SOPHOS

Sophos Network Detection and Response

Sophos NDR (Network Detection and Response) による セキュリティオペレーションの強化

ソフォス ホワイトペーパー 2023 年 4 月

はじめに

脅威環境が刻々と変化する現在、潜在的なサイバー攻撃を特定して対応するための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。このアプローチにおいて重要な役割を果たすのが、NDR (Network Detection and Response) テクノロジーです。

NDR テクノロジーは、ディープラーニングアナリティクス、従来型のルールベースマッチング、リスクベースのフロー統計を活用してネットワークトラフィックを分析し、ネットワークで攻撃が疑われるアクティビティや潜在的に悪意のあるアクティビティを特定します。これにより、セキュリティチームはサイバー攻撃を防止し、その影響を最小限に抑える予防措置を講じることができます。

一般的には、NDR テクノロジーの課題として、高い確率で誤検出が発生することが挙げられます。Sophos NDR は、複数の脅威検出エンジンから収集した証拠を組み合わせる特許取得済みのクラスタリングおよびスコアリングテクノロジーを活用することで、この問題に対処しています。

NDR テクノロジーの利用は 1990 年代から始まっていますが、その複雑さと精度はベンダーによってさまざまです。誤検出を最小限に抑えると同時に、高度な脅威検出機能を提供する Sophos NDR のような堅牢な NDR ソリューションを検討することが、組織のセキュリティを向上するために極めて重要です。本ホワイトペーパーでは、Sophos NDR の機能と利点を掘り下げ、あらゆる組織のセキュリティオペレーションの基盤として組み込むべき理由を説明します。

目次

はじめに 2
ネットワークセキュリティ監視の進化: NDR テクノロジーの年表 3
Sophos NDR: 最新の脅威に対する高度なネットワーク監視 4
Sophos NDR の主な利点: 4
NDR センサーの概念的なアーキテクチャ 5
ネットワークパケット処理 (NPP) 5
NPP: パケットヘッダーデータ 6
NPP: アプリケーション層のデータ 7
Sophos NDR の検出エンジン 8
IDS (侵入検知システム) エンジン 9
雑多なアクティビティ 9
ポリシー違反 9
悪意のある未知のトラフィック 9
マルウェアのダウンロード 9
トロイの木馬のアクティビティ 9
TLS ブラックリスト 9
SRA (セッションリスク分析) エンジン 10
DGA (ドメイン生成アルゴリズム) エンジン 12
DDE (データ検出エンジン) 12
CSS (クラスタリング/深刻度スコアリング) 13
付録 14
付録 A: SRA のフローリスク 14
付録 B: NPP プロトコル 17

ネットワークセキュリティ監視の進化：NDR テクノロジーの年表

Sophos NDR は今日のセキュリティオペレーションに欠かせない要素ですが、NDR の歴史はネットワーク型侵入検知システム (NIDS) が登場した 1990 年代にまでさかのぼります。初期の NIDS は、ネットワークベースの攻撃の特定とブロックに重点を置いていましたが、複数のイベントを相関させたり、複数のシステムにまたがる高度な脅威を検出する機能が欠けていました。

2000 年代初頭、NDR テクノロジーはこうした課題に対処するために進化しました。NDR ソリューションは、単にネットワークベースの攻撃を特定するのではなく、ネットワークトラフィックを分析し、複数のシステムのイベントを相関させて高度な脅威を特定できるようになりました。Sophos NDR は、ディープラーニングアナリティクス、従来型のルールベースマッチング、リスクベースのフロー統計を利用して、ネットワークで攻撃が疑われるアクティビティや潜在的に悪意のあるアクティビティを特定する、最先端の NDR ソリューションです。

時代とともに NDR テクノロジーはさらに高度化し、ネットワークアクティビティのほぼリアルタイムでの可視化と、他のセキュリティソリューションとのシームレスな統合が可能になりました。次の年表に、NDR テクノロジーの進化における主要なマイルストーンの概要を示します。

年	マイルストーン
1980 年代	ネットワークセキュリティ製品が登場し、ファイアウォールテクノロジーが広く採用されるようになる
1990 年代	ネットワーク型侵入検知システム (NIDS) が登場し、ネットワークセキュリティの監視が始まる
2000 年代	NDR (Network Detection and Response) テクノロジーが進化し、ネットワークトラフィックの分析と複数システムのイベントの相関付けが可能になる
2010 年代	高度な機械学習アルゴリズムが NDR ソリューションに統合され、複雑な脅威の識別が可能となり、誤検出が低減する
2016 年	IoT デバイスを悪用する Mirai ボットネットが最大級の DDoS (分散型サービス拒否) 攻撃を開始し、高度なネットワークセキュリティの必要性が浮き彫りになる
2019 年	Gartner が、それまでの「ネットワークトラフィック分析 (NTA)」に代わる、「Network Detection and Response (NDR)」という用語を提唱
2020 年代	NDR ソリューションが、リアルタイムの可視化と柔軟な展開オプションを提供し、あらゆる環境への導入が可能に

Sophos NDR などの NDR ソリューションを導入することで、高度な脅威の効果的な検出と対応が可能になります。

Sophos NDR: 最新の脅威に対する高度なネットワーク監視

Sophos NDR は、進化し続ける複雑な脅威環境に対応するために設計された、高度なネットワーク監視ソリューションです。

従来の NDR ソリューションとは異なり、複数のソフォス独自の検出エンジンとディープラーニングアナリティクスを組み合わせることで、さまざまなネットワーク脅威に関するリアルタイムで実用的なインテリジェンスを提供します。

Sophos NDR の検出エンジンは、330 以上のプロトコル、50 のフローリスク、数千の IOC (セキュリティ侵害の痕跡) に基づいてネットワークトラフィックを分類します。これらのエンジンには、複数のディープラーニングモデルによる予測も組み込まれているので、誤検出を最小限に抑えながら、これまでにない精度で脅威を検出します。

Sophos NDR の主な利点 :

従来の NDR	Sophos NDR	改善点
プロトコルの適用範囲が限定されている	330 以上のネットワークプロトコルに対応	Sophos NDR は、330 以上のプロトコルに基づいてトラフィックを分類するため、ネットワークトラフィックをより包括的に把握できます。これは、新たに出現した脅威を特定する上で極めて重要です。プロトコルのリストについては、付録 B を参照してください。
基本的な IOC	数千件の IOC	Sophos NDR は、何千もの IOC を利用してセキュリティ侵害の痕跡を検出するため、より高い精度で脅威を検出します。
最小限のフローリスク識別	50 のフローリスク	Sophos NDR 独自の検出エンジンには 50 のフローリスクが組み込まれており、他の NDR ソリューションでは検出できないような、複雑な脅威の検出が可能です。フローリスクのリストについては、付録 A を参照してください。
ルールベースのマッチング	ディープラーニングアナリティクス	Sophos NDR はディープラーニングアナリティクスを活用することで、誤検知を最小限に抑えながら、かつてない精度での脅威検出を実現します。
高い誤検出率	特許取得済みのクラスタリング / スコアリングテクノロジー	Sophos NDR は、特許取得済みのクラスタリング / スコアリングテクノロジーを使用して誤検出を削減し、さまざまなネットワーク脅威に関する実用的なインテリジェンスを提供します。

これらの改善は特に NDR に関連するものであり、Sophos NDR は誤検出を過剰に発生させることなく、ネットワークの脅威を正確に識別して対応できます。Sophos NDR は、スピード、正確性、およびトラフィックの復号化を実行せずに暗号を処理する機能に重点を置いていることから、包括的なセキュリティ戦略にとって不可欠な要素となっています。

Sophos NDR は、進化し続ける脅威を効果的に検出して対応するように設計された、高度なネットワーク監視ソリューションです。Sophos NDR は、複数の独自の検出エンジンとディープラーニングアナリティクスを組み合わせることで、正確かつ最新の脅威に対応した実用的なインテリジェンスを提供します。

NDR センサーの概念的なアーキテクチャ

Sophos NDR ソリューションは、SPAN/ ミラーポートをリスンするパッシブなトラフィックモニターとして展開され、ネットワークトラフィックに遅延を発生させることも、過負荷やオフラインの場合にネットワークに障害点を生じさせることもありません。

データがセンサーを通過すると、メタデータが収集され、ネットワークフローの詳細データが検出エンジンに送信されます。その後、送信されたデータはクラスター化され、スコア化されます。クラスター化されたネットワークフローの結果は、Sophos Data Lake に送信され、Sophos Central の検出ダッシュボードに表示されます。

ネットワークパケット処理 (NPP)

NDR ソリューションが適切に機能するには、ネットワークフローのメタデータを効果的に収集することが極めて重要です。このプロセスでは、ネットワークパケットが 1 つの通信またはフローに集約され、ディープパケットインスペクション (DPI) を使用して各ネットワークパケットからメタデータが収集されます。収集したメタデータは、地理的な位置情報や、通常とは異なる宛先、周期性、パケットダイナミクスなどの指標により強化されます。最終段階では、不正な TLS 情報、単方向トラフィック、大きな DNS パケットなどのリスク指標が検出されます。

次の表では、この段階で収集されるパケットヘッダーとアプリケーション層のデータの意味を深く理解できるように、各カテゴリーからどのような結論を導き出せるのか、また、それらが脅威ハンティングにとってなぜ重要であるのかを示します。

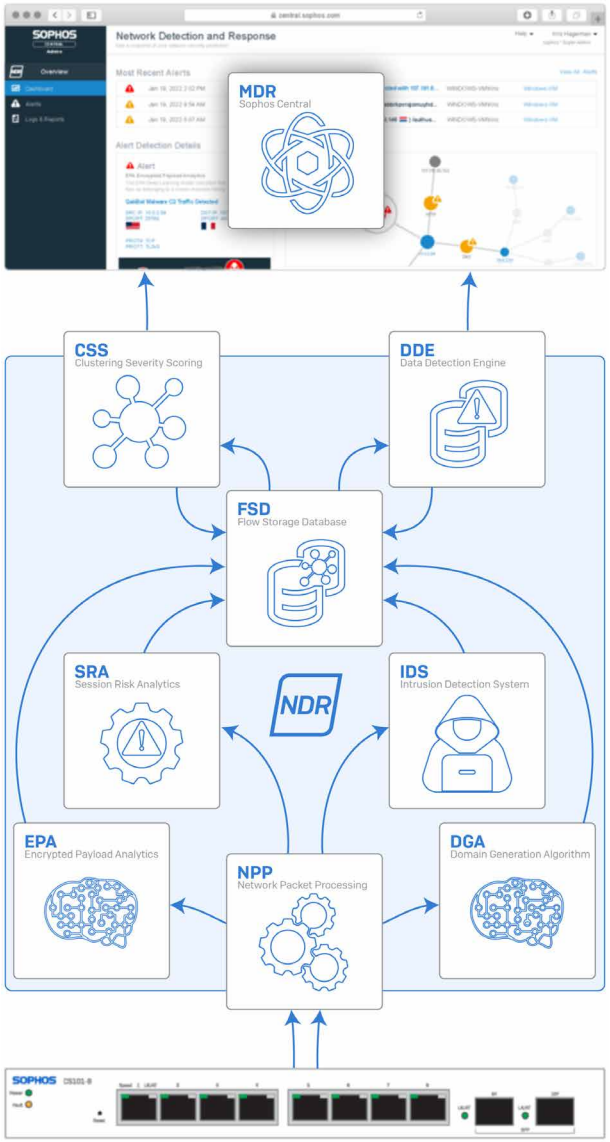

図 1: Sophos NDR のアーキテクチャ図

NPP: パケットヘッダーデータ

パケットヘッダーデータには、送信元アドレス、宛先アドレス、トランスポートプロトコル、期間、サイズなど、ネットワーク通信に関する情報が含まれています。この情報は、NDR ソリューションが通信の送信元を明らかにし、そこからもたらされる可能性のある脅威を特定するのに役立ちます。パケットヘッダーデータから判断できる情報には、以下のようなものがあります。

パケットヘッダーデータ	説明	NDR 脅威ハンティングにおける重要性
送信元 IP	送信者の IP アドレス	通信の発信元を識別し、不審なアクティビティの追跡や感染したホストの特定に利用できます。
送信元 MAC アドレス	送信者の MAC (Media Access Control) アドレス	MAC アドレスは、ネットワークトラフィックに関連する物理デバイスの識別に使用されます。また、他のセンサー情報と組み合わせることで、複数のセンサーからのアラートを特定のデバイスに関連付けることができます。
送信元ポート	送信者が通信に使用するポート	通信に関連する特定のサービスやアプリケーションを識別するのに役立ち、不審なアクティビティや不正なアクティビティの検出に利用できます。
宛先 IP	受信者の IP アドレス	通信のターゲットを識別するのに役立ち、外部からの脅威の発生源の特定に利用できます。
宛先 MAC アドレス	受信者の MAC アドレス	通信に関連している物理デバイスの識別に役立ち、不審なアクティビティの追跡や感染したホストの特定に利用できます。
宛先ポート	受信者が通信に使用するポート	通信に関連する特定のサービスやアプリケーションを識別するのに役立ち、不審なアクティビティや不正なアクティビティの検出に利用できます。
TCP フラグ	SYN、ACK、FIN、RST など、TCP 接続のステータスを示します。	不審なネットワークアクティビティや攻撃 (ポートスキャン攻撃、DoS 攻撃など) の検出に使用できます。
通信の継続時間	通信が継続した時間	予想以上に長い接続、異常に短い接続、ビーコンに関連する定期的な通信など、不審なアクティビティを特定するのに役立ちます。
受信バイト数	通信中に受信したデータ量	データの窃取やマルウェアのダウンロードなど、不審なアクティビティや攻撃の検出に利用できます。
レイヤー 3 (ネットワーク) とレイヤー 4 (トランスポート) のプロトコル	IP、OSPF、ICMP、TCP、UDP など、通信に使用されるプロトコル	トラフィックの種類や関連サービスの特定に役立ち、不審または不正なアクティビティの検出に利用できます。
ネットワーク VLAN (仮想ローカルエリアネットワーク) ID	通信に関連する VLAN タグ	通信に関連する特定のネットワークセグメントを識別するのに役立ちます。

NPP: アプリケーション層のデータ

アプリケーション層のデータからは、ネットワーク通信の内容に関する情報を得られるため、NDR ソリューションはその中に隠れている潜在的脅威を特定できます。ネットワーク通信で使用されているアプリケーションやサービスに関する情報が提供され、平文のユーザー名やパスワードの特定に役立ちます。アプリケーション層のデータから判断できる情報には、以下のようなものがあります。

アプリケーション層のデータ	詳細	NDR 脅威ハンティングにおける重要性
アプリケーション層プロトコル	HTTP、TLS、SMB (Server Message Block) など、アプリケーション層で使用されているプロトコル	使用されているアプリケーション層のプロトコルを把握しておくことで、悪意のあるトラフィックやプロトコルの異常な動作を特定できます。
送信元ホスト名と宛先ホスト名	送信元と宛先の IP アドレスに関連するホスト名を、DNS などで解決したもの	ホストやドメインに関連する悪意のあるトラフィックや異常な動作を特定するのに役立ちます。
HTTP コンテンツタイプ	テキスト、画像、動画など、HTTP で転送されるコンテンツの種類	コンテンツの種類に関連する悪意のあるトラフィックや異常な動作を特定するのに役立ちます。
レスポンスコード	HTTP リクエストに応答してサーバーが返す HTTP ステータスコード	「404 Not Found」や「500 Internal Server Error」など、特定のレスポンスコードに関連する悪意のあるトラフィックや異常な動作を特定するのに役立ちます。
URL	リクエストされた、またはアクセスされた完全な URL	URL やドメインに関連する悪意のあるトラフィックや異常な動作を特定するのに役立ちます。
ユーザーエージェント	Web ブラウザやモバイルアプリなど、クライアントがリクエストを行う際に使用するソフトウェアエージェント	悪意のあるトラフィックや、ユーザーエージェントに関連する異常な動作 (既知の悪意のあるソフトウェアに関連するもの、など) を特定するのに役立ちます。
平文のユーザー名とパスワード	暗号化されていない HTTP リクエストなど、平文で送信されるユーザー名やパスワード	これは、潜在的なセキュリティ上の問題や不正なアクセスの試みを特定するのに役立ちます。
TLS 証明書情報	セキュアな接続で使用される TLS 証明書に関する情報 (JA3 ハッシュを含む)	これは、悪意のある証明書や偽装証明書の特定に役立つだけでなく、暗号化されたトラフィックに関する情報を提供します。
SSH クライアントとサーバーの HASSH	SSH クライアントとサーバーを識別するためのフィンガープリント手法	悪意のある SSH トラフィックの特定や、不正な SSH アクセス試行の検出に役立ちます。
CAPWAP カプセル化	ワイヤレスアクセスポイントの管理に使用される CAPWAP (Control and Provisioning of Wireless Access Points) プロトコル	悪意のある、または不正なワイヤレスアクセスの試行、または異常なワイヤレスネットワークのアクティビティを特定するのに役立ちます。

結論として、ネットワーク通信に関する情報を提供し、潜在的な脅威の検出を可能にするネットワークフローのメタデータを収集することは、NDR ソリューションにとって不可欠な要素です。収集されたパケットヘッダーとアプリケーション層のデータは、通信の送信元、種類、および潜在的リスクを特定するのに役立つ重要な情報を提供します。NDR ソリューションはこの情報を活用することで、ネットワーク脅威の効果的な検出と対応が可能になります。

Sophos NDR の検出エンジン

Sophos NDR には特徴の異なる 5 つの検出エンジンが組み込まれており、脅威を包括的に検出できます。これらの検出エンジンが連携してさまざまな IOC (セキュリティ侵害の痕跡) を特定し、相関付けます。その後、顧客やアナリスト向けにスコアリングされ、実用的な脅威インテリジェンスとして Sophos Central に表示されます。

パフォーマンスを向上させるため、機械学習の検出エンジン (EPA：暗号化パケット分析、DGA: ドメイン生成アルゴリズム) はすべてのネットワークフローでは実行されず、他の検出エンジンによる発見に基づいてトリガーされるようになっています。検出エンジンが連携して分類できるようにするのは、パフォーマンスを維持し、誤検出を減らす上で重要です。

検出エンジンの結果は、CSS (クラスタリング / 深刻度スコアリング) アルゴリズムに入力され、総合的な脅威スコアが生成されます。生成されたスコアは、管理者向けの検出結果として Sophos Central の検出ダッシュボードに表示されます。検出記録には、各エンジンの貢献の結果が含まれます。

IDS (侵入検知システム) エンジン

この独自の IDS エンジンは、暗号化されていないトラフィックに含まれる IOC (セキュリティ侵害の痕跡) を識別する機能を備えた、合理的で効率化されたエンジンです。多くのセキュリティベンダーは今なお、暗号化によって可視性が失われているにもかかわらず、過度に堅牢なコンテンツマッチングシステムを使用しています。

Sophos NDR は厳選された脅威インテリジェンスを使用し、IOC のタイプに基づいて 6 つのグループに分類される IDS ルールを作成します。そのルール分類とその説明は、次の通りです。

雑多なアクティビティ

このルール分類は、深刻度が「低」で、他の分類と関連のないネットワークトラフィックを検出するために使用されます。たとえば、パブリック DNS サーバーへのトラフィック、コンテンツ配信ネットワークへのトラフィック、信頼できるクラウドサービスへのトラフィックなどがこれに該当します。雑多なアクティビティを特定することで、正常なネットワークトラフィックのベースラインを確立し、そのベースラインから逸脱したものを明確にできます。

ポリシー違反

このルール分類は、深刻度が「低」で、企業ポリシーに違反する可能性のあるトラフィックを検出するために使用されます。たとえば、不正な Web サイトやサービスへのトラフィック、不正なデバイスからのトラフィックなどがこれに該当します。ポリシー違反を検出した場合には、セキュリティポリシーを強制し、不正アクセスやデータ窃取を防止できます。

悪意のある未知のトラフィック

このルール分類は、深刻度が「中」で、不正な宛先とのネットワーク通信を特定するために使用されます。たとえば、既知の悪意のある IP アドレスやドメインとの通信、悪意のあるインフラストラクチャにトラフィックをリダイレクトするために使用されるシンクホールドメインとの通信などです。悪意のある未知のトラフィックを検出することで、セキュリティ侵害を受けたエンドポイントを特定し、データ窃取やさらなる攻撃を防止することができます。

マルウェアのダウンロード

このルール分類は、深刻度が「高」で、既知のマルウェア配信元とのネットワーク通信を特定するために使用されます。これには、マルウェアのダウンロードや配信に使用される既知の C2 (C&C) サーバーとの通信や、既知のマルウェア配信サイトとの通信も含まれます。マルウェアのダウンロードを検出することで、感染したエンドポイントを特定・隔離し、マルウェアのさらなる拡散を防止できます。

トロイの木馬のアクティビティ

このルール分類は、深刻度が「高」で、既知のマルウェア C2 サーバーとのネットワーク通信を特定するために使用されます。これには、セキュリティ侵害を受けたエンドポイントをリモートからコントロールするために使用される C2 サーバーとの通信や、データの窃取に使用される C2 サーバーとの通信が含まれます。トロイの木馬のアクティビティを検出することで、セキュリティ侵害を受けたエンドポイントを特定して隔離し、データ窃取やさらなる攻撃を防止できます。

TLS ブラックリスト

このルール分類は、深刻度が「重大」で、TLS 認証の一致に基づき、既知の攻撃者とのネットワーク通信を特定するために使用されます。TLS ブラックリストには、侵害された TLS 証明書を使用する既知の不正ドメインとの通信や、有効な TLS 証明書を使用していない既知の不正ドメインとの通信が含まれます。TLS ブラックリストに登録されているトラフィックを検出することで、既知の悪意のあるインフラとの通信を阻止し、サイバー攻撃から保護することができます。

SRA (セッションリスク分析) エンジン

SRA エンジンは、文書化されたプロトコル標準から逸脱しているネットワークトラフィックを検出します。このようなトラフィックは、不審な、または危険なネットワークアクティビティが存在していることを示します。これは、攻撃が疑われる非標準的な動作を特定するのに役立つため、脅威ハンティングにおいて重要です。SRA エンジンはこのような動作を確認すると、その動作に関する情報をフローメタデータに追加します。これらのフローリスクは、単独では IOC とはみなされませんが、他のエンジンによる検出結果と組み合わせることで、悪意のあるアクティビティの特定が可能になります。

複数のプロトコルで見られる一般的なフローリスクとその意味を、以下の表に示します。

タイプ	フローリスク	説明
一般	エクスプロイトの可能性	Log4J/Log4Shell などのエクスプロイトの可能性が検出されたことを示します。エクスプロイトアクティビティの検出や攻撃を防止 / 軽減する上で重要です。
一般	非標準ポート上の既知のプロトコル	標準の TCP/80 ではなく、TCP/8000 の HTTP のように、プロトコルが標準以外のポートで使用されていることを示します。非標準ポートを使用し、検出を迂回する攻撃者を検出する上で重要です。
一般	リスクの高い ASN	危険とされる ASN (自律システム番号) に属するサーバーとネットワークトラフィックが交換されたことを示します。悪意のあるホストやネットワークを特定するために重要です。
一般	単方向トラフィック	セッションが一方向のみであることを示します。これは、そのアドレスで現在は動作していないサーバーに対する C2 アクティビティが存在している可能性があることを意味します。侵害を受けたホストまたは C2 サーバーを特定するために重要です。
一般	デスクトップまたはファイル共有セッション	TeamViewer や AnyDesk など、デスクトップまたはファイル共有データを送信するフローであることを示します。これらのツールを使用して、侵害されたホストをリモートで制御する攻撃者を検出する上で重要です。
一般	安全でないプロトコル	SSH の代わりに Telnet を使用するなど、使用されているプロトコルが安全ではなく、使用すべきでないことを示します。安全でないプロトコルで送信されたトラフィックを傍受して読み取ることができる攻撃者を検出する上で重要です。
一般	平文の認証情報	FTP、HTTP、IMAP、POP3、SMTP など、既知のプロトコルで平文の認証情報が送信されたことを示します。平文の認証情報を傍受して読み取ることができる攻撃者を検出する上で重要です。
一般	パケットの改ざん	パケットの形式が予期していなかったものであることを示します。これは、プロトコルエラーが発生したか、別の種類のデータを送信する目的で有効なプロトコルが乗っ取られた可能性を示しています。パケット操作やプロトコルの不正使用を用いた攻撃を検出する上で重要です。
一般	TCP の問題	ネットワークセッションの TCP 設定で問題が検出されたことを示します。TCP の問題を悪用して検出を妨害 / 迂回する攻撃者を検出する上で重要です。
一般	定期的なフロー	ネットワークセッションが設定された間隔で繰り返されていることを示しており、トロイの木馬やボットネットからの C2 アクティビティの可能性があります。侵入したホストを制御し続けることを目的に、定期的な通信を使用する攻撃者を検出する上で重要です。

すべてのフローリスクの一覧については、付録 A を参照してください。

EPA (暗号化ペイロード分析) エンジンと機械学習 (ML)

機械学習は、企業ネットワーク上の不審なトラフィックを検出する NDR (Network Detection and Response) ソリューションでの活用が広がっています。NDR ソリューションは、生のトラフィックやフローの記録 (NetFlow など) を継続的に分析し、正常なネットワークの挙動を反映したモデルを構築する、と Gartner は説明しています。ディープラーニングは、複数の属性にまたがるパターンを検出することでこのアプローチをさらに前進させ、IOC ベースの脅威インテリジェンスなしでの検出を可能にします。

ソフォスは、暗号化されたトラフィックの脅威を旧来のテクノロジーで検出するという課題を解決するため、EPA (暗号化ペイロード分析) というソリューションを開発しました。ネットワークフローは、ヘッダーとペイロードデータを含んだパケットで構成されており、暗号化された通信を検査する場合、ペイロードデータのみが暗号化されているため、内容を知るためには復号化する必要があります。EPA は、SPLIT (パケット長・到着間隔のシーケンス) に基づき、ネットワークフローのパターンを検出するように学習させられたマルチクラスのディープランニング予測モデルです。これらの SPLI T 属性は簡単に計算でき、分類のための CNN (畳み込みニューラルネットワーク) のトレーニングに使用されます。Sophos NDR は特許取得済みのプロセスを使用し、このデータを分類できるように正規化、変換、CNN への提供を行います。

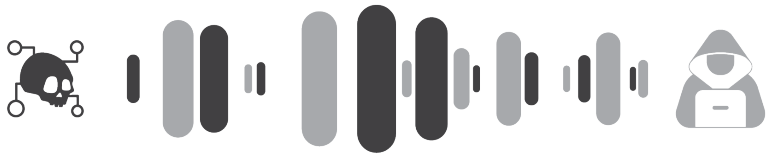

図 2: SPLIT (パケット長・到着間隔のシーケンス)

EPA モデルはマルウェアの実際の検体を使用することで、ゼロデイや未知のマルウェアの亜種や C2 サーバーなどの悪意のあるアクティビティを、それらの間のネットワークフローのパターンに基づいてリアルタイムで特定します。また、EPA エンジンは、検出されたマルウェアファミリと信頼度スコアを追加してフローメタデータを強化して、誤検出の件数を削減します。概して、EPA はこれまで検出されなかった暗号化された脅威を検出して対応することを可能にします。このアプローチの有効性が特に高まるのは、エンドポイントデバイスで従来のエンドポイント保護製品を実行できない場合や、個人情報保護の要件によりネットワーク通信を復号化すべきでない場合です。

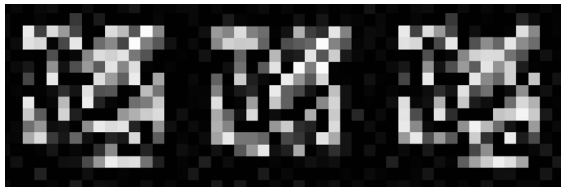

図 3: EPA CNN 用の画像として処理した後の Cobalt Strike の亜種

暗号化ペイロード分析 (EPA) エンジンは、特定のマルウェアファミリ (Bumblebee、Cobalt Strike、Emotet、Dridex、QakBot など) を識別してフローメタデータを強化し、0 ～ 100 の信頼度スコアを提供します。誤検出の数を減らすために、このモデルには「不明」という分類も含まれています。

DGA (ドメイン生成アルゴリズム) エンジン

攻撃者がドメイン生成アルゴリズム (DGA) を使用する目的は、ブラックリストに載ることなく、C2 (C&C) に使用できるドメイン名を生成することです。マルウェアはこれらのアルゴリズムを使用することで、C2 サーバーがホストされている可能性のあるドメイン名のリストを生成できます。DGA は試行錯誤を何度も繰り返して存在するドメインを見つけ、接続を確立します。

husbbrkpvrqjomuyhdpd[.]com

図 4: DGA ドメインの例

これまでにも DGA は、注目を集めた攻撃で使用されてきました。たとえば、2008 年に流行した Conficker ワームでは、DGA が使用され C2 サーバーとして使用可能な 5 万以上のドメイン名のリストが毎日生成されていました。そのため、セキュリティリサーチャーにとって、Conficker ワームの C2 ネットワークを停止させることは非常に困難でした。また、Gameover Zeus マルウェアでは、C2 として使用するために 1 日あたり最大 1,000 個のドメイン名を生成する目的で DGA が使用されました。Gameover Zeus ボットネットは、世界中の被害者から 1 億ドル以上を盗みました。

Sophos NDR の DGA 検出エンジンは、悪意のあるアクティビティをリアルタイムで特定するために不可欠です。このエンジンにはディープラーニングの長・短期記憶 (LSTM) ニューラルネットワークが搭載されており、クエリおよびアクセスされたすべてのドメイン名を評価します。ただし、すべての DGA アクティビティが悪意のあるものではなく、多くの正規サービスで DGA が使用されている点に留意してください。そのため、Sophos NDR は DGA が検出されるたびにアラートを生成するわけではありません。その代わりに、信頼度スコア (0 ～ 100) がフローメタデータに追加され、DGA の検出に関わるアクティビティが本当に悪意のあるものかどうかを判断するために、CSS (クラスタリング / 深刻度スコアリング) エンジンによって使用されます。

DDE (データ検出エンジン)

DDE (データ検出エンジン) は、各センサー上で実行される Sophos NDR のコンポーネントです。DDE は軽量の相関エンジンで、ネットワークフローやフロークラスターのオンボードデータベースストレージを利用します。スケジュール設定されたデータマイニングを、この情報に対して実行し、複雑なネットワーク脅威 (列挙するアクティビティなど) を特定します。この情報は Sophos Central に送信され、ネットワーク情報レポートの作成に使用されます。

さらに、DDE が収集したデータを Sophos XDR (Extended Detection and Response) エンドポイントセンサーのデータと相関させ、ネットワーク上の管理されていない資産を特定できます。この相関は Sophos Data Lake で行われ、ネットワークを包括的に可視化するため、管理者は潜在的なセキュリティリスクを特定し、適切な対策を講じることができます。重要なのは、DDE がリアルタイムではなく、設定されたスケジュールでデータマイニングを実行するという点です。

CSS (クラスタリング / 深刻度スコアリング)

CSS (クラスタリング / 深刻度スコアリング) は、Sophos NDR の脅威検出機能に不可欠な機能です。クライアントとサーバー間のネットワークセッション中に、さまざまな脅威指標を観測します。これらの指標は、単独で分析しただけでは問題や悪意のあるアクティビティを正確に示さない場合があります。そこで、Sophos NDR は、特許取得済みのプロセスを利用して指標を長期的にクラスタリングし、脅威の特定の信頼性を高めます。

このクラスタリングプロセスにより、基本的なネットワーク情報 (送信元と宛先の IP/ポートやプロトコル情報など) に基づいて、ネットワークフローをグループ化します。長期にわたって発生した複数のフローをクラスター化することで、不審なアクティビティをより包括的に表示し、関連するネットワークフローを 1 つの検出イベントに集約することができるため、フロー間の相関関係から不審なアクティビティに対する理解が深まります。

作成されたクラスターは、各検出エンジンから収集された情報に基づいてスコアリングされます。CSS アルゴリズムは、クラスター内のすべてのアクティビティを評価し、コンテキストを追加することで、精度を向上させ、誤検出を低減します。

CSS 内のスコアリングシステムは、さまざまな検出エンジンによって特定された深刻度レベルや脅威インジケーターなど、さまざまな要素に基づいています。Sophos NDR はこれらの情報を組み合わせることで、ネットワークアクティビティがもたらす潜在的なリスクを反映させたスコアを各クラスターに割り当てます。このスコアリングシステムにより、ネットワーク管理者は潜在的な脅威に関する重要情報を取得できるため、リスクの深刻度に基づいて対応の優先順位を決定することができます。

付録

付録 A: SRA のフローリスク

プロトコル	フローリスク	説明
全般	エクスプロイトの可能性	エクスプロイトの可能性が検出された (Log4J/Log4Shell など)
全般	非標準ポート上の既知のプロトコル	プロトコルが標準以外のポートで使用されている (TCP/8000 で HTTP を使用する、など。標準は TCP/80)
全般	リスクの高い ASN	リスクのある ASN (自律システム番号) に属するサーバーと、ネットワークセッションが交換された
全般	単方向トラフィック	セッションは一方向のみ。これは、そのアドレスで現在は動作していないサーバーに対する C2 アクティビティが存在している可能性がある。
全般	デスクトップまたはファイル共有セッション	デスクトップまたはファイル共有データを送信するフロー (TeamViewer、AnyDesk など)
全般	安全でないプロトコル	使用されているプロトコルが安全ではなく、使用すべきでない (SSH の代わりに Telnet が使用されている、など)
全般	平文の認証情報	既知のプロトコルで平文の認証情報が送信された (FTP、HTTP、IMAP、POP3、SMTP など)
全般	パケットの改ざん	ネットワークパケットの形式が予期していなかったものだった。これは、プロトコルエラーが発生したか、別の種類のデータを送信する目的で有効なプロトコルが乗っ取られた可能性を示している。
全般	TCP の問題	ネットワークセッションの TCP 設定で問題が検出された。
全般	匿名のサブスクライバー	送信元 IP アドレスが匿名化されており、サブスクライバーの特定に使用できない (iCloud-private-relay の出口ノードで生成されるフロー、など)
全般	定期的なフロー	ネットワークセッションが設定された間隔で繰り返されている。トロイの木馬やボットネットからの C2 アクティビティの可能性がある
TLS、HTTP、DNS	不審な DGA ドメイン	ドメイン名が DGA であっても、DGA はマルウェアが好んで使用するドメイン名を生成するために使われる
TLS、HTTP、DNS	リスクのあるドメイン	危険とされるドメインでネットワークトラフィックが発生した
TLS、HTTP、DNS	無効な文字	デコードされたプロトコルに、そのプロトコルフィールドで許可されていない文字が含まれている (たとえば、DNS ホスト名に含めることができるのは、すべての印刷可能文字のサブセットのみ)
TLS、HTTP、DNS	Punycode IDN	ドメイン名が IDN 形式で確認された。Punycode IDN ドメインは、ホモグラフを悪用したフィッシング攻撃の可能性がある
HTTP、DNS	エラーコード検出	プロトコルでエラーが検出された
DNS	不審なトラフィック	予期しない、または廃止された DNS レコードタイプが観測された

プロトコル	フローリスク	説明
DNS	大きなパケット	DNS over UDP パケットがサイズ制限の 512 バイトを超えている。これは、DNS トンネリングまたはデータ窃取が行われている可能性を示している
DNS	フラグメント化	UDP DNS がフラグメント化された。これは、DNS トンネリングまたはデータ窃取が行われている可能性を示している
SSH	旧式のクライアントバージョンまたは暗号	SSH クライアントが、廃止されたプロトコルバージョン、または安全でない暗号を使用している
SSH	旧式のサーバーバージョンまたは暗号	SSH サーバーが、廃止されたプロトコルバージョン、または安全でない暗号を使用している
SMB	安全でないバージョン	SMB の安全でないバージョン (SMBv1 など) が確認された
ICMP	不審なエントロピー	ICMP パケットに不審なエントロピーが確認された。これは、ICMP を介してデータが窃取されている可能性があることを示している
TLS	自己署名証明書	自己署名証明書が使用された
TLS	悪意のある SHA1 証明書	観測対象の TLS 証明書が悪意のある証明書で発見された
TLS	証明書の不一致	TLS 証明書が、アクセス先のホスト名と一致しない
TLS	SNI が見つからない	アクセス先のサーバーの SNI が見つからない
TLS	不審な ESNI 使用	暗号化された SNI が確認された。ドメインフロンティング攻撃の可能性がある
TLS	HTTPS を送信していない	TLS フローが HTTPS の送信に使用されていなかった
TLS	悪意のある JA3 フィンガープリント	JA3 フィンガープリントが悪意のある JA3 ブラックリスト上で発見された
TLS	不審な拡張子	SNI 拡張子のドメイン名が印刷可能でなかった
TLS	一般的でない ALPN	TLS フローで一般的でない APLN 拡張が確認された (HTTP/1.1 など)
TLS	証明書の有効期限切れ	フローで使用されている TLS 証明書の有効期限が切れている
TLS	証明書の有効期限が迫っている	フローで使用されている TLS 証明書が期限切れ間近
TLS	証明書の有効期限が長すぎる	フローで使用している TLS 証明書の有効期限が 13 か月を超えている
TLS	廃止されたバージョン	TLS のバージョンが 1.1 よりも古い
TLS	脆弱な暗号	フローのセットアップで安全でない TLS 暗号が使用された
TLS	致命的なアラート	TLS プロトコルがフローで致命的なアラートを発生させた
HTTP	数値 IP ホスト	Web サーバーがホスト名ではなく、IP アドレスを使用してアクセスされた

プロトコル	フローリスク	説明
HTTP	不審な URL	アクセス URL が疑わしい (例 : http://127.0.0.1/msadc/..%255c../..%255c../winnt/system32/cmd.exe.)
HTTP	不審なヘッダー	HTTP ヘッダーに想定していない不審な項目が含まれている (例 : UUID、TLS バージョン、OS 名)
HTTP	不審なユーザーエージェント	ユーザーエージェント文字列に不審な文字や書式が含まれていた (例 : <?php something ?>)
HTTP	不審なコンテンツ	HTTP フローに、想定していない形式のコンテンツが含まれていた (例 : HTTP ヘッダーは、コンテンツが text/html であることを示しているが、コンテンツはバイナリデータであるため読むことができない)
HTTP	バイナリアプリケーションの転送	バイナリアプリケーションがダウンロードまたはアップロードされている。検出されたファイルには、Windows バイナリ、Linux 実行ファイル、Unix スクリプト、Android アプリが含まれている
HTTP	XSS の可能性がある URL	XSS (クロスサイトスクリプティング) 攻撃の可能性があることが確認された
HTTP	SQL インジェクションの可能性がある URL	SQL インジェクション攻撃の可能性がある
HTTP	RCE インジェクションの可能性がある URL	RCE (リモートコード実行) 攻撃の可能性がある
HTTP	クローラーボット	クローラー / ボット / ロボットが検出された
HTTP	旧式のサーバー	旧式の Apache または Nginx サーバーを使用したネットワークセッションが検出された

付録 B: NPP プロトコル

1KXUN	GIT	MICROSOFT_365	SPOTIFY
ACCUWEATHER	GITHUB	MICROSOFT_AZURE	SSDP
ACTIVISION	GITLAB	MINING	SSH
ADS_ANALYTICS_TRACK	GMAIL	MODBUS	STARCRAFT
ADULT_CONTENT	GNUTELLA	MONGODB	STEAM
AFP	GOOGLE	MPEGDASH	STUN
AJP	GOOGLE_CLASSROOM	MPEGTS	SYNCTHING
ALIBABA	GOOGLE_CLOUD	MQTT	SYSLOG
ALICLOUD	GOOGLE_DOCS	MS_ONE_DRIVE	TAILSCALE
AMAZON	GOOGLE_DRIVE	MS_OUTLOOK	TARGUS_GETDATA
AMAZON_ALEXA	GOOGLE_MAPS	MSSQL_TDS	TEAMSPEAK
AMAZON_AWS	GOOGLE_PLUS	MSTEAMS	TEAMVIEWER
AMAZON_VIDEO	GOOGLE_SERVICES	MUNIN	TELEGRAM
AMONG_US	GOTO	MYSQL	TELNET
AMQP	GTP	NATPMP	TENCENT
ANYDESK	GTP_C	NATS	TENCENTVIDEO
APPLE	GTP_PRIME	NEST_LOG_SINK	TEREDO
APPLE_ICLOUD	GTP_U	NETBIOS	TFTP
APPLE_ITUNES	GUILDWARS	NETFLIX	THREEMA
APPLE_PUSH	H323	NETFLOW	TIDAL
APPLE_SIRI	HALFLIFE2	NFS	TIKTOK
APPLESTORE	HANGOUT_DUO	NINTENDO	TINC
APPLETVPLUS	HBO	NOE	TIVOCONNECT
ARMAGETRON	HOTSPOT_SHIELD	NTOP	TLS
AVAST	HPVIRTGRP	NTP	TOCA_BOCA
AVAST_SECUREDNS	HSRP	OCS	TOR
BADOO	HTTP	OCSP	TPLINK_SHP

BGP	HTTP_CONNECT	OOKLA	TRUPHONE
BITTORRENT	HTTP_PROXY	OPENDNS	TUENTI
BJNP	HULU	OPENVPN	TUMBLR
BLOOMBERG	I3D	ORACLE	TUNEIN
CACHEFLY	IAX	PANDORA	TUNNELBEAR
CAPWAP	ICECAST	PASTEBIN	TUYA_LP
CASSANDRA	ICLOUD_PRIVATE_RELAY	PINTEREST	TVUPLAYER
CHECKMK	IEC60870	PLAYSTATION	TWITCH
CISCOVPN	IFLIX	PLAYSTORE	TWITTER
CITRIX	IHEARTRADIO	PLURALSIGHT	UBNTAC2
CLOUDFLARE	IMO	POSTGRES	UBUNTUONE
CLOUDFLARE_WARP	INSTAGRAM	PPSTREAM	ULTRASURF
CNN	IP_EGP	PPTP	USENET
COAP	IP_GRE	PSIPHON	VEVO
COLLECTD	IP_ICMP	QQ	VHUA
CORBA	IP_ICMPV6	QUIC	VIBER
CPHA	IP_IGMP	RADIUS	VIMEO
CRASHLYSTICS	IP_IP_IN_IP	RAKNET	VK
CROSSFIRE	IP_OSPF	RDP	VMWARE
CRYNET	IP_PGM	REDDIT	VNC
CSGO	IP_PIM	REDIS	VUDU
CYBERSECURITY	IP_SCTP	RIOTGAMES	VXLAN
DAILYMOTION	IP_VRRP	RPC	WARCRAFT3
DATASAVER	IPP	RSH	WAZE
DAZN	IPSEC	RSYNC	WEBEX
DEEZER	IRC	RTCP	WEBSOCKET
DHCP	JABBER	RTMP	WECHAT
DHCPV6	KAKAOTALK	RTP	WHATSAPP

DIAMETER	KAKAOTALK_VOICE	RTSP	WHATSAPP_CALL
DIRECTV	KERBEROS	RX	WHATSAPP_FILES
DISCORD	KISMET	S7COMM	WHOIS_DAS
DISNEYPLUS	KONTIKI	SALESFORCE	WIKIPEDIA
DNP3	LASTFM	SAP	WINDOWS_UPDATE
DNS	LDAP	SD_RTN	WIREGUARD
DNSCRYPT	LIKEE	SFLOW	WORLD_OF_KUNG_FU
DOFUS	LINE	SHOWTIME	WORLDOFWARCRAFT
DOH_DOT	LINE_CALL	SIGNAL	WSD
DRDA	LINKEDIN	SIGNAL_VOIP	XBOX
DROPBOX	LISP	SINA	XDMCP
DTLS	LIVESTREAM	SIP	XIAOMI
EAQ	LLMNR	SIRIUSXMRADIO	YAHOO
EBAY	LOTUS_NOTES	SKINNY	YANDEX
EDGECAST	MAIL_IMAP	SKYPE_TEAMS	YANDEX_CLOUD
EDONKEY	MAIL_IMAPS	SKYPE_TEAMS_CALL	YANDEX_DIRECT
ELASTICSEARCH	MAIL_POP	SLACK	YANDEX_DISK
ETHERNET_IP	MAIL_POPS	SMBV1	YANDEX_MAIL
FACEBOOK	MAIL_SMTP	SMBV23	YANDEX_MARKET
FACEBOOK_VOIP	MAIL_SMTPS	SMPP	YANDEX_METRIKA
FASTCGI	MAPLESTORY	SNAPCHAT	YANDEX_MUSIC
FIX	MDNS	SNAPCHAT_CALL	YOUTUBE
FORTICLIENT	MEGACO	SNMP	YOUTUBE_UPLOAD
FTP_CONTROL	MEMCACHED	SOAP	Z3950
FTP_DATA	MERAKI_CLOUD	SOCKS	ZABBIX
FTPS	MESSENGER	SOFTETHER	ZATTOO
FUZE	MGCP	SOMEIP	ZMQ
GENSHIN_IMPACT	MICROSOFT	SOUNDCLOUD	ZOOM

Sophos NDR の詳細については、sophos.com/ndr をご覧ください

2023-03-29 (WP-NP)

SOPHOS