DARKTRACE

EDRへの依存から レジリエンス構築へ

ネットワークとエンドポイント間のギャップを解消する

概要

EDRとXDRはセキュリティに不可欠なシステムですが、これらは現在のマルチドメイン型脅威のすべてを防御するように設計されてはいません。攻撃者はエンドポイント、ネットワーク、クラウドサービス、OT環境感の継ぎ目を狙います。これらはまさに、可視性が消失し、ポイントソリューションでは点と点を結びつけることができない部分です。

本書は組織のリジリエンス構築方法を再考するための情報を提供します。なぜエンドポイント中心型の防御だけでは現在の脅威についていくことができないのか、そして、エンドポイントプロセスデータをネットワークテレメトリーと統合することにより、脅威検知、調査、対応のためのより強固な基盤を構築する方法を解説します。その中で、エンドポイントツールをすり抜けた攻撃の例を取り上げ、これらのギャップがSOCチームにもたらす負担、そしてテレメトリーの統合による新たなアプローチについて説明します。

EDR/XDRは必要、しかし不完全

これらのツールはエンドポイントの保護に有効ですが、管理されていないデバイス、エージェントレスの環境、ネットワークベースの攻撃に対する可視性が欠けています。

テレメトリーの統合が調査のギャップを解消

ネットワークアクティビティとエンドポイントプロセスデータを組み合わせることにより、アナリストは一元的な視野を得ることができ、偽陽性の削減、トリアージの加速、より早期の脅威封じ込めにつながります。

レジリエンス構築には新たなSOC基盤が必要

自己学習型の、ネットワークの可視性に基づいた適応型プラットフォームは、アナリストの燃え尽きを防ぎ、MTTRを短縮し、複数の領域にわたってブラインドスポットを解消するのに必要なコンテキストと効率性を提供します。

EDRは必要であるものの不完全な理由

今日、ほとんどの企業はEDR（Endpoint Detection and Response）およびその進化系であるXDR（eXtended Detection and Response）に投資しています。

EDRはエンドポイント**専用に構築**されたものです。ホストレベルのプロセス、メモリ、ログを監視し、デバイスレベルでの封じ込めと修復を行うことができます。

XDR は EDR ベンダーにより生み出され、複数のセキュリティツールからのアラートを単一のプラットフォームで相関付けることにより、**スプロール問題を解決**しようとするものです。しかし実際には、ほとんどの XDR 製品はいまだに EDR 中心型です。可視性は外側に拡大されましたが、依然としてエンドポイントエージェントに基づいています。

組織の57%はNDR（Network Detection and Response）能力をXDRツールセットに追加しようと計画しています。

Gartner、2023

カバレッジのギャップ

検知がエンドポイントテレメトリーに基づいている場合、ネットワーク、管理されていないデバイス、クラウドワークロード、アイデンティティシステムなどにブラインドスポットが残ります。EDR 中心型の XDR は、水平移動や、OT などのエージェントレス環境内のアクティビティを識別することができず、重要なインフラがカバーされない状態で残ります。

断片的な対応

ほとんどの NDR ツールにはエンドポイントのコンテキストが欠けているため、アナリストは複数のコンソールを切り替えながら攻撃をつなぎ合わせる作業を強いられます。この手作業の工程は調査の遅れを招き、MTTR を長期化させ、エンドポイントとネットワークの間を移動する脅威は検知されないままです。

EDRが注目しているのは...

EDRは「既知の悪」に注目しています。つまりエンドポイント上のアクティビティが「既知」の条件や事前に定義されたルールやシグネチャに一致した場合にアラートを作成します。

EDRが理解しないのは...

EDRはホストにとって何が正常で何が異常かということは理解していません。既知の攻撃者の振る舞いに基づくルールに従います。既に知られている脅威に対してはこれで対応できますが、今までに出現したことのない脅威、あるいは正規のツールを悪用し隠れ蓑にした攻撃については、カバレッジの隙間が生じます。

その結果...

強力なエンドポイントカバレッジが存在しているにもかかわらず、ランサムウェア、データ抜き出し、多段階攻撃が成功する結果となります。EDRはホストのアクティビティを監視するには非常に効果的です。しかし、現代の攻撃者はエンドポイントに限定されることなく、領域間のつなぎ目を悪用します。そこでは可視性が消失しており、アナリストは点と点をつなぎ合わせることが困難となります。

問題の裏付け
EDR可視性の限界

エージェントキラーを使った EDR 回避

攻撃者は EDRKillShifter や EDRSilencer などのツールを使ってエンドポイントエージェントを無効化し、エンドポイント専用防御を瞬時に盲目にします。これらの戦術は、エージェントベースのセキュリティがどれほど洗練されていても、攻撃者が簡単に無効化できることを示しています。

CISA のレッドチーム演習

CISA が米国の重要インフラの評価を行ったところ、EDR への過剰な依存によりネットワークレイヤーに致命的なギャップが残されていることがわかりました。敵対者はホストベースのアラートをトリガーすることなく何か月もの間永続性を維持し、エンドポイントだけの可視性では不十分であることが証明されました。

ネットワークレイヤー内のゼロデイエクスプロイト

2024 年に発生した Ivanti Connect Secure エクスプロイトでは、脆弱性が公開される前に、ネットワークテレメトリーから異常が検知され、エンドポイントツールからは見えない、認証情報の不正使用と C2 アクティビティが確認されています。NDR はこの脅威を早期に封じ込めるのに必要な可視性を提供していました。

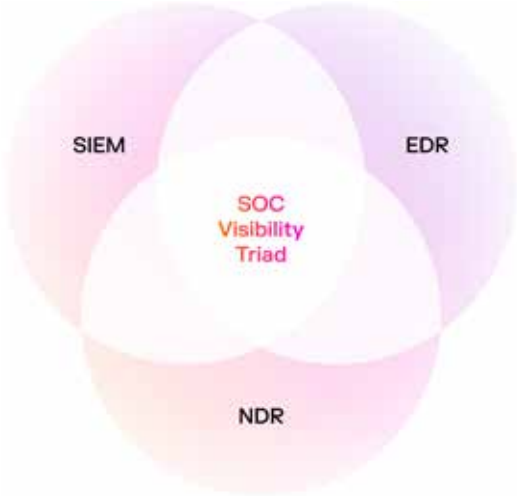
防御のレジリエンスを構築するには

EDRはエンドポイントセキュリティの基本ですが、適応力を備えた総合的なセキュリティアーキテクチャの一部となるためには、完全なネットワーク可視性との連携が必要です。XDRソリューションはカバーする範囲が広いものの、ホストベースの監視に大きく依存しており、ネイティブなネットワーク可視性が欠けていることがしばしばです。

エンドポイント、ネットワーク、クラウド、OT、アイデンティティにわたる一元的可視性

管理されているアセット、されていないアセット両方からの統合されたテレメトリー

通常の動作を理解し未知の動作を検知する適応型システム



EDR回避
Ivanti CS/PSアプライアンスの エクスプロイト後のアクティビティ

攻撃事例

このIvantiキャンペーンでは攻撃者はエンドポイント可視性の限界を知っていました。攻撃者は管理されていないネットワークアセットをエクスプロイトし、水平移動し、暗号化されたトラフィックに隠れました。しかし防御する側にとって本当の問題は検知だけではありません。問題はすべてを解明しなければならないSOCチームにのしかかります。

未知の外部 IP への初期ビーコニングが観測される。エンドポイントエージェントはここには関与していません。侵入された Ivanti アプライアンスはネットワークアセットであり、従来型のエンドポイントではないからです。ネットワーク可視性によってのみ、この最初の異常が明らかになりました。

別の未知のホストへの二次ビーコニングが検知される。攻撃者はネットワークレイヤーを通じて足掛かりを拡大しました。エージェントのカバレッジがないため、EDR ツールには相関付けを行う対象がなかったはずです。

OAST サービスを使ったエクスプロイト検証アクティビティが見つかる。攻撃者は帯域外チャネルを使ってエクスプロイトを確認しました。これらのチェックはエンドポイントスタックには接触しておらず、このことはネットワークテレメトリーの重要性を裏付けています。

外部サーバーに対する .dat/.sys ファイルの大規模な POST 転送によりホストデータの抜き出しが判明。 機密性の高いシステムファイルがネットワーク経由で抜き出されました。ホストプロセスを監視していたエンドポイントツールからはこのアウトバウンドトラフィックは見えませんでした。

AWS S3 エンドポイントから悪意ある Rust ELF ペイロードが投下される。ペイロード投下はクラウドサービスを使って行われました。別の場所で EDR が存在していても、これらのインプラントはネットワークエッジを通じて侵入することによりホストベースの防御を回避しています。

Web シェルおよび JavaScript スティーラーが展開され認証情報が収集される。 認証情報の盗み出しはユーザーエンドポイントではなくネットワークアプライアンスのコンテキストで展開されました。これは、アイデンティティ侵害が EDR の視界の範囲外で発生していることを意味します。

環境内でネットワークスキャンおよび水平移動が観測される。管理されていないアセットが攻撃者によりトラバースされる典型的な例です。EDR はこれらのデバイスを計測することができず、NDR がなければアナリストは何も見ることができません。

暗号化されたコマンド & コントロールトラフィックが DNS を介して転送され、その後クリプトマイニングツールが投下される。隠れたネットワークチャネルが永続化につながりました。エンドポイントベースの監視では暗号化された DNS の不正使用を正しく検知できません - これにはネットワークレイヤーでの異常検知が必要となります。

ネットワークテレメトリーはこれらの異常を脆弱性が公開される何日も前から示していた。これらの事象はシグネチャやエンドポイントログからではなく、ネットワークトラフィックの動作の異常から検知されました。このことは、マルチドメインのカバレッジがなぜ必要なのかを示しています。

SOCが直面する限界点
ブラインドスポット、疲弊、ビジネスリスク

可視性の制限

攻撃者中心型の検知手法では新手の脅威を検知することが困難です。なぜならば、これらは静的なルールや過去の攻撃データに依存し、「既知の悪」を識別することに集中しているからです。これらのツールは、一見正常に見える次のような悪意あるアクティビティをしばしば見逃してしまいます：

- 環境寄生型 （LotL）攻撃
- 有効な認証情報の不正使用
- 内部関係者からの脅威
- 承認済みのサードパーティアプリケーション

複雑化 = より多くの問題

OT環境ではほとんどのベンダーがアセットの可視性またはルールに基づいた検知に依存しており、攻撃者がどのようにITからOTに移動し、露出したCVEをエクスプロイトし、あるいはセグメンテーションの設定ミスを通じてクリティカルなオペレーションを中断することができるかについてはモデル化していません。

真のIT/OT統合モデリングを行わなければ、防御者はサイロ化したビューと不完全な脅威カバレッジで対応しなければなりません。

解決策
テレメトリー統合によるレジリエンス構築

これらの課題を解決するには、最も低レベルなエンドポイントプロセスデータとネットワークテレメトリーを単一のストリームに統合することが必要です。これらのデータソースを収集点で融合することにより次が実現できます：

より迅速な調査
エンドポイントプロセスデータとネットワークアクティビティを統合することで分析を加速することができます。

インシデントに対する一元的ビュー
複数のツールからの断片情報をつなぎ合わせる作業が不要、プロセスのアクティビティと水平移動を一元的なビューから追跡できます。

成果の改善
偽陽性の削減、トリアージサイクルの短縮、封じ込めの強化が可能です。

重要なことは、この能力が EDR や XDR に対する投資を**置き換えるものではなく**、それらを補強するということです。エンドポイント防御は引き続きセキュリティの基盤として重要ですが、ネットワークレベルの情報と組み合わせることにより、カバレッジを管理されていないデバイスや、クラウドワークロード、暗号化されたトラフィックにも拡大することができます。

その結果、エンドポイント中心の可視性に制限されることのない、最新の脅威の現実に即したセキュリティスタックが実現されます。

SOC の基盤を再考する

細切れの防御から一歩先へ進むためには、SOC 全体を支える基盤が必要です。その基盤となるのはネットワークです。あらゆるエンドポイント、クラウドワークロード、OT デバイス、そしてアイデンティティは、最終的にはネットワークトラフィックにその痕跡を残します。ネットワークを " ホームベース” と位置付けることにより、他のすべてのドメインを理解することのできる共通のレンズを得ることができます。

この基盤は、どの組織に対しても同じではありません。すべての組織には固有のデジタルエステートがあり、異なるクラウドサービスの組み合わせ、レガシーインフラ、リモートエンドポイント、そして OT 環境が存在しています。静的な、あらかじめ定義済みの検知では、新手の攻撃経路や構成のドリフトをすべて予期することはできません。必要なのは、適応力です。それは、組織の環境の通常のパターンを学習し、環境とともに進化し、異常の発生に応じてそれらを特定できるシステムです。

ネットワーク可視性を基盤として構築される、一元的プラットフォームは次のようなきわめて重要な利点をもたらします：

適応力：継続的な自己学習を通じ、環境や脅威が変化しても適応することができます。

効率性：複数のドメインに渡って検知と対応を一元化することにより、ベンダースプロールを抑えることができます。

レジリエンス：テレメトリーをリアルタイムに相関付け、雑音を排除し、重要なインシデントを明らかにします。

Darktraceを選ぶ理由

Darktraceは、組織のネットワーク全体を理解し、過去の攻撃データに依存することなくインテリジェントに異常を検知し高度な脅威を封じ込める、Self-Learning AI ™により、NDR分野のリーダーとして業界で高く評価されています。

最先端の教師なし機械学習に基づいたこのアプローチにより、Darktraceは、従来のツールでは見逃されてしまう、他のベンダーでは検知できない新手の脅威、未知の脅威、そして内部関係者による脅威をキャッチすることができます。

今や攻撃はEメール、クラウド、OT、SaaS、そしてエンドポイントにも拡大していることから、Darktraceはこのアプローチを大きく一歩先へ進め、これらのドメインのテレメトリーとコンテキストを統合し、AI駆動の調査を大規模に適用しています。Darktraceはプロセスレベルのエンドポイントデータをネットワークに対する可視性と組み合わせることにより、セキュリティチームが攻撃ライフサイクル全体を確認できるようにし、また自律的にアクションを実行することにより、ブラインドスポット、調査時間、アナリストへの負荷を削減します。

“Darktraceは単なるテクノロジーではありません。当社のシステムとサイバーセキュリティ環境全体に対して **スマートな拡大を可能にし支援しつつ信頼を構築していく** ためのツールです。

■ **CIO**
行政サービス

詳しく読む

Darktrace / ENDPOINTソリューション概要

ソリューション概要をダウンロード ↗

デモを予約

Darktraceがお客様の環境で何を発見できるか実際にご確認ください

デモを予約する ↗