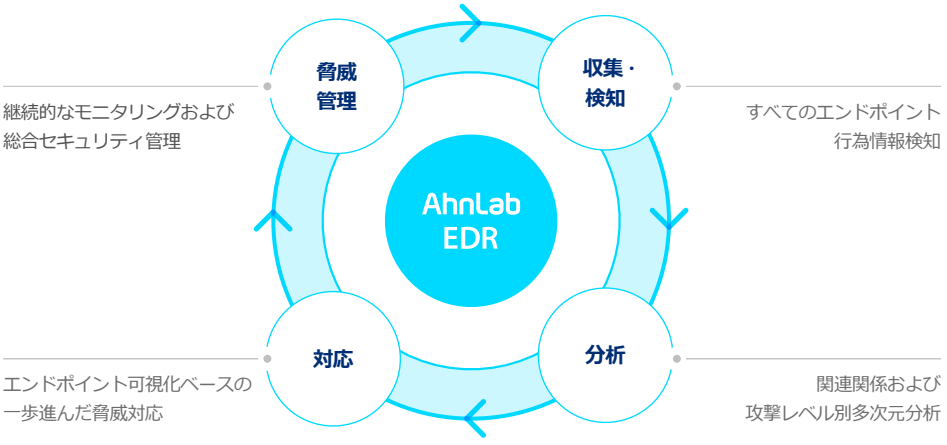
AhnLab EDR

巧妙な検知、専門的な分析と対応、能動的な追跡

AhnLab EDR は、MITRE ATT & CK 評価にて検証された検知・分析・対応力をベースに脅威を能動的に追跡し、企業の強力なセキュリティシステムの樹立に貢献します。

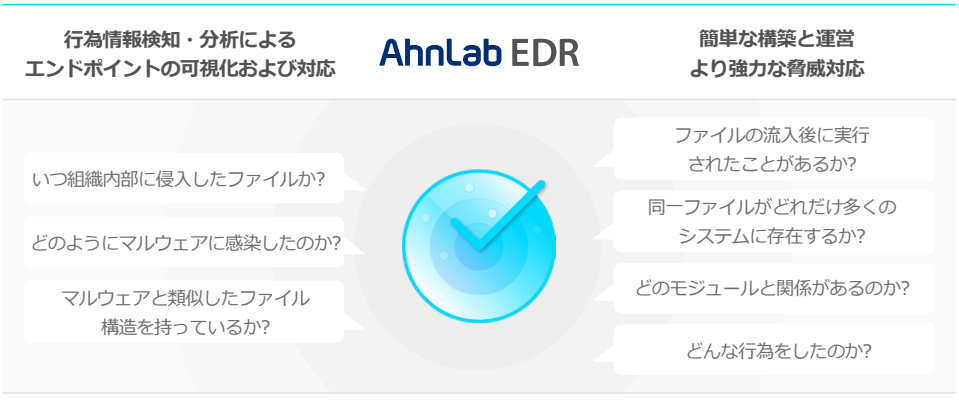
製品紹介

AhnLab EDR は、韓国国内唯一の行為ベースの分析エンジンに基づき、エンドポイント領域に対して強力な脅威モニタリングと分析、対応力を提供する次世代エンドポイント脅威検知および対応ソリューションです。MITRE ATT&CK 評価で優秀な成績を収めた AhnLab EDR は、MDR (Managed Detection & Response) サービスと結合し、脅威検知および対応プロセス全般の専門性を強化します。



AhnLab EDR

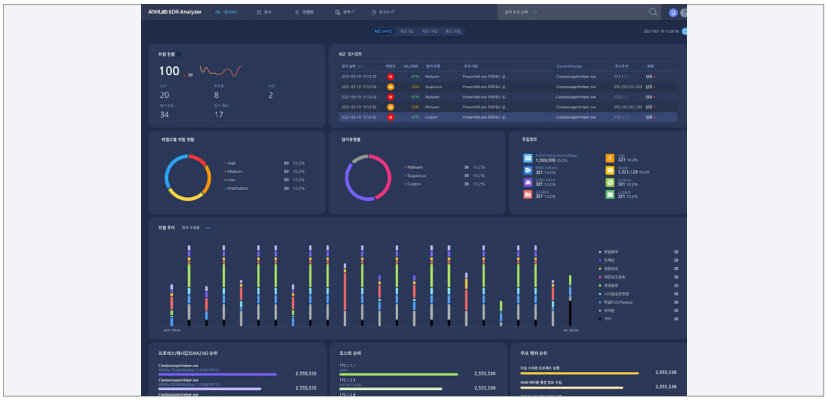
エンドポイントを狙った攻撃はますます高度化しています。日々数多くの新・亜種マルウェアが出現しており、全ての脅威を事前に遮断することはほぼ不可能です。したがって、常時監視と迅速な侵害事故の認知により、脅威を最小限に抑えるセキュリティシステムを樹立する必要があります。AhnLab EDR は、行為情報を検知・分析して幅広いエンドポイント可視性を提供し、簡単な構築と運用で一歩先の脅威検知 & 対応を具現化します。また、脅威を能動的に追跡するため、企業が事前予防および再発防止システムを構築するのに役立ちます。



特長

運営の利便性

AhnLab EDR は、アンラボの技術力・専門性を備えた専用コンソール「EDR Analyzer」を提供します。EDR Analyzer ダッシュボードは、単純な統計を超えて検知・分析・対応の観点からユーザーが脅威を正確に認知し、条件を設定できるように構成されています。また、AhnLab EDR は疑わしい行為に関連するタイプ別情報を常時収集し、EDR Analyzer 中央サーバーに保存して顧客企業の環境に応じて行為収集レベルをオプション化し、管理を最適化して容量負担を軽減します。



▲ AhnLab EDR Analyzer ダッシュボード

巧妙な脅威検知 & 分類

AhnLab EDR は、韓国国内唯一の独自の行為ベースのエンジンにより、自主的に国内外の攻撃グループを分析し、検知パターンと規則 (Rule) を作成して脅威検知に巧妙さを加えます。また、脅威を MITRE ATT & CK フレームワークの戦術 (Tactic) に基づいて16種類の行為カテゴリーに分類し、ユーザーが脅威を直感的に識別できるようにします。このほか、マシンラーニング技術の適用により、脅威別の危険度とマルウェア危険確率に関する情報も提供します。

専門的な分析 & 対応

AhnLab EDR は、検知した脅威に対して MITRE ATT & CK フレームワークベースの脅威情報と流入経路、主要行為、関連性、危険度、脅威情報リンクなどについて詳細な分析内容を提供します。このように多様な分析情報を ▲相関図 ▲タイムライン ▲プロセスツリーを通じて直感的に具現化し、ユーザーが攻撃の流れ全般を簡単に把握できるようにします。また、主要行為に対するオンデマンド (On-Demand) スキャンと AhnLab TIP および AhnLab MDS 連動による追加分析も可能です。

より強固にする基本サービス

AhnLab EDR で検知されたイベントのうち、明らかに知られている脅威に対して1 / 2次レポートを提供し、顧客が EDR をより効果的に活用できるようにします。さらに、顧客との事前協議のもと、脅威対応も行います。

*上記の内容は、AhnLab EDR 導入時に基本的に提供されますが、EDR 検知ログを外部に送信できない場合は提供されません。

MITRE ATT & CK 評価検証

AhnLab EDR は、直近に行われた MITRE ATT & CK Evaluation Round 4 で、攻撃グループ 「ウィザードスパイダー (Wizard Spider)」 と 「サンドワーム (Sandworm)」 が使用する最新技術を模擬遂行した 90個の攻撃ステップ (Step) で83個を検知して 92%の検知率を記録しました。これにより、高度化した実際の脅威に対する卓越した検知力を立証しました。

主要機能

AhnLab EDR は検知タイプ別に脅威を分類し、脅威認知から分析、対応まで迅速なワークフローをサポートします。また、様々なソリューションと連動して対応力を最大化し、AhnLab EPP 製品間の連携規則設定を通じて企業環境に最適化されたエンドポイントセキュリティ運用が可能です。

高度化した脅威検知・分類・分析・対応

- 全ての行為情報の収集および保存 - イベントに関連する全般的な脅威情報を常時確認可能
  - プロセス、ファイル、レジストリ、ネットワーク、システムなどに対する行為情報収集
- エージェント、ファイル、行為など情報単位で詳細な条件別検索および照会可能
- ユーザー定義規則 (IoC、Yara、静的 / 動的行為ルール) の設定による検知および自動対応サポート
- 脅威検知時に即時対応可能 (ネットワーク遮断、プロセス終了、ロールバック、ファイル収集 / 検索 / 削除 / 復元など)
- ユーザー設定による自動対応 (ユーザー定義規則、連携規則、Blacklist Hash ベースプロセスの事前遮断)
- ユーザー (セキュリティ管理者) 定義レポート作成 - CSV、XLS、PDF など様々なフォーマット提供
- オンデマンド (on-demand) スキャンによる主な行為および V3 診断マルウェア行為分析
- MITRE ATT & CK Tactics ベースの16の脅威カテゴリー分類
- ランサムウェア、インジェクション、ネットワーク接続、C&C アクセス、システム設定変更、権限昇格、ファイルレス、情報奪取など主要マルウェア類似行為別監視ファイル情報提供
- 侵害対応分析のための追加資料 (AhnReport / Artifacts / Windows イベントログ) 収集可能

プラットフォームベース統合セキュリティ運用および管理

- 次世代エンドポイントセキュリティプラットフォーム AhnLab EPP ベースの強力な脅威対応システム構成
  - 単一マネジメント、単一エージェントベースの効率的なセキュリティ運用および管理
- 柔軟な連携規則の設定により、有機的な脅威への対応および処理可能
- 拡張されたエンドポイントの可視性に基づいて脅威検知および対応時間最小化

柔軟な連動による脅威インテリジェンスの確保および対応力の向上

- 第三者ソリューションとの連動により、豊富な脅威インテリジェンス (Threat Intelligence) 確保
- SIEM、SOAR、統合ログなどと API & Syslog 連動可能
  - コンソールによる手軽な連動設定 & 様々なプロトコル提供 (UDP / TCP / TCP over SSL など)

EDR Premium

EDR Premiumは、AhnLab EDRとともに専門的な脅威検知 & 対応力を提供する「MDR (Managed Detection & Response)」サービスが結合された商品です。EDR Premium を使用する場合、アンラボの専門家が既知の脅威や疑わしい行為をモニタリング、分析および判断して能動的に対応します。

EDR Premium の背景には、長年蓄積してきたアンラボの業界随一の脅威対応力があります。EDR Premium は、顧客のエンドポイント環境で発生する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、マルウェア行為情報などを活用してアンラボ脅威対応プロセスに基き、体系的に処理します。

この他にも、アンラボは侵害事故分析サービス、マルウェア専門家の分析サービス、疑わしいシステム診断サービスなど多様なプロフェッショナルサービスを EDR Premium と連携し、セキュリティ脅威分析および対応力向上のための様々なオプションを提供します。

*EDR Premium は有償サービスであり、サービス費用および具体的な内容については別途お問い合わせください。

脅威検知
幅広い脅威の
リアルタイム検知

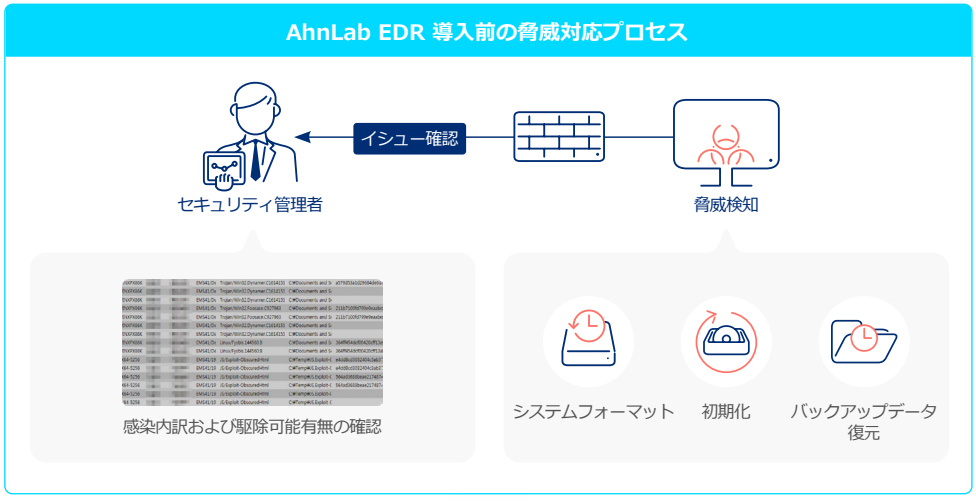
専門家の分析 & 対応
能動的分析 & 対応による
脅威軽減および復元

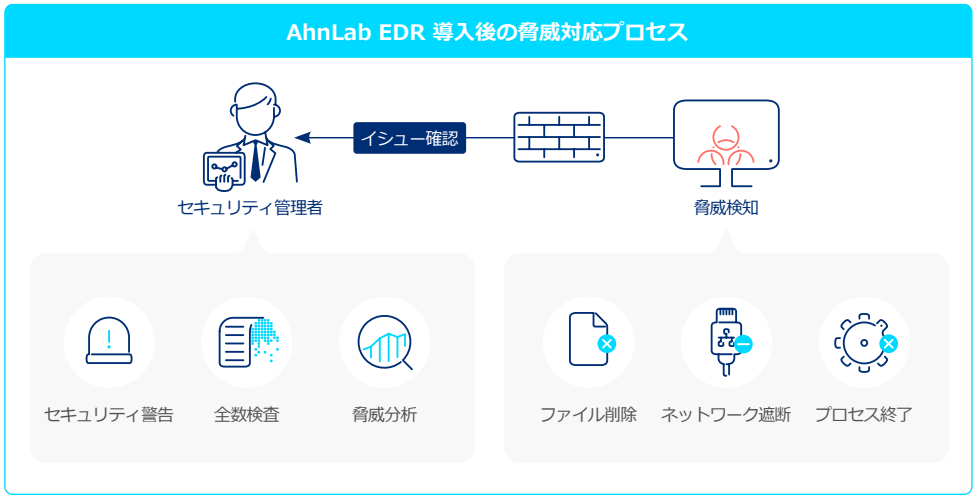
レポート
脅威検知&対応プロセス強化のため
多様なレポート提供

導入効果

AhnLab EDR 導入前は脅威対応が一回限りにとどまり、再発防止の樹立にも限界があります。マルウェア感染履歴が確認されれば、システムフォーマットあるいは初期化を進め、バックアップされたデータがあれば復元して業務を再開する形でした。ワクチン管理サーバーにユーザー PC マルウェア感染履歴が存在しますが、マルウェアがどこから感染し、どこに拡散したのかなどは確認できませんでした。

しかし、AhnLab EDR 導入後は総合的な分析により、原因把握、適切な対応、再発防止プロセスの樹立が可能です。侵害が発生すると、管理者が警告アラームを受信した後、 事前に定義された規則に基づいて脅威分析と全社的なスキャンを行います。これにより、マルウェアと疑われるファイルの収集、プロセス終了、ネットワーク遮断など、適切な対応を行うことができます。また、脆弱性の確認などによる先制的な事前対応と感染履歴の確認による事後対応も可能です。





東京都港区芝4丁目13-2 田町フロントビル3階 〒108-0014
ホームページ: www.jp.ahnlab.com
TEL: 03-6453-8315 FAX: 03-6453-8316