AhnLab

White Paper

「検知を超えた対応」EDR を活用したセキュリティ戦略

Contents

EDR の理解

エンドポイントは、サイバー攻撃者の最終目標である。エンドポイントの脆弱性は年間数万件に達しており、一日に発見される新種マルウェアは数十万個に及ぶ。さらに最近は、従来のセキュリティソリューションの検知回避、ラテラルムーブメントによるサーバーの窃取、侵入した痕跡の削除など、高度な攻撃タイプも登場している。これを解決するために、常時監視および事後調査システムを確立する方向にセキュリティパラダイムが変化しており、そこで登場したのが 「EDR (Endpoint Detection and Response)」 である。

2013年、ガートナー (Gartner) によって初めて紹介された EDR は、エンドポイントで持続的なモニタリングと脅威情報の収集および解析を通じて脅威に対する適切な可視性を確保し、対応力を強化するセキュリティソリューションである。これにより、脅威の潜伏期間 (Dwell Time) を最小化し、潜在的な被害を防止することが目的である。また、ガートナーによると、EDR は ▲セキュリティ侵害検知 (Detect security incident) ▲セキュリティ侵害調査 (Investigate Security incident)、▲エンドポイント領域での侵害抑制 (Contain the incident at the endpoint) ▲感染前の状態に戻す処置/回復 (Provide remediation guidance) の 4つの機能をすべて提供する必要がある。

簡単に説明すると、EDR は監視カメラに近い役割を担う。エンドポイントで発生するすべての振る舞いを検知してエンドポイントロギングを強化し、侵害事故の調査に必要な情報を常時収集する。収集した振る舞い情報をもとに脅威を能動的に追跡・解析し、長期的な脅威対応システムの確立に貢献する。

EDR の核心: 保護に留まらず、積極的な検知と対応、再発防止の役割まで遂行する次世代のエンドポイントセキュリティソリューション

参考に、EDR はエンドポイントセキュリティを補うためのツールであり、セキュリティ環境を完璧にする万能ソリューションではない。この点を理解し、アンチウィルス (Anti-Virus、AV) など、従来のセキュリティ製品と連携して使用することが望ましい。

EDR 導入の必要性

EDR は 「収集できない対象は解析できず、解析できなければマルウェアの有無を判別できず、マルウェアを確認することができなければ対応もできない」 を基本的な前提としている。

この前提条件を満たすために、EDR は端末で発生したすべての振る舞いを持続的にモニタリングして可視化し、従来のソリューションとの連携を通じて脅威の潜伏期間を最小にすることを目標に作動する。脅威の潜伏期間とは、外部から流入した脅威の確認から、サンプリングおよび解析、エンジン登録およびアップデートまでにかかる時間を意味する。この期間中に発生する可能性があるセキュリティの脆弱性に、 EDR を活用し対応することができる。

攻撃者がマルウェアを配布する代表的な経路は、電子メールまたは Web である。攻撃者は脆弱性を持つ特定の PC を確保し、攻撃を実行した後、バックドアをインストールして外部に存在する C&C サーバーを通じて追加のマルウェアをダウンロードする。また、内部にアクセス可能なサーバーを探り、そのサーバーに接続可能な PC に対してラテラルムーブメント (Lateral Movement) を実行する。これによりサーバーのデータを流出させた後、その痕跡をすべて削除する。

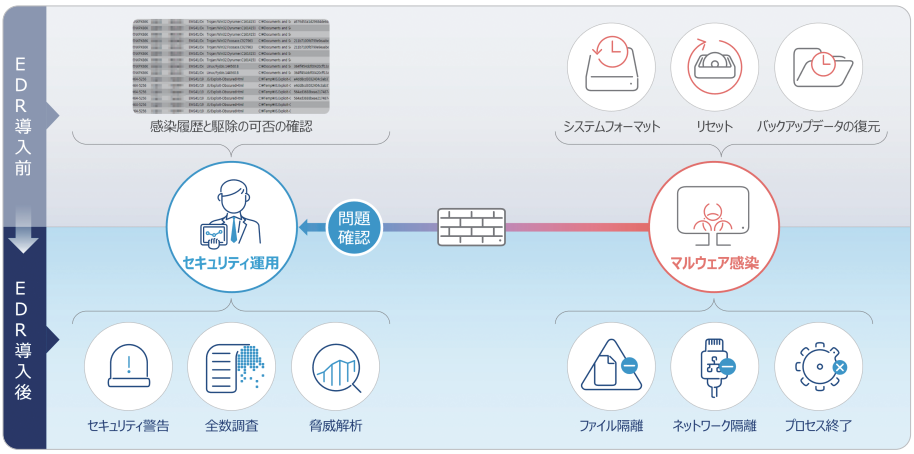
このようなタイプの攻撃は従来のセキュリティソリューションでは追跡が不可能である。これを補うためには EDR の導入が必要だ。EDR は、タイムラインをベースにエンドポイントで発生するファイルやプロセスなどの振る舞い履歴をロギングし、必要な場合には能動的に脅威を追跡する脅威ハンティング (Threat Hunting) を遂行することができる。

このほかに、脅威の拡散を防止するためのネットワーク隔離、プロセスの実行遮断、ファイルの収集および復元など、様々な対応方法を提供し、企業の事前予防および再発防止システムの構築をサポートする

EDR が必要な理由:
・未知の脅威対応の限界
・高レベルのフォレンジック解析技術が必要
・侵害原因の解析による再発防止戦略の導出

さらには、EDR にマイターアタック (MITRE ATT&CK) フレームワークを適用することで、様々な攻撃手法をより効果的に検知し、識別することができる。攻撃の特定段階と使用された技術を参考に、脅威がとこから始まり、どう進行されたのかを確認することができ、今後発生する可能性のある攻撃方式を予測することも可能である。そのため、セキュリティ担当者は脅威をよりよく理解して迅速に対応するなど、組織の全般的なセキュリティ態勢を強化することができる。

従来は、脅威対応が単発に過ぎず、脅威の高度化により解析と対応に限界があったが、今では EDR を活用することで未知の脅威にも全方位から管理・対応でき、総合的な解析により原因を把握することで再発を防止する戦略まで立てることができる。



[図 1] EDR 導入前と導入後の比較

そこで、アンラボは 「AhnLab EDR」 を 2018年に初めてリリースした。さらに、2022年には、使用性と脅威の可視性をより一層強化したアップグレードバージョンである 「AhnLab EDR 2.0」 も発表した。

AhnLab EDR の攻撃対応方法

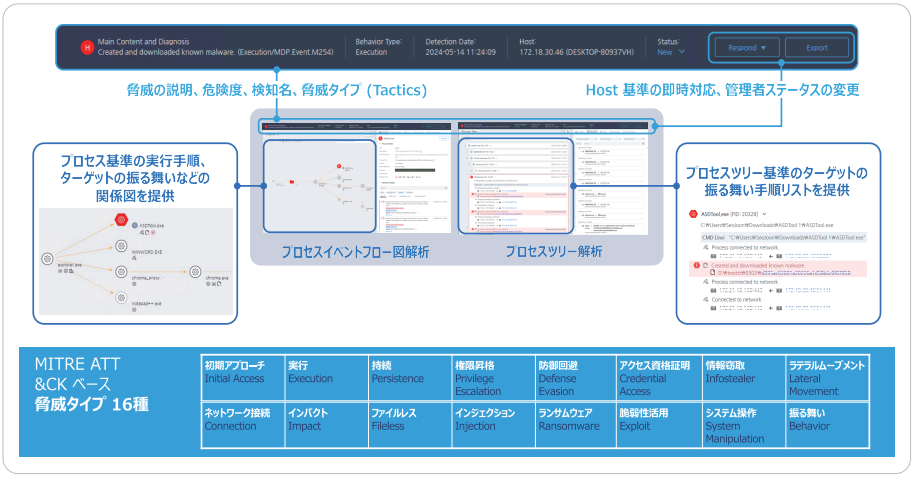
AhnLab EDR は、以下の 7つの核心機能をもとに、エンドポイント脅威に対応する。

AhnLab EDR の主要機能 (1):
ダイアグラムおよびタイムライン解析を通じた脅威情報の提供

AhnLab EDR の主要機能 (2):
脅威インテリジェンスプラットフォームと連動した専用コンソールの提供

(1) ダイアグラムおよびタイムライン解析

マイターアタック (MITRE ATT&CK) ベースの脅威タイプ 16種や脅威の流入経路、主な振る舞い、相関関係、危険度、脅威情報リンクなどに関する解析内容と、プロセス、ファイル、システム、レジストリ、ネットワークターゲット別の振る舞いおよび詳細情報を提供し、リアルタイムで対応する。また、検知された脅威の解析情報を主な振る舞い別 (オブジェクトの種類/危険度)、一般振る舞い別 (オブジェクトの種類)、アーティファクト (Artifacts) 情報を基準に、事前分類できるフィルターとこれらの必要条件を組み合わせてタイムライン別に情報を提供する



[図 2] ダイアグラム解析

(2) 専用コンソールベースの脅威情報および統計の提供

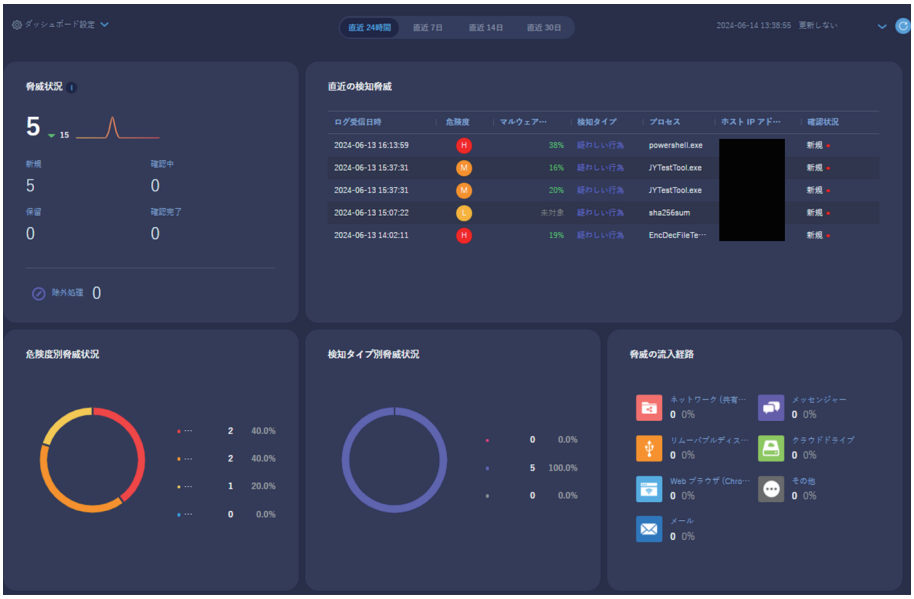
AhnLab EDR は、運用の利便性とアンラボの専門技術力を搭載した専用コンソールである 「EDR Analyzer」 を提供する。EDR Analyzer は、検知や解析、対応の観点からユーザーが脅威を正確に認識し、条件を設定するように構成されている。AhnLab EDR は疑わしい振る舞いに関するタイプ別の情報を常時収集し、EDR Analyzer の中央サーバーに保存しており、ユーザーの環境やモニタリンググループの重要度に応じて振る舞い収集レベルを調整することで、管理を最適化し、容量の負担を軽減する。

また、EDR Analyzer をアンラボ脅威インテリジェンスプラットフォーム AhnLab TIP と連動することで、最新の IoC (ファイル、IP アドレス、URL) 状況の情報と最新のセキュリティアラートを提供し、ユーザーの EDR で検知されたイベントに関するレピュテーションも照会することができる

AhnLab EDR の主要機能 (3):
機械学習ベースの高度な検知および解析

AhnLab EDR の主要機能 (4):
ユーザー指定ルールおよび自動対応の設定

AhnLab EDR の主要機能 (5):
ランサムウェアに感染した PC の重要データの復旧



[図 3] EDR Analyzer ダッシュボード

(3) 機械学習 (ML) ベースの危険度解析

AhnLab EDR には、「教師あり学習 ML」 が適用されており、アンラボのクラウドサーバーである ASD(AhnLab Smart Defense) に収集された数百億の大容量データをベースに学習を行う。学習時には 10個以上のモデルを使用し、その中から最適なモデルを選定して製品に反映する。EDR に適用された ML は、EDR が検知した疑わしい振る舞いや脅威が不正である確率を提供し、セキュリティ担当者が EDR の解析結果における優先順位および重要度を把握する際に役立つ。

(4) ユーザー指定ルールの設定による自動対応

AhnLab EDR は、様々な種類のユーザー指定ルール (IoC/Yara/振る舞いベースのルール) やネットワークおよびファイル隔離、プロセス遮断など自動対応の設定機能を提供する。特に、振る舞いベースのユーザー指定ルールは、組織の環境に合わせて重点的なモニタリングが必要な疑わしい振る舞いを定義することができ、組織の環境に特化した脅威管理をサポートする。

(5) ロールバック (Roll back) 機能

ロールバック機能も、AhnLab EDR の主な機能のひとつである。AhnLab EDR は、Windows の VSS 技術を活用して、ランサムウェアで暗号化されたファイルを復元する。また、不正な振る舞いや、 VSS 機能の無効化、スナップショットの削除を防ぐ。これにより、ユーザーは PC データを被害に遭う前の状態に安全に復元できる。

AhnLab EDR の主要機能 (6):
侵害事故の詳細解析および追加証跡の収集

AhnLab EDR の主要機能 (7):
EDR の運用と活用をサポートする MDR サービスをデフォルトで提供

[図 4] ロールバック機能適用プロセス

(6) 侵害事故の証跡取集および対応

AhnLab EDR は、詳細解析が必要な端末を対象に、追加の証跡情報を収集して対応する。デフォルトおよびユーザー指定条件別にアーティファクトの情報を収集して解析し、ファイルの全数調査を行う。その後、多数の端末から収集された詳細情報をもとに、統合検索システムを通じて侵害事故の詳細解析および検索を行う。

(7) EDR の運用と活用をサポートする MDR サービスの提供

AhnLab EDR は、アンラボのセキュリティ専門家が EDR の運用と活用をサポートする 「MDR サービス」 を基本提供する。企業にインストールされ運用される EDR を活用して、脅威に対するチケット (Ticket) を発生させ、レピュテーション情報、マルウェアの振る舞い解析など、アンラボの脅威対応プロセスに合わせて体系的に対応し、脅威解析レポート、マンスリー統計レポートだけでなく、脅威の緩和および復旧のための措置ガイドも共に提供する。

より専門的なカスタマイズ型 MDR サービスを希望する企業は、追加料金を支払うことで、脅威全体に対するモニタリングや解析、対応サービスを提供し、四半期別に専門家の意見を含むレビューレポートを発行する 「EDR Premium」 を利用できる。

[図 5] MDR サービスの概要

AhnLab EDR の実戦活用方法

AhnLab EDR は、単独で構築すると本領を発揮できない。他のセキュリティ製品と連携して統合セキュリティを実現してこそ、さらに強力なセキュリティシステムを構築できる。

AhnLab EDR は、アンラボの AV ソリューションである V3 製品群や、サンドボックスソリューション MDS、エンドポイント統合セキュリティプラットフォーム EPP (Endpoint Protection Platform) のような EP 専用ソリューションだけでなく、SIEM (Security Information and Event Management)、SOAR (Security Orchestration、Automation、and Response) などのリモートコントロールシステム、そして様々な連携システムと共に使用することで、セキュリティ強化の相乗効果を発揮することができる。

(1) EP ソリューション連携 - エンドポイント統合セキュリティの実現

まず、AhnLab EDR は AhnLab V3、AhnLab MDS と有機的に連携され、エンドポイント領域に対する統合セキュリティを実現できる。V3 と連携すると、すでに発生した脅威と疑わしい振る舞いを不正/警告/注意の 3段階に分類し、解析情報を提供する。MDS と連携すると、疑わしいファイルに対して追加で動的および静的解析を行う。

さらに詳しく説明すると、 AhnLab V3 をインストールしたサーバーに AhnLab MDS と AhnLab EDR を追加することで、エージェントに不正なファイルの削除、PC の隔離、お知らせの送信などの対応コマンドを出し、ML とビッグデータベースの脅威検知機能を通じて APT 攻撃のような未知の脅威を効果的に検知、対応できる。また、ファイルの実行から終了までの振る舞いを詳細解析した結果のレポートを提供し、ウイルストータル (VirusTotal) との連動でユーザーが不正の有無を判断できるようにサポートする。

AhnLab EDR は、未知の脅威に加えて、AhnLab V3 と AhnLab MDS を回避する攻撃も遮断する。エンドポイントで発生するすべてのプロセスやファイル、レジストリ、システムの振る舞いを収集し、アンラボのノウハウとマイターアタック (MITRE ATT&CK) フレームワークを利用した検知パターンおよびルール (Rule) で脅威をモニタリングし、検知する。さらには、ユーザーの環境に合わせた IoC、YARA、振る舞いルール生成による脅威検知および対応も可能である。

また、V3 が検知したマルウェアの流入経路、主な振る舞いのマイターアタック情報、プロセスイベントのフロー図、プロセスツリー、タイムライン情報など、今後発生し得る同一の脅威を先制して防御できる様々な解析情報を提供する。EDR で収集された疑わしいプロセスまたはファイルは、MDS でサンドボックス解析が可能であり、解析結果および追加証跡も確認できる。

AhnLab EDR と V3、MDS 間の連携による効果: 既知/未知のマルウェア検知とサンドボックスベースの動的解析、振る舞い情報の収集およびモニタリングによる全方位的なセキュリティ力量の確保

AhnLab EDR と EPP の統合: 従来のエンドポイント製品比、迅速な脅威検知および自動対応可能

[図 6] AhnLab EDR と AhnLab MDS 間の連動

まとめると、AhnLab V3 がシグネチャおよびパターンベースのマルウェア検知と不正なファイルや URL の遮断・削除・処置などの事前対応を行い、AhnLab MDS がサンドボックス技術をベースに未知の脅威を正確に検知し、AhnLab EDR は最終的にエンドポイントで脅威の可能性があるすべての振る舞いをモニタリングおよび検知し、脅威を追跡、解析するという点でさらに高度な機能を担う。これら 3つのソリューションを連携して構築すると、複雑なエンドポイントシステム環境を安全に守ることができる。

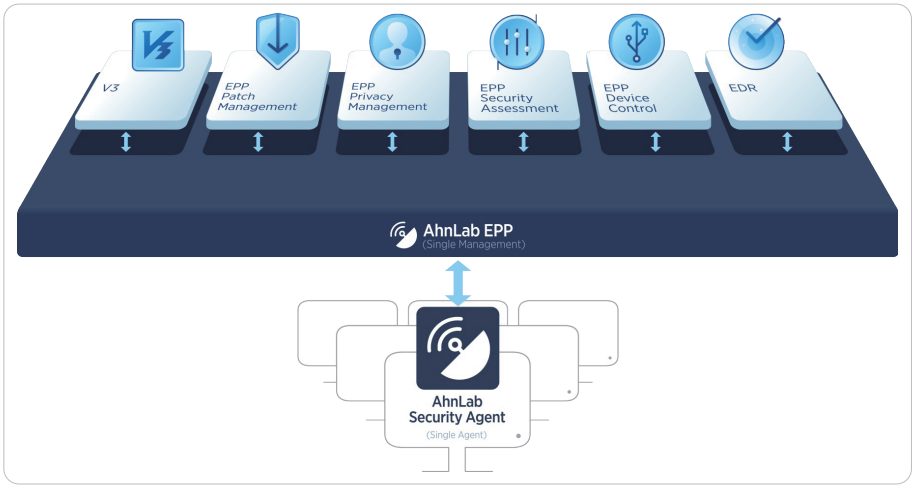
[図 7] エンドポイント統合エージェントベースの脅威対応アーキテクチャ

このほかにも、AhnLab EDR は AhnLab EPP と統合し、脅威をさらに素早く検知して対応する。EPP に含まれたソリューションがエンドポイントハードニング (Endpoint Hardening) のためのセキュリティ機能を提供し、脅威を直接検知・対応することに対して、EDR は EPP が検知・対応した結果を解析してセキュリティ担当者に知らせ、侵害事故の発生や進行有無、対応の必要性に関するインサイトを提供する。

エンドポイントハードニング: 様々な保護措置を通じてエンドポイント領域のアタックサーフェスを最小にすること

AhnLab EDR の実戦活用方法 (2):：SIEM および SOAR との連動でセキュリティ脅威対応の自動化

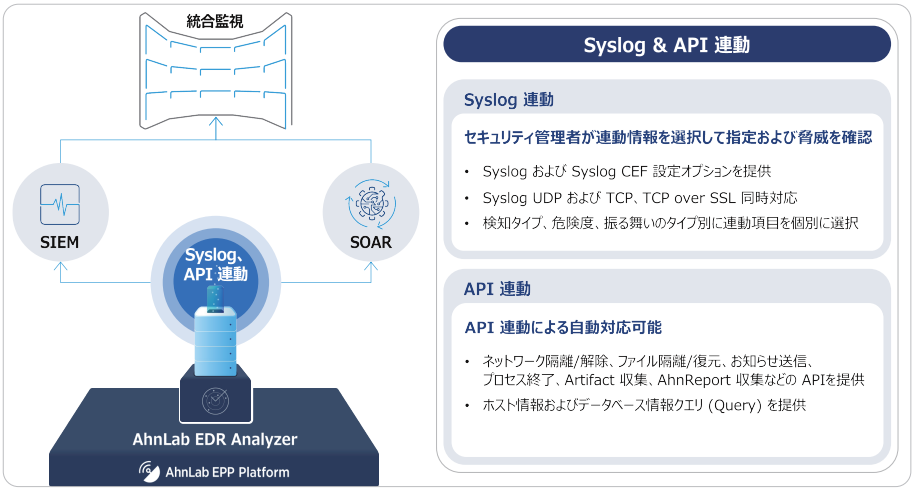
また、EPP と連携した AhnLab EDR は、エンドポイントの脆弱性の有無、疑わしい振る舞いなどに対する個別または連携ポリシー設定を提供し、セキュリティ管理者がセキュリティポリシーを違反したシステムに対する通知、ネットワーク隔離、マルウェア処置、パッチ適用などを主導的・能動的に措置できるようにサポートする。



[図 8] AhnLab EPP プロダクトラインとの相互補完の運用

(2) SIEM & SOAR 連携 - セキュリティ監視 (SOC) 運用効果の極大化

AhnLab EDR は、SIEM、SOAR との Syslog、API 連動機能を提供する。したがって、セキュリティ管理者は脅威検知タイプ、危険度、振る舞いタイプなどの連動情報を選択して脅威を確認することができ、ネットワーク隔離または解除、ファイル隔離および復元、お知らせ送信、プロセス終了、アーティファクト収集、AhnReport 収集などの API を連動して自動対応が可能である。また、ホスト情報およびデータベース (DB) 情報クエリ (Query) を提供している。



[図 9] AhnLab EDR と SIEM & SOAR 連携

AhnLab EDR の
実戦活用方法 (3): アンラボプロフェッショナルサービス連携による侵害事故の解析および脅威対応策の策定

また、SIEM はネットワーク情報もしくは単純な AV 検知情報だけでアラート条件を設定するため、エンドポイントの様々な情報との相関分析の実行や連携条件の設定に限界がある。しかし、AhnLab EDR を SIEM と連携すると、問題イベントのアラート条件を多様化し、深刻度の基準を細分化して脅威および対応の優先順位に関する判断が容易になり、エンドポイント脅威にリアルタイムで対応できるため平均修復時間 (MTTR) および運用リソースを減少できる。

(3) アンラボ専門家サービス連携 – 最適の対応方法の提示

AhnLab EDR を MDR サービスと一緒に 「アンラボプロフェッショナルサービス (Professional Service) 」と連携すると、韓国国内最高のマルウェア専門解析者が企業および機関に流入したマルウェア (ファイル) のダウンロードや複製、生成、ネットワークなどの機能と特性を詳細解析し、疑わしい振る舞い情報に応じた対応策を提示する。また、内部に流入したマルウェアの基本情報、不正の有無、振る舞い情報などをまとめた解析レポートも提供する。

さらには、侵害事故による影響と流入経路をデジタルフォレンジック技術で解析してリスクを管理し、APT 攻撃などのセキュリティ事故の再発を防止する。

まとめ

AhnLab EDR は、マルウェア感染や侵害事故の予防のための技術的な保護措置が必要なすべての企業と機関に必須のセキュリティソリューションである。ただし、AhnLab EDR を導入する際には、画一的な観点からアプローチしてはならない。EDR 自体、検知および解析情報が多く、重いソリューションであるため、現在の組織の規模や IT インフラの状況、コスト、具体的な活用方法など様々な要素を考慮する必要がある。また、単独で運用するより他の製品と連携した場合に大きなセキュリティ価値を提供するという点を踏まえて考慮するべきである。従来の IT 環境で EDR により補完できる領域を積極的に検討し、それに合わせて EDR を 「カスタマイズ型」 で構築することが望ましい。必要な場合、アンラボのような専門企業のコンサルティングを受けることも良い方法である。

AhnLab EDR に関する詳細は アンラボドットコム (www.ahnlab.com) で確認できる。

▶AhnLab EDR 製品紹介ページに移動

AhnLab

株式会社アンラボ
東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
Tel: 03-6453-8315 | URL: www.ahnlab.com/jp | Mail: jp.sales@ahnlab.com