に検出し、ダウンストリームのセキュリティデバイスの負荷を軽減
3. データの持ち出しと DGA を検出するためのストリーミング分析を使用して、**DNS の誤用を監視**

> *DNS の脅威のレビューと、より広範な XDR フレームワーク内でのそれらへの対応方法を計画することは、「もし（実行したら）」ではなく「いつ（実行するか）」という問題であるべきです。"*
>
> **HardenStanc**

> *ZK Research は、DNS セキュリティがあらゆるセキュリティ戦略の最もシンプルで効果的な出発点であると考えています。この分野のリーダーとして、Infoblox は、ネットワークとセキュリティを統合し、問題になる前にほとんどのマルウェアを阻止するための最優先候補となるはずです。"*
>
> **ZK Research**

4. **攻撃者のインフラストラクチャを特定し**、インフラストラクチャ中心の脅威インテリジェンスを使用して、犯行前に攻撃をブロック
5. **ユーザーとデバイスのアトリビューション**により、侵害されたデバイスの IP アドレスだけでなく、デバイスの種類、ユーザー名、ネットワークの場所、過去の IP なども提供
6. DNS データで**セキュリティツールを強化し**、イベントへの応答を自動的にトリガー
7. **デジタルブランド保護**により、類似ドメインを特定し、Domain Mitigation Service で問題のあるドメインを迅速に削除

詳細情報

Infoblox DNSDR 機能の詳細については、当社のウェブサイトをご覧ください。DNSDR について説明したアナリストレポートも[2,3]公開されています。

2 https://www.hardenstance.com/wp-content/uploads/2023/07/HardenStance-Briefing-Wheres-DNS-in-the-XDR-Roadmap-FINAL.pdf

3 https://insights.infoblox.com/resources-whitepaper/infoblox-whitepaper-transform-security-effectiveness-with-dns-detection-and-response

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: 20240118v1