AhnLab

安全月刊

2023.09 Vol.130

CEREBRO-XTD 上市

“CEREBRO-XTD”上市，

增强了 OT 环境的可见性和威胁响应能力

AhnLab和NAONWORKS联合推出了OT安全解决方案“CEREBRO-XTD”。CEREBRO-XTD是在现有的OT可见性和威胁检测监控专用解决方案“CEREBRO-IDS”的基础上，添加并增强了与AhnLab安全解决方案的集成等各种功能的解决方案。通过此次CEREBRO-XTD的发布，预计将进一步强化两家公司建立的“集成OT安全框架”。

本文将介绍CEREBRO-XTD的发布消息以及其主要功能。

AhnLab和AhnLab的OT安全子公司NAONWORKS共同推出了进一步升级OT环境可见性和威胁响应能力的“CEREBRO-XTD”。CEREBRO-XTD是在AhnLab和NAONWORKS去年推出的OT可见性和威胁监控产品“CEREBRO-IDS”的基础上，增强了主要功能后重新推出的解决方案。

CEREBRO-XTD与AhnLab的OT端点安全产品系列集成，提供端点区域的可见性以及恶意代码扫描和修复功能。此外，通过对多个OT协议的深度数据包检查（Deep Packet Inspection）分析技术，提高了多种设备识别和异常控制扩机检测与分析能力。值得注意的是，DPI是一种可以分析网络传输数据包（packet）的深层部分的技术。

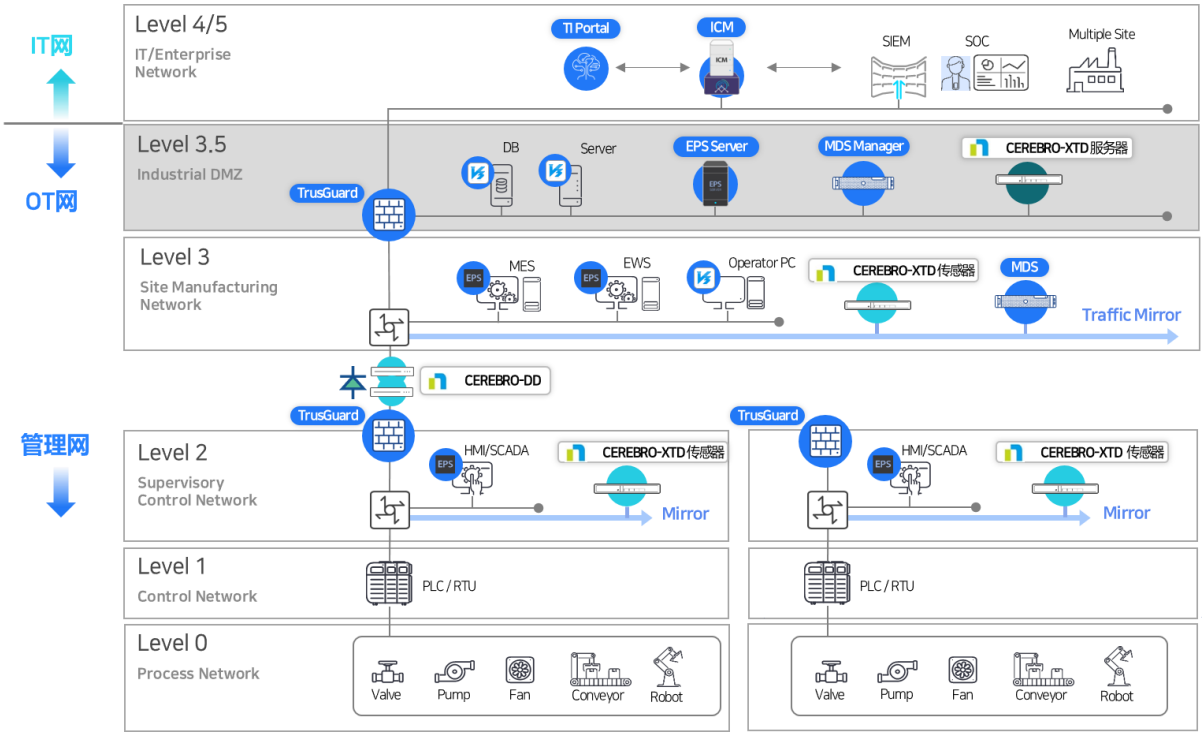
NAONWORKS首席执行官Jungyeong，Lee表示：“CEREBRO-XTD将提供升级后的OT网络可见性和威胁检测功能，将在保护担心勒索软件等安全事件的客户数字化转型环境中扮演重要角色。”

AhnLab产品服务企划部部长Changhee，Kim表示：“在OT环境中，‘攻击面’的范围从网络到端点越来越扩展。对此，‘CEREBRO-XTD’专注于扩大OT环境中的各种资产和设备的可见性范围，并提高分析与响应能力。”

满足适合用户环境的 OT 安全需求

近年来，针对工业设施和社会基础设施的安全威胁日益增多，造成的损害也愈加严重。特别是，随着连接IT和OT的外部接触点的增加，容易受到安全威胁的OT系统正在成为各种网络攻击的目标。为了有效响应渗透到OT网络或在内部系统之间传播的安全威胁，需要构建专门针对OT环境的安全解决方案和涵盖IT-OT环境的集成安全系统。

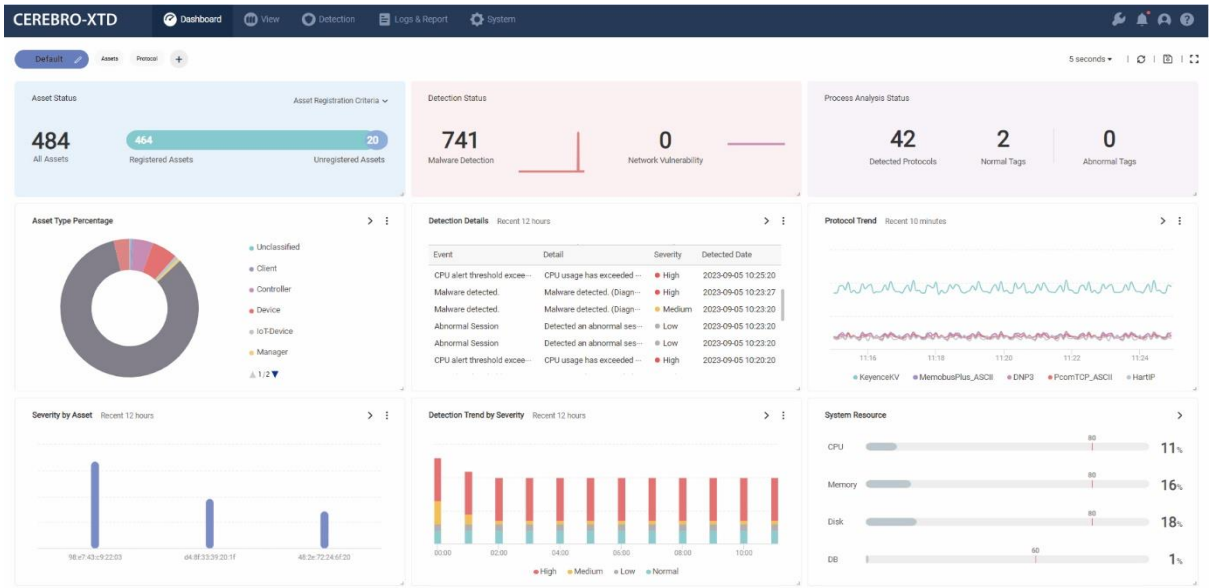
对此，AhnLab和NAONWORKS构建了兼具安全威胁检测&响应专业性与OT技术的“集成OT安全框架”，在OT网络普渡模型的所有阶段实现▲可见性、▲威胁检测、▲响应，从而提供全面安全。两家公司能够灵活提供多种解决方案以满足客户需求，并通过联动各产品而产生的协同效应实现差异化。



【图1】AhnLab-NAONWORKS“集成OT安全框架”

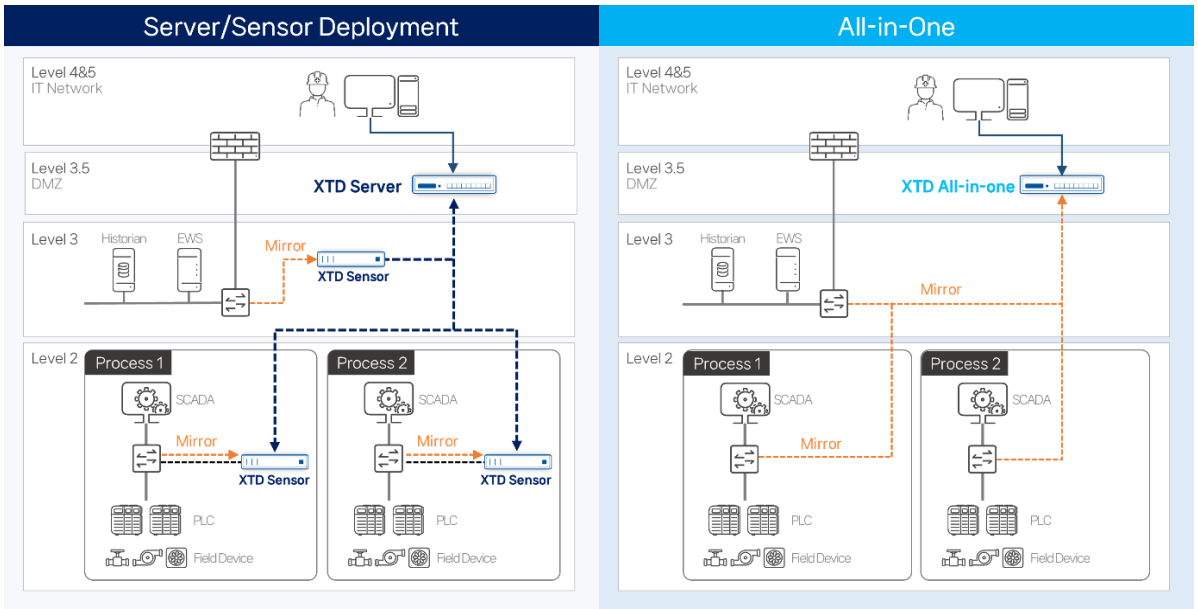
CEREBRO-XTD是“集成OT安全框架”的主要解决方案，可提供集成OT网络可见性，并实时检测安全威胁和异常行为。考虑到OT环境重视易用性的特点，它会以不影响设施运行的“被动监控”方式运行，从而增加了运行稳定性。

通过仪表板直观显示可见性信息和威胁检测信息，使用户能够实时查看情况。此外，通过用户仪表板设置，管理员可以创建单独的仪表板和微件来配置需要额外确认的信息。



【图2】CEREBRO-XTD仪表板

从结构上看，CEREBRO-XTD由中央服务器和每个流程的传感器组成。为每个流程安装的传感器可分析镜像流量并将检测结果发送到中央服务器，届时中央服务器会分析收集到的信息以提供可见性和威胁信息。此外，根据环境的不同，还可以采用传感器和服务器相结合的“一体式”配置。



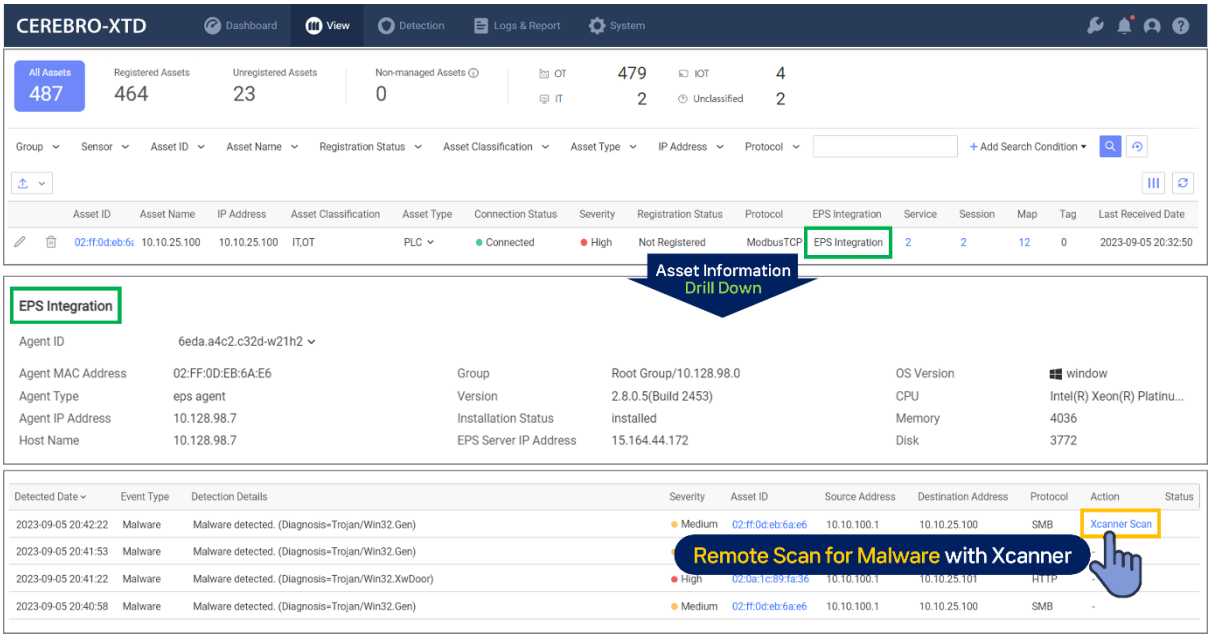
【图3】CEREBRO-XTD结构

一般情况下，为每个流程构建传感器并连接到中央服务器的“传感器/服务器配置”通常用于由多个流程构成的环境。另一方面，由一体式服务器集成多个流程流量的“一体式配置”则适用于由较少流程构成的环境。

通过端点安全集成和威胁追踪，进一步加强了功能

传统CEREBRO-IDS的功能包括：▲提供IT/OT主要资产和网络会话的情况及拓扑（topology）图等集成可见性；▲检测恶意代码入侵、有害流量、漏洞等各种安全威胁；▲深入分析OT协议和基于机器学习的异常控制检测；▲与第三方（3rd Party）控制平台联动等。

全新推出的CEREBRO-XTD在原有功能的基础上新增了▲通过联动AhnLab EPS提供从网络级到OT环境端点区域的详细资产信息，▲通过联动AhnLab Xcanner远程检测恶意代码等与AhnLab OT端点安全解决方案的链接功能，实现了真正的“端点和网络集成安全”。

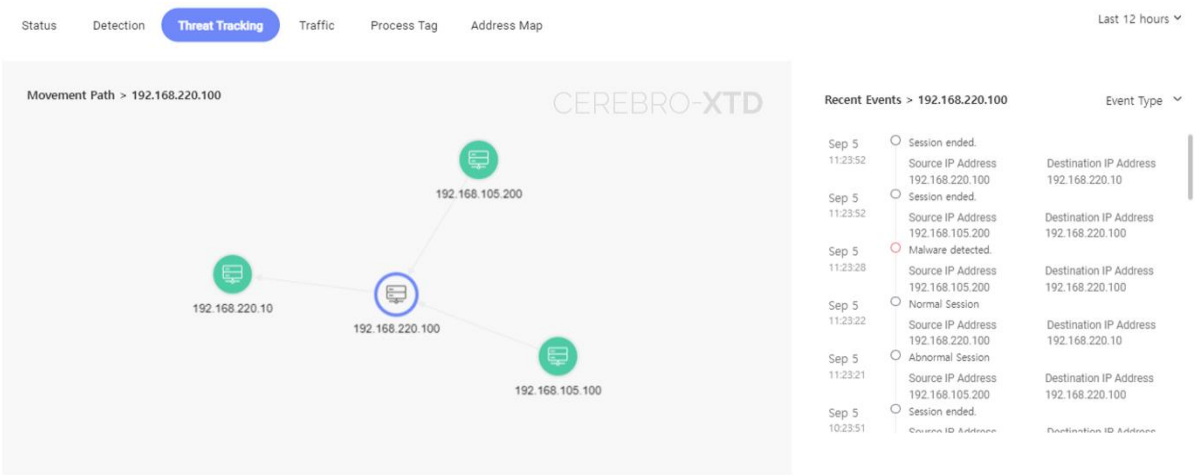


【图4】CEREBRO-XTD与OT端点安全解决方案的联动

首先，通过连接专门针对专用系统的安全解决方案“AhnLab EPS”，可见性可以扩展到连接到OT网络的端点。普通的同类解决方案基本上只提供至网络区域的资产状态。而CEREBRO-XTD通过与AhnLab EPS连接，除了网络区域数据，还可以提供连接到OT网络的服务器和工作站（Workstation）的操作系统补丁版本等详细的端点信息。

此外，还可以通过与AhnLab Xcanner（专门针对专用系统的诊断和修复解决方案）连接来扩展恶意代码扫描范围。在网络区域进行首轮恶意代码扫描后，能够对位于端点区域的可疑系统再次执行恶意代码扫描。此外，大多数同类解决方案只执行到检测流程，而该产品还能在扫描后进行修复，从而实现主动响应威胁。

产品还添加了“威胁追踪（Threat Tracking）”功能，通过该功能可逆向追踪所检测到威胁的分发路径，提供相关威胁信息。通过该功能可以确认传播攻击的先前分发站点，从而识别攻击的传播和移动路径。由此，用户可以确认已检测威胁事件的分发路径及最先发生事件的资产等威胁之间的联系，进而执行系统性的威胁响应。



【图5】CEREBRO-XTD威胁追踪功能

有关CEREBRO-XTD的更多详细信息可以前往NAONWORKS网站查阅。

► 前往NAONWORKS主页

AhnLab

安全月刊

https:// cn. ahnLab .com

https://global. ahnLab .com

https://www. ahnLab .com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ AhnLab .com
© 2023 AhnLab , Inc. All rights reserved.