AhnLab XTD

OTの可視化および脅威検知ソリューション

**AhnLab XTDは、OTネットワークを可視化し、リアルタイムで異常行動や
セキュリティ上の脅威を検知する、OT環境に特化したセキュリティソリューションです。**

製品概要

AhnLab XTDは OTネットワークの資産可視性とセキュリティ脅威を検知して監視および管理できるようにサポートするOT専用セキュリティソリューションです。OT環境の可用性を保証するパッシブスキャン(passive scan)方式で動作し、独自に開発したプロトコルプロファイリング技術とディープパケットインスペクション(DPI)機能をもとにさまざまな種類の資産を識別して監視します。また、ITネットワークから流入したりOTネットワーク内部のシステム間で感染するマルウェア、脆弱性などのセキュリティ脅威をリアルタイムで検知して管理できるようにサポートします。

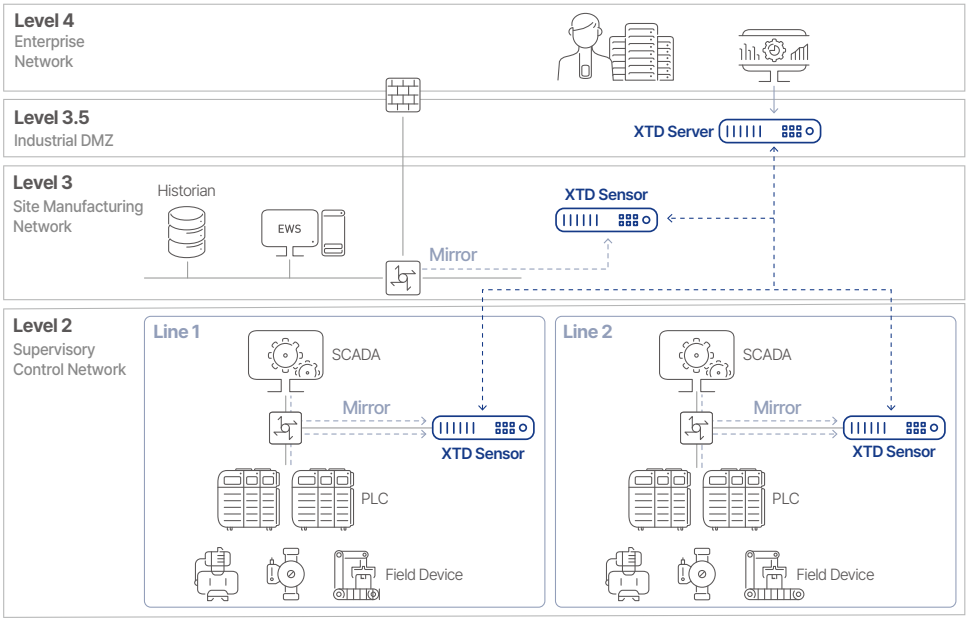
資産とDPIベースのプロトコル分析
ネットワークセッションとトポロジー

マルウェア、脆弱性などの脅威の検知
異常プロトコルと制御ロジックの検知

可用性のためのミラーモードの設定
ネットワーク構成の変更は不要

システム構成

AhnLab XTDは、中央サーバーと各ネットワーク区間ごとに構築されるセンサーで構成されています。ネットワーク区間ごとに設置されたセンサーは、ミラーリングされたトラフィック分析情報とセキュリティ脅威の検知結果を中央管理サーバーへ転送します。中央管理サーバーは収集された情報を分析し、さまざまな可視性と脅威情報を監視し、セキュリティポリシー設定を提供します。小規模の資産で運用中の環境では、センサーとサーバーを組み合わせたオールインワン構成も可能です。



主要機能

可視性の確保

OTとITを包括するCPS(Cyber-Physical System)環境の効果的なセキュリティ管理のためには、資産関連のさまざまな情報をリアルタイムで収集して監視することが重要です。AhnLab XTDは、OT環境の可用性を確保するためにパッシブモニタリング方式でトラフィックを分析し、幅広い可視性を確保します。

AhnLab XTDはOT資産の詳細情報を収集し、直感的に提供します。さらに、資産の各種ネットワーク接続、トラフィックおよびネットワーク情報だけでなく、さまざまなIT、OTとICSプロトコルの分析情報も同時に提供します。

AhnLab XTDは、効率的な可視性の提供とセキュリティ管理のための学習モードと運用モードを提供します。学習モードでは、構築後一定期間、管理対象資産を識別して登録します。そして、運用モードで識別されていない未登録のUnknown資産を別々に管理することができ、隙の無いセキュリティと運用効率性を同時に確保することができます。

- 資産タイプ、製造元
- IP/MACアドレス、ゾーン、グループ
- OS情報、危険度など

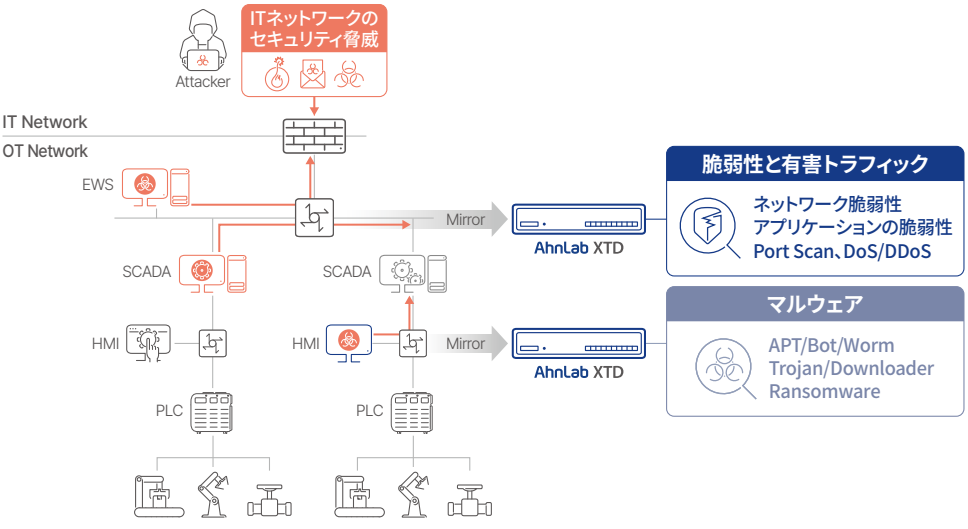
- サービス、セッション
- トラフィック
- トポロジー

- ICSプロトコル
- Function code、valueなど

脅威の検知と管理

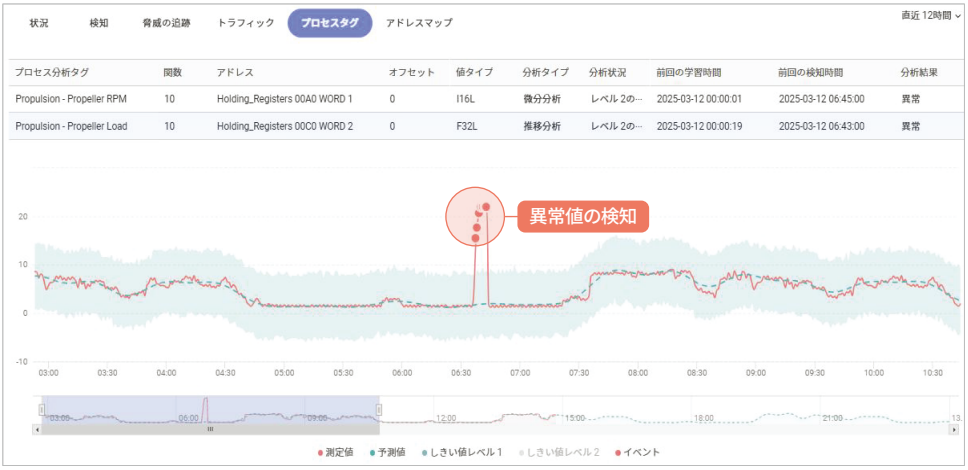
CPS環境の大部分を構成するOTネットワークは独立したネットワークで運用されていますが、古いOSの使用、不十分なセキュリティパッチおよび管理されていないリムーバブルデバイスの使用により、セキュリティ上の脅威に脆弱です。しかし、内部ネットワークの脅威の検知と監視は比較的に不足しています。

AhnLab XTDは、OTネットワークの内部トラフィックを介して感染する様々なセキュリティ脅威を検知および管理します。ランサムウェアを含む様々なマルウェア、ソフトウェアの脆弱性を悪用するトラフィック、スキャン、DoSなど、有害なトラフィックをリアルタイムで検知し、管理者に通知します。特に、アンラボの長年の技術力が反映された独自のアンチウイルスエンジンを適用し、現存するマルウェアと新しいマルウェアまで迅速かつ正確に検知します。



ベースラインの異常検知

AhnLab XTDは、さまざまなICSプロトコルに対するディープパケットインスペクション(DPI)分析技術に基づいて、ベースライン(Baseline)の異常検知機能を提供します。管理者が設定した特定のプロセス値(Value)を統計をもとに学習し、基準値に該当するベースラインを設定します。そして、ベースラインを未達あるいは超過する値を異常変更として検知します。これにより、誤動作に関するリアルタイム通知を送信し、セキュリティ管理者は、悪意のある攻撃者が引き起こす制御システムの誤動作や、管理者のミスによる設備の誤動作をリアルタイムで検知することができます。

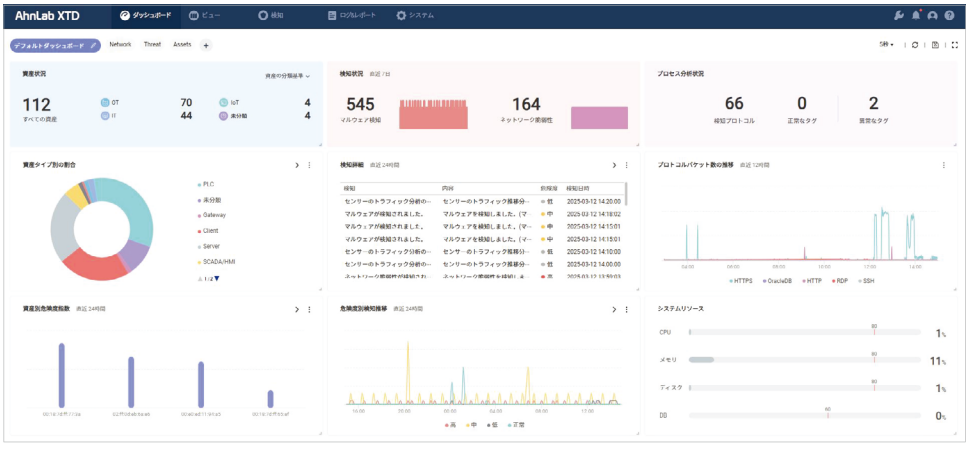


脅威の根源地の追跡

AhnLab XTDは、OTネットワーク内部で感染するセキュリティ脅威の根源地を追跡し、可視性が確保されていない環境でのセキュリティ脅威の可視性を高めます。攻撃を伝播した以前の配布地を確認することで攻撃の移動経路を把握でき、攻撃が伝播される経路を追跡できます。また、ポータブルAVソリューション「AhnLab Xcanner」を活用して、セキュリティ脅威が伝播されたシステムのマルウェアスキャンまたは駆除を実行できます。

ダッシュボード監視

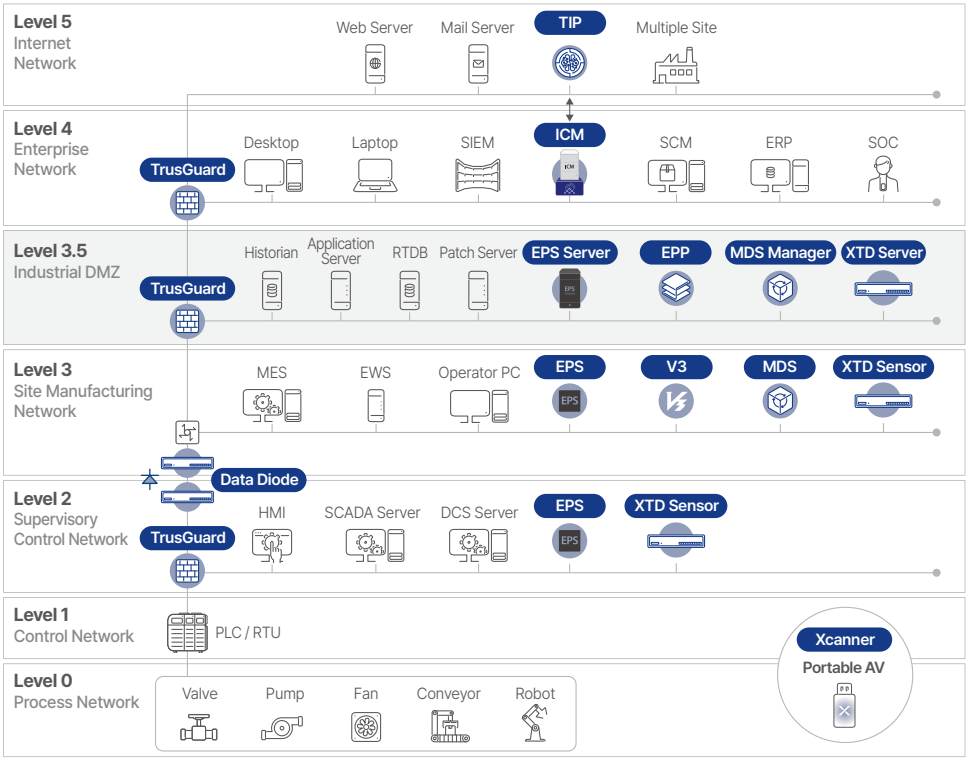
AhnLab XTDは、便利なソリューション運用のためにWebベースの管理コンソールとさまざまな管理メニューを提供しています。動的UXベースの直感的なダッシュボードを使用して、さまざまな資産の可視性と脅威情報をリアルタイムで監視できます。また、ユーザー定義ダッシュボードを通じて、管理者が確認したい情報を別途のダッシュボードパネルとウィジェットで作成および構成できます。



プラットフォームベースのCPSセキュリティ

アンラボは、統合CPSセキュリティのためにOTエンドポイントとネットワーク、そしてOTと接続されたIT環境まで幅広く保護するCPSセキュリティプラットフォーム「AhnLab CPS PLUS」を運用しています。アンラボの脅威検知&対応専門性とOT技術力を組み合わせたAhnLab CPS PLUSは、エンドポイントとネットワークセキュリティ技術をもとにITとOTを組み合わせたCPS環境で▲識別(可視性) ▲脅威検知 ▲対応へと続く隙のないセキュリティを提供します。柔軟に連携するAhnLab CPSセキュリティモジュールは、CPSセキュリティ統合管理ソリューション「AhnLab ICM」を通じて集中管理および監視されます。

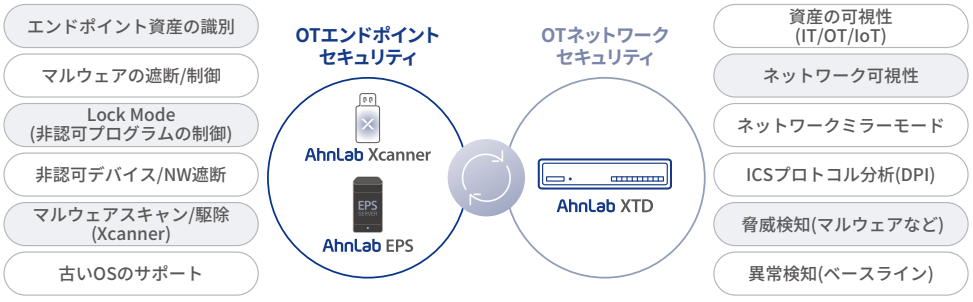
AhnLab CPS PLUSは、現存するCPSセキュリティプラットフォームの中で最も幅広いカバレッジを誇っています。ここに、優れた技術力と統合のシナジーが加わり、顧客に差別化されたCPSセキュリティ体験を提供します。



エンドポイント – ネットワーク連携セキュリティ

AhnLab XTDは、OTエンドポイントセキュリティソリューションAhnLab EPS連携を通じて、他社のセキュリティオファリングでは経験できない独自のOTエンドポイント-ネットワーク連携セキュリティを提供します。

まず、AhnLab XTDが識別したネットワークおよび資産の可視性情報にAhnLab EPSエージェントが収集したエンドポイント資産情報を加え、CPS環境内の可視性を拡張および検証できます。また、検知された脅威に対してもAhnLab EPSとの連携により、疑わしいシステムのマルウェア感染をリモート診断し、リアルタイムで対応することができます。



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.ahnlab.com/jp
TEL: 03-6453-8315 FAX: 03-6453-8316
© AhnLab, Inc. All rights reserved.

AhnLab