

アンラボ・セキュリティレター

Press **Ahn**

2023.9 Vol.117

OT 環境の可視性と脅威対応を強化した「CEREBRO-XTD」リリース

OT 環境の可視性と脅威対応を強化した「CEREBRO-XTD」 リリース

アンラボとナオンワークスがOTセキュリティソリューション「CEREBRO-XTD」をリリースした。CEREBRO-XTDは、既存のOT可視性および脅威検知モニタリング専用ソリューション「CEREBRO-IDS」にアンラボのセキュリティソリューションの連動など、様々な機能を追加および強化したソリューションだ。今回のCEREBRO-XTDのリリースを通じて両社が構築した「統合OTセキュリティフレームワーク」も一層強化されると期待される。

CEREBRO-XTDのリリースニュースと主な機能を紹介する。



アンラボとアンラボのOTセキュリティ子会社ナオンワークスがOT環境の可視性および脅威対応能力をアップグレードした「CEREBRO-XTD」をリリースした。CEREBRO-XTDは、アンラボとナオンワークスが昨年披露したOT可視性および脅威モニタリング製品である「CEREBRO-IDS」をベースに主要機能を強化し、新たにリリースしたソリューションだ。

CEREBRO-XTDは、アンラボのOTエンドポイントセキュリティ製品群と連動し、エンドポイント領域に対する可視性とマルウェア検査と治療まで提供することが特徴である。加えて、多数のOTプロトコルに対するDPI（Deep Packet Inspection）分析技術により、様々な種類の設備識別と異常制御ロジックに対する検知および分析能力を高度化した。ちなみに、DPIとは、ネットワークを行き来するデータであるパケットを深層レベルまで分析できる技術である。

ナオンワークスのイ・ジュンギョン（Jun Kyung, Lee）代表は「CEREBRO-XTDは高度化されたOTネットワークの可視性と脅威検知機能を提供し、ランサムウェアなどのセキュリティ事故を懸念する顧客のデジタル切り替え環境を保護する上で中心的な役割を果

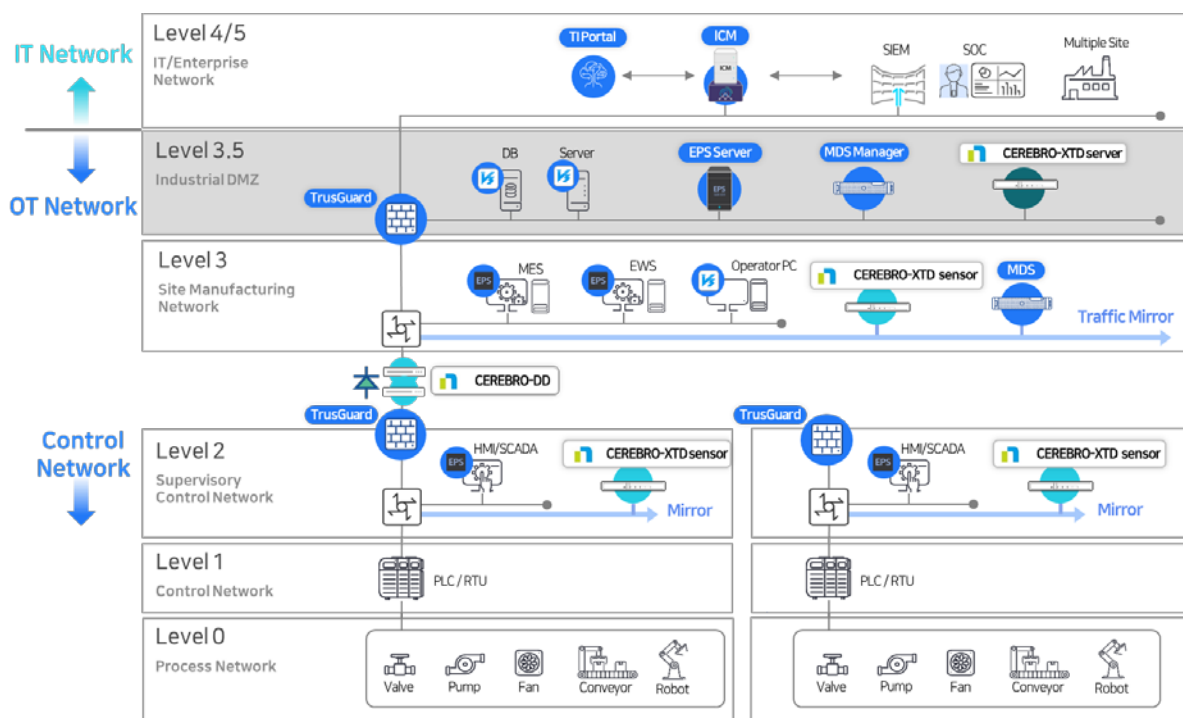
たすだろう」と述べた。

アンラボ製品サービス企画室のキム・チャンヒ（Chang Hee, Kim）室長は「OT環境でも「攻撃表面」はネットワークからエンドポイントまでますます広がっていく中、「CEREBRO-XTD」はOT内の多様な資産と設備に対する可視性を上げ、分析および対応能力の高度化に重点を置いた」と話した。

ユーザー環境に応じたOTセキュリティ要件を満たす

近年、産業施設と社会インフラを対象とするセキュリティ脅威がますます増加する傾向にあり、これによる被害も深刻化している。特に、OT環境がIT環境とつながり、外部との接点が増え、セキュリティに脆弱なOTシステムが各種サイバー攻撃のターゲットとなっている。OTネットワーク内に流入したり、内部システム間で伝播するセキュリティ脅威に効果的に対応するためには、OT環境に特化したセキュリティソリューションと、ITとOT環境を組み合わせた統合セキュリティ方式が必要だ。

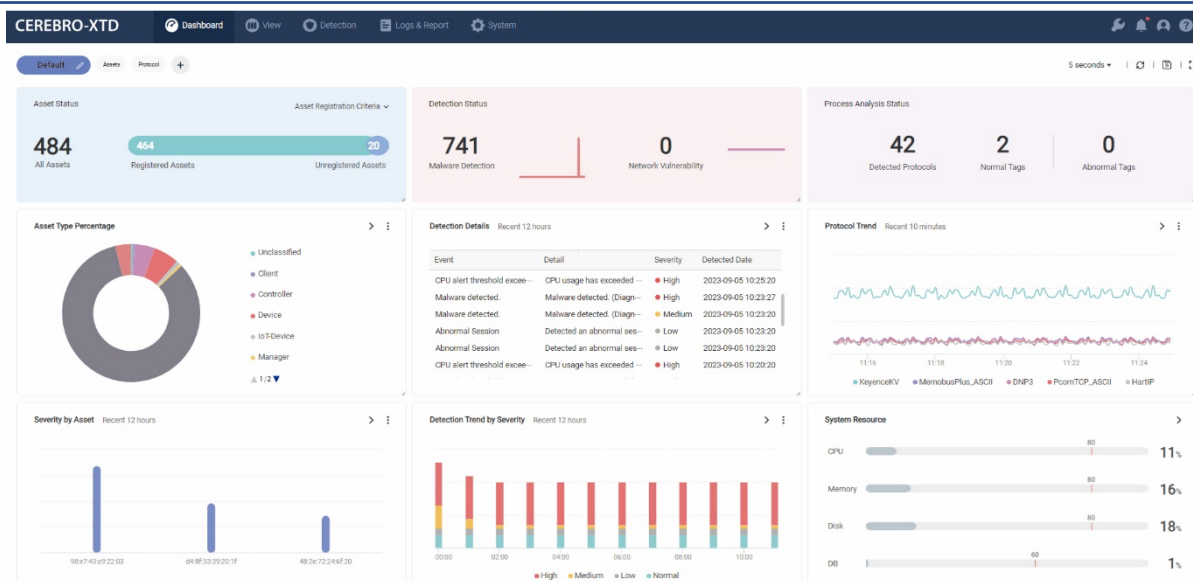
アンラボとナオンワークスは、セキュリティ脅威検知&対応専門性とOT技術力を組み合わせた「統合OTセキュリティフレームワーク」を構築し、OTネットワークパーデューモデル（The Purdue Model）の全層にわたって▲可視性▲脅威検知▲対応につながる隙間のないセキュリティを提供している。両社の様々なソリューションは、お客様のニーズに合わせて柔軟に提供され、製品間の連動シナジーを介し、差別化を図る。



[図1]アンラボ-ナオンワークス「統合OTセキュリティフレームワーク」

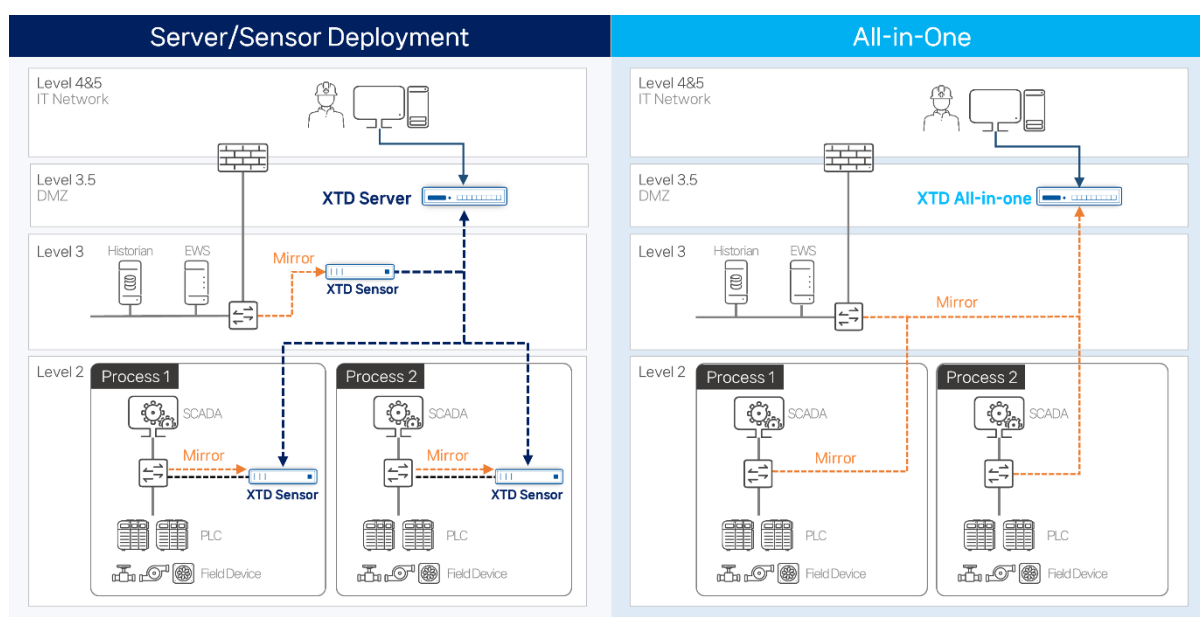
「統合OTセキュリティフレームワーク」の主なソリューションであるCEREBRO-XTDは、総合的なOTネットワークの可視性を提供し、セキュリティ脅威や異常行為をリアルタイムで検知する。可用性を重視するOT環境の特性を考慮し、設備運営に影響を与えない「パッシブモニタリング」方式で動作することで運用安定性を加える。

可視性情報と脅威検知情報は直感的なダッシュボードを介して出力され、ユーザーがリアルタイムで現状を確認できるようにする。また、ユーザーダッシュボード設定により、管理者が追加の確認が必要な情報を別々のダッシュボードとウィジェットで生成し構成することもできる。



[図2] CEREBRO-XTD ダッシュボード

構造的な観点から見ると、CEREBRO-XTDは中央サーバーと各工程固有のセンサーで構成されています。工程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を分析して検知結果を中央サーバーに転送し、中央サーバーは収集された情報を分析して可視性と脅威情報を提供します。また、環境に応じてセンサーとサーバーが結合された「オールインワン」構成も可能である。



[図3] CEREBRO-XTDの構成

一般的に、工程ごとにセンサーを構築し、中央サーバーに接続する「センサー/サーバー構成」は、多数の工程で構成された環境で使用されている。一方、工程の少ない環境では、オールインワンサーバ（All-in-one server）に複数の工程トラフィックを統合する形態の「オールインワン構成」が適している。

エンドポイントセキュリティ連動と脅威の逆追跡、より強力になった機能

既存のCEREBRO-IDSは、▲IT/OT主要資産・ネットワークセッションの状態やトポロジー（topology）マップなどの統合可視性を提供 ▲マルウェアの侵入や有害トラフィック、脆弱性など各種セキュリティ脅威の検知 ▲OTプロトコル 深層分析及び機械学習ベースの異常制御検知 ▲サードパーティー(3rd Party)管制プラットフォームと連動などの機能を提供した。

新リリースしたCEREBRO-XTDは、既存のCEREBRO-IDSの機能に加え、▲AhnLab EPS連動時ネットワークレベルからOT環境のエンドポイント領域までの資産に関する詳細情報を提供 ▲AhnLab Xcanner連動によるマルウェアのリモート検知など、アンラボのOTエンドポイントセキュリティソリューションとの連動機能を追加し、真の「エンドポイント-ネットワーク連携セキュリティ」を実装した。

【図4】 CEREBRO-XTDとOTエンドポイントセキュリティソリューションの連動

まず、特殊目的システム専用のセキュリティソリューションである「AhnLab EPS」を連動すれば、OTネットワークに接続されているエンドポイントまで可視性を拡大することができる。同種のソリューションのほとんどは、ネットワーク領域までの資産の情報を提供している。しかし、CEREBRO-XTDはAhnLab EPSと連動して、ネットワーク領域のデータだけでなく、OTネットワークに接続されたサーバやワークステーション（Workstation）のオペレーティングシステムのパッチバージョンなどのエンドポイントの詳細情報まで提供する。

特殊目的システム専用の診断および治療ソリューションであるAhnLab Xcannerと連動すれば、マルウェア検査領域も拡張することができる。ネットワーク領域で一次マルウェア検査を行った後、エンドポイント領域に位置する疑わしいシステムに対しても再びマルウェア検査を行うことができる。また、検知だけにとどまるほとんどの同種ソリューションとは異なり、検査後の治療まで可能であるため、脅威に能動的に対応できる。

検知された脅威が配布された経路を逆追跡して脅威情報を知らせる「Issue Tracking」機能も追加された。この機能は、攻撃が伝播された以前の配布地を確認し、攻撃の伝播と移動経路を把握できるようにする。これにより、ユーザーは、検知された脅威イベントが配布される経路や、最初に発生した資産などの脅威間の接続性を確認し、体系的な脅威対応を行うことができる。



[図5] CEREBRO-XTDの Issue Tracking 機能

CEREBRO-XTD の詳細はナオンワークスのホームページで確認できる。

▶ [ナオンワークスWebサイト](#)



<http://jp.ahnlab.com/site/main.do>

<http://global.ahnlab.com/site/main.do>

<http://www.ahnlab.com/kr/site/main.do>



アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2023 AhnLab, Inc. All rights reserved.