EDR 選定ガイド

EDR（Endpoint Detection and Response）プラットフォームは、皆さんのセキュリティチームが、お使いのネットワーク内に潜んでいる最も見つけにくい危険な脅威を検知する能力を向上させます。ただし、すべての EDR プラットフォームが等しく作成されているわけではありません。EDR プラットフォームを評価する場合、可視性のレベル、調査や応答の有効性、展開のしやすさ、環境への影響、サーバーの強度を含む、さまざまな機能を評価する必要があります。

環境に対する深い可視性がキルチェーンのあらゆる段階での攻撃検知を可能にします

EDR プラットフォームは、任意の与えられた時点で何が起こっているかに関して深い可視性を提供するために、IT 環境全体を通じて重要な情報を収集する必要があります。EDR プラットフォームは、次の機能を含んでいる必要があります。

- ファイルレス型のマルウェアやラテラルムーブメントなどの、最先端の流行している脅威を自動的に検知する機能。
- 統計分析や行動分析を使用することで、容易に判定可能なシグネチャを持たない脅威を見分ける機能。
- 使用されているオペレーティングシステムにかかわらず、複数のエンドポイント間で疑わしいアクティビティ同士を相互に関連付ける機能。
- 短命のプロセスを補足するために継続して稼働できる機能。これにより、可視性の格差をなくすことができ、スナップショットは不要となります。
- メモリベースおよびファイルベースのアクティビティを監視する機能。

効果的な調査と応答が SOC チームを英雄にします

EDR プラットフォームは、SOC（Security Operations Center）チームが、効率的に脅威を探し出し、かつ素早く攻撃に対応できるようにする必要があります。EDR プラットフォームは、次の機能を含んでいる必要があります。

- お使いの環境を各自のためにプロアクティブに監視する機能。
- アラートを各自向けに優先順位付けする一方で、あらゆる疑わしい行動に関して完全な可視性を提供し続ける機能。
- 検知した脅威を完全に調査しそれらに対応するためのコンテキストと機能を備えたレベル 1 およびレベル 2 のアナリストを、プロセスの強制停止、ファイルの隔離、持続メカニズムの削除、エンドポイントの分離、実行可能ファイルのブロックなどの機能を含む修復ツールの完全なスイートと共に提供すること。
- レベル 3 のアナリストが、最も見つけにくい攻撃に関する詳細を調べることができるようにする機能。
- 疑わしいユーザー、マシン、ネットワーク接続に関連付けられている疑わしいアクティビティを自動的に特定し収集する機能。
- 検知、調査、修復、再侵入（re-infiltration）からなるライフサイクル全体をサポートする機能。
- 手動調査に関して SOC アナリストをガイドする機能。

容易な展開により、短期間で大きな価値を取得することが可能となります

理想的な EDR プラットフォームは、運用開始が容易で、かつ IT 組織内の同僚から容易に受け入れられる必要があります。また、同ソリューションはお客様の管理の負担を軽減する必要があります。

同ソリューションは、次の機能を含んでいる必要があります。

- エンドポイントの運用を中断せず、他のプログラムやオペレーティングシステムにも影響を与えないセンサーを備えていること。EDR センサーは、展開およびサポートが容易なものであることが必要です。
- 数万から数十万台のエンドポイントを、スケーラブルでコスト効率の良い方法で素早く展開できること。
- 設定いらずで、直ちに動作できること。既存の行動モデルを使用して、個々のお客様の環境のユニークな特性に対応できること。
- 監視やインシデント対応のようなサポートサービス（ただし、外部向けではなく、プラットフォームそれ自身により使用されるように設計されたもの）を提供すること。

影響の少ないセンサーによりユーザーに与える影響を最小化します

理想的な EDR プラットフォームは、エンドポイントに対して、ユーザーや展開の方法論に与える影響が最小またはゼロである必要があります。また、エンドポイントセンサーは、ユーザーの機能停止を引き起こすリスクを最小化するだけでなく、運用開始前の統合試験要件を最小化する必要もあります。同ソリューションは、次の機能を持つエンドポイントセンサーを使用する必要があります。

- ユーザーモードで動作し、完全な可視性を提供すること。他のソフトウェアとの干渉により「ブルースクリーン」を発生させるリスクがなく、運用開始やシステムアップデートの前に統合試験に多くの時間を費やす必要もないこと。
- エンドポイントリソースをあまり多く消費しないこと。
- いかなるユーザータスクも妨げないこと。例えば、ユーザーが実行するアクティビティの速度を低下させないこと。
- ネットワークパフォーマンスへの影響を最小に抑えつつ、リアルタイムでサーバーと情報を共有できること。
- フォレンジック情報収集のためのディープなオンデマンドアクセスを提供すること。

強力な中央サーバーが、あらゆるデータを相互に関連付けることで、脅威の検知、修復、回避を効率的かつ効果的に実現します

理想的な EDR プラットフォームは、エンドポイントに関するデータ分析を超えた機能を実行する必要があります。同ソリューションは、データを中央で一元的に分析することで、複数のエンドポイント間でのパターンや異常な行動を特定する必要があります。同プラットフォームは、次の機能を持つサーバーを含んでいる必要があります。

- 重要な情報をサーバー上に格納することで、安定した情報の可用性を保証すること。
- 複数のセンサー間で悪意のあるアクティビティを相互に関連付けることにより、別の場所でより攻撃的な脅威アクティビティが発生する前に脅威を特定すること。
- 脅威インテリジェンスを活用して、エンドポイントから収集した情報をリッチ化すること。

購入者のためのチェックリスト

検知

ソリューションはファイルレス型のマルウェアやラテラルムーブメントを自動的に検知しますか？

ソリューションは統計分析や行動分析を実行しますか？

ソリューションは複数のエンドポイント間でアクティビティを相互に関連付けますか？

エージェントはエンドポイント上で継続して稼働しますか？

ソリューションはメモリベースおよびファイルベースのアクティビティを監視しますか？

調査と応答

ソリューションはセキュリティインシデントをプロアクティブに監視し、それに関するアラートを発行しますか？

ソリューションはインシデントを優先順位付けし、疑わしいアクティビティに関する可視性を提供しますか？

ソリューションは影響を受けたエンドポイント上で、ユーザーによるプロセスの強制停止、ファイルの隔離、レジストリキーの削除が行えますか？

展開

エージェントはエンドユーザーに影響を与えずに素早く展開できますか？

ソリューションは脅威の検知や探し出しが行えるように事前設定された状態で提供されますか？

ソリューションはクラウドまたはオンプレミス環境で展開するためのオプション付きで提供されますか？

ソリューションはマネージドサービスに関するオプションを提供しますか？

環境への影響

エンドポイントはユーザーモードで動作しますか？

ソリューションの CPU リソースの使用率は 5%未満であり、かつそれが使用するメモリ量は 50MB 未満ですか？

ソリューションがやり取りするネットワークトラフィック量は 10MB 未満ですか？

サーバー処理

ソリューションは重要な情報を中央に保存しますか？

ソリューションは、中央での一元化された脅威分析や行動分析を実施しますか？

Cybereason について

Cybereason は、イスラエル国防軍の諜報機関におけるサイバーセキュリティのエリート部門、8200 部隊のメンバーを母体として設立されました。世界でも最高レベルの複雑さが要求されるさまざまなハッキング対策に従事してきた経験から得たノウハウを、ソリューションに活かしています。

リアルタイムでの攻撃検知と対応を可能にする世界で唯一のミリタリーグレードプラットフォームを開発し、フォーチュン 1,000（売上高の多い米国企業上位 1,000 社）のセキュリティをグローバルレベルで支えてきた確かな実績があります。

Cybereason は、株式非公開企業です。本社を米国のボストンに構え、イスラエルのテルアビブと東京に支社があります。