AhnLab

White Paper

Unified Approach to OT Security

What Is OT Security?

What is the definition of "OT" that is commonly mentioned nowadays? OT refers to the operational technology environment of an industry and it covers a wide range of areas including industrial control systems (ICS) and is also connected or utilized together with Information Technology (IT). Additionally, OT security refers to the actions or systems with the goal of protecting OT environments mentioned above.

This prompts another question: What is the difference between IT security and OT security? This question also asks whether or not the IT security system can protect OT environments. To answer that question, we must first understand the essence of IT and OT and the differences between the two.

The most basic answer lies within the terms themselves. While IT security focuses on "information," OT security focuses on "operations." Although the two may not seem too different at first, this difference leads to fundamentally different approaches.

First, let us examine IT and OT security in terms of the three pillars of cyber security: confidentiality, integrity, and availability. All of them are essential aspects of security, but they have different priorities. Typically, in IT security, the highest priority is given to confidentiality followed by integrity and availability, thus being abbreviated as "C.I.A."

As for OT security, it is more important to prioritize availability and then integrity and confidentiality, thus being abbreviated as "A.I.C." One might ask why the two types of security differ in their priorities, and the reason is actually quite simple: computers can be rebooted, but industrial facilities can never stop running.

IT and OT environments are also comprised of different machines. As already known, the IT environment is composed of devices like desktops, laptops, mobile, and servers while there are industrial control systems added in the OT environment. The exemplary ICS machine is a programmable logic controller (PLC) that issues commands to pumps, valves, and robot arms in facilities.

All in all, there is an essential difference between IT and OT environments and organizations should consider both IT and ICS securities to protect their businesses.

OT Security Breach Cases

Until now, the importance of security in the OT sector has been relatively understated due to the closed nature of the environment with strict control over external access. Yet as digitalization rapidly advanced for OT, more areas became intertwined with the IT sector, leading to an increase in attacks against OT environments with the scale of damage growing as well. In fact, OT environments tend to have multiple vulnerabilities as they often operate systems that are not just 10 years old or more, but are also outdated with insufficient patches applied, hence the reason damage from cyberattacks can easily be spread.

The recent major OT security incidents have been focused on the manufacturing industry. There have also been cases targeting social infrastructures such as power plants and energy sectors. The types of attacks against OT environments can largely be classified into two categories. The first type is done by applying attack techniques from the IT environment to the OT environment. There has been an increasing trend of infecting OT environments with ransomware in the same manner as in IT environments, along with malware infections that exploit the residual vulnerabilities from inadequate internal system security patches. The second type involves modifying control commands to disrupt the operation processes. Let's examine key examples of both attack types.

First, there was the case of the WannaCry ransomware infection at the Taiwanese semiconductor company TSMC in 2019, which forced TSMC to shut down its factories for approximately 48 hours, resulting in significant financial losses. The ransomware infection at TSMC initially began due to the use of an infected USB device within the internal OT network, which quickly spread through the "Eternal Blue" vulnerability. The ransomware then caused further damage by propagating to other overseas factory locations that were connected to the affected factory.

The second example case is the hacking incident at the water treatment facility in Oldsmar, Florida. The attacker infiltrated the OT network and extorted account credentials and control facility connection information by planting malware on a website that was likely to be visited by the facility administrator. They then attempted to manipulate the concentration of sodium hydroxide by using the remote access program TeamViewer. Thankfully, an administrator who had been monitoring at the time noticed the unusual mouse movements and prevented the attack. Nevertheless, this incident could have potentially led to a major terrorist act, changing the drinking water supply for thousands of citizens into lye water.

Understanding OT Security Threats

Malware strains that target OT environments often have the ability to self-propagate like computer worms and ransomware. They can either enter the system through the carelessness of users or through the connected IT network via the Internet. Unlike typical malware, those designed to attack ICS-related systems are capable of causing serious damage by leaking industry secrets or disrupting facility operations.

Then how are OT environments infiltrated? The breach incidents usually follow one of the two methods below.

1. Hacking

Systems within OT networks are normally separated from external access, but they are partially connected to systems in the IT network. Because the system is managed through remote control programs, it is important to prevent the leakage of any account credentials of remote control programs. Furthermore, caution should be exercised against possible insider threats from internal employees with malicious intent.

2. Malware - Worms, Viruses, Ransomware, Etc.

Malware infections often occur within OT networks due to not following established security protocols. Typical malware strains do not have the ability to attack OT environments, so they may not have a significant impact on system operations aside from causing issues such as increased traffic and system crashes. However, those that target specific OT or ICS environments are able to manipulate or damage data as the attacker desires.

Also, OT systems can be directly connected with storage devices such as USB drives. In principle, the maintenance personnel should scan all storage devices with anti-malware programs before they are connected to the production line system. However, if a storage device is used without proper scanning, it can lead to malware infections, such as worms or ransomware. There may also be a case where the storage device itself is infected from the vulnerable inner system and spreads its infection when it is connected to other systems. In extreme cases like the TSMC incident in Taiwan, malware with the self-propagation ability can infect and halt the entire production line.

Now let us look at the attack pathways. Most attacks targeting OT environments occur through the "IT network, "direct access (third-party), or supply chain.

1. IT Network

OT networks are usually difficult to attack directly due to being separated from external and Internet connections. However, internal systems in OT networks that are connected to IT networks can still be infected with malware through the IT network. Thus, the attacker will not directly target the OT networks themselves, but instead try to attack through the IT network. Because OT network systems also use common operating systems used in IT networks, such as Windows or Linux, malware can be used as in the same way it would be in an IT network.

2. Direct Access (Third-Party)

Partner companies that perform maintenance among other tasks often have direct access to systems within OT networks. If the attacker is able to place malware into storage devices and other utilities used by partner companies, they can gain direct access to the internal systems. However, since the threat actor cannot communicate externally, they must collect information about the system type and versions being used in the OT network to create a customized malware strain.

3. Supply Chain

Systems that are operated within OT networks are usually provided by specialized manufacturers. The attacker can target these companies to include malware in the programs that are being produced or replace installation files with ones that are infected with malware. The "Havex" malware which was discovered in 2013 is a notable hacking case where malware was injected into the installation file on a software manufacturer's website intended to operate within the OT network. Obviously, it becomes difficult to detect the infection if the software provided by the supply chain contains malware.

Understanding the OT Architecture

OT security has never been considered as a priority due to various reasons in the past, but it can no longer be ignored. As threats against OT environments continue to grow, it has become essential to focus on OT security for true manufacturing innovation. So how should an OT security framework be established in the current landscape?

It is essential to first understand the structure of an OT environment in order to establish an effective OT security strategy. The "Purdue Model" is often used as a reference when discussing OT security structures. In this model, the OT environment is divided into six levels ranging from Level 0 to Level 5.

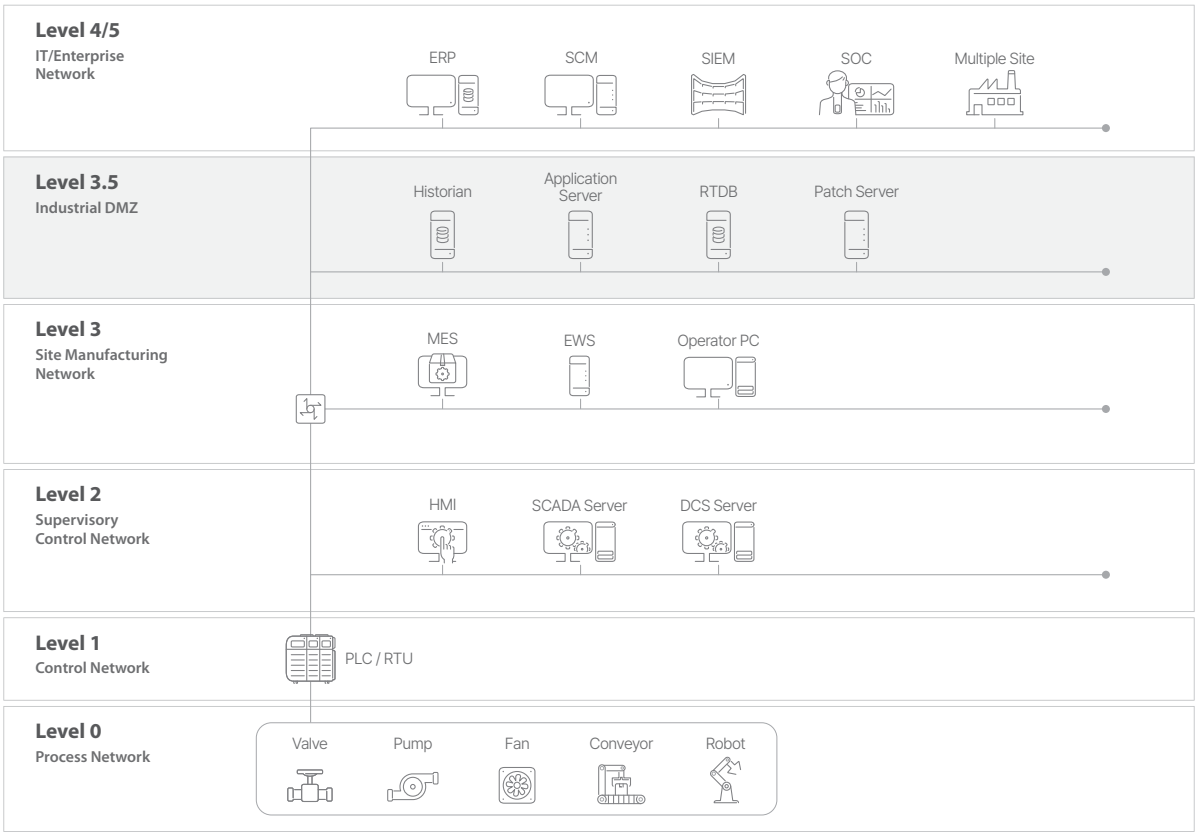

Figure 1. Purdue Model

Meanwhile, considering the characteristics of Level 3, an additional level of Level 3.5 is introduced to further refine the model. The description of each level is as follows:

Level 0: Process Network - The level for the physical devices operating in the facility. This consists of sensors that collect data from production devices such as valves, pumps, conveyors, and robots, actuators that operate by receiving commands from level 1 machines such as switches, etc.

Level 1: Control Network - Level 1 processes commands from Level 2 and delivers them to Level 0. It also sends information and data collected from Level 0 to Level 1. As mentioned earlier, the main devices include programmable logic controllers (PLC) and remote terminal units (RTU), responsible for issuing commands and controlling devices at level 0.

Level 2: Supervisory Control Network - Level 2 consists of systems responsible for remotely managing and operating lower-level devices. Key systems include supervisory control and data acquisition (SCADA) and human-machine interface (HMI). SCADA collects field data through PLC and RTU in level 1 and controls multiple devices simultaneously. HMI converts data collected from the field into an interface similar to bank ATMs to enable effective operation.

Level 3: Site Manufacturing Network - Level 3 manages the overall production system and enhances operation efficiency. This level consists of systems such as the manufacturing execution system (MES) for optimizing overall production activities, engineering workstations (EWS) for controlling devices, and product lifecycle management (PLM) for managing the product lifecycles.

Level 3.5: Industrial DMZ - Also known as the industrial demilitarized zone, this level is where the OT environment connects with the external IT environment. Real-time databases (RTDB) for saving sensor data, historians, application servers, and patch servers are all part of level 3.5. More attention has been drawn to this level with the increase in OT security breaches and focus on the importance of IT-OT converged security.

Level 4-5: Enterprise Business System - This level consists of resources generally used by companies in IT environments, such as enterprise resource planning (ERP), supply chain management (SCM), and customer relationship management (CRM). This is where company-wide businesses related to production are managed.

OT Environment Attack Process

From a security perspective, the levels 0 to 5 from the figure above can be categorized into the following table based on the network perimeter. The levels can largely be divided into the IT network (levels 4 - 5) and OT network (levels 0 - 3.5), and the OT network can be further divided into the control network (levels 0 - 2) and operational network (levels 3 - 3.5). The table below shows a summary of the structure and components of the OT environment levels and network types.

Level	Type	Key Components	Description
0	Control network (OT)	· Sensors · Actuators · Production devices	Devices performing field tasks
1		· PLC · RTU	Issues commands and controls field devices
2		· SCADA · HMI · DCS	Systems for remotely managing and operating field devices
3	Operational network (OT)	· MES · PLM	Overall production system management and operation
3.5		· RTBD · Historian · Application servers	Interfaces or buffer areas between OT and IT fields
4 - 5	IT network	· ERP · SCM · CRM	Manages the company-wide businesses related to production

Table 1. Summary of OT environment levels

Based on the table above, we will now examine the latest flow of attacks breaching OT environments.

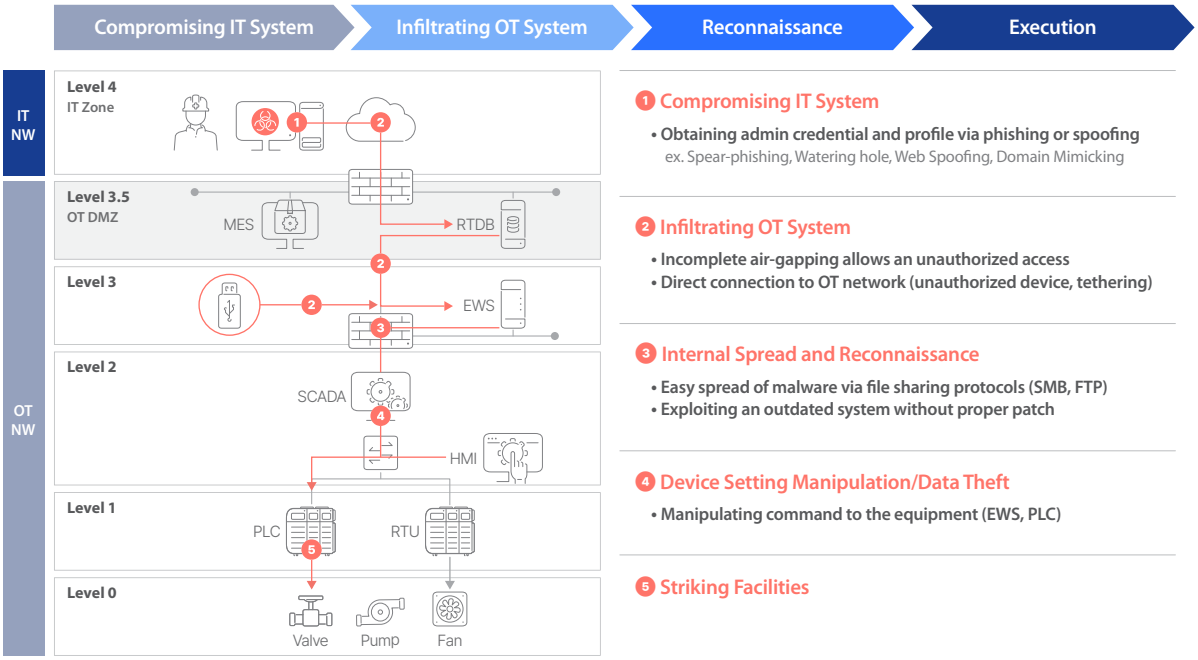

Figure 2. OT environment attack process

Security threats to OT environments often start from IT environments. There are incidents where unauthorized devices are directly connected to the OT network, but most incidents occur after the IT network has been infiltrated and connected to the OT network. OT environments are usually closed networks and isolated through air-gapping and network segmentation, which limits the attack surface. However, because OT environments are often connected to the IT network's management systems, the OT network system's connection and account credentials may be stolen by the attacker if the IT network system is compromised.

Attackers use a variety of techniques such as phishing and advanced persistent threats (APT) to breach the IT network that manages the OT network. They can then steal various profile information such as administrator account details, IP addresses, and URLs required for accessing the OT network system. Afterward, they can spot and exploit a weak network air-gapping policy or poorly managed area to infiltrate the OT network. Besides such cases, malware can spread to the OT network through unsecured USB drives and by connecting unauthorized laptops to the field device through mobile tethering which allows malware to bypass the OT network perimeter security.

Subsequent attack operations are relatively easy from the attacker's perspective. Malware strains are spread by identifying the target system. Due to the characteristics of the OT environment, SMB ports, remote file transfers, and remote accesses are frequently used. With the prevalence of outdated systems that are not properly patched, infection can spread rapidly. The attacker can make direct attacks by connecting to operational systems such as SCADA or HMI to issue abnormal control commands through PLC or manipulate the device settings.

This process can serve as a starting point for OT attacks. As mentioned earlier, OT security should not be viewed separately but considered together with IT security.

OT Security Requirements and Unified Approach

In terms of the approach, OT security is no different from IT security since it requires the same process of "identification > detection > response". However, to effectively respond to the latest OT security threats, it is important to prepare the IT & OT converged security system that can cover all aspects: the OT domain, IT and OT connection points, and IT domain. IT & OT converged security should be capable of securing endpoint, network, and ICS which follows the previously mentioned process. The figure below is a summary of the entire process and the requirements for each security domain.

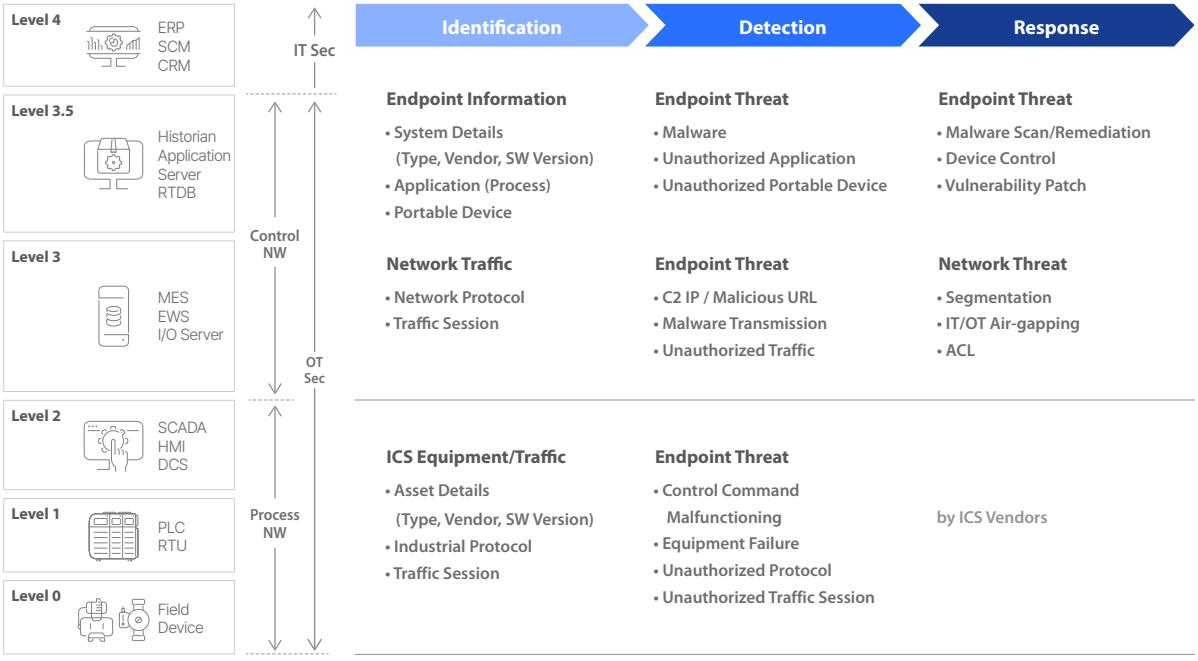

Figure 3. OT security process and requirements for each security domain

A. Identification

In IT & OT converged security, the "identification" refers to securing transparent visibility on assets that are in operation and relevant information. Visibility is necessary in OT environments because it establishes the foundation for effective OT security. There are various assets with long lifecycles in OT networks, making it a challenge to centrally manage their locations, statuses and network communications. This means if each asset is not precisely identified, it becomes difficult to detect and respond to security threats or device malfunctions that may compromise availability.

The standard of visibility can be divided into asset perspective and network perspective. The asset perspective includes visibility for various devices on the control network and different servers or workstations on the operational network. The network perspective includes visibility for network sessions between each asset and the various IT/ICS application protocols being used.

Due to the characteristics of OT network environments where asset or network changes seldom occur, identified elements can be used as a baseline to detect unidentified security threats and abnormal activities.

When examining control networks based on the OT network, the asset information such as asset types, vendors, software versions, as well as industrial protocols and traffic sessions of devices must be monitored. The ability to standardize different industrial protocols that are mixed together in order to analyze them is particularly essential.

Moving on to the operational network, there are security requirements that exist for both endpoint and network domains. First, the visibility of system information must be secured in the endpoint domain. System information refers to various details including system types, vendors, and software versions. Also, it is required to identify the applications, processes, and removable devices that are being used across the entire operation. As for the network domain, it is necessary to monitor network protocols and traffic sessions.

B. Detection

After securing visibility through identification, all present threats and abnormalities in the OT environment must be detected.

First of all, abnormalities in ICS machines within the control network must be checked. Comprehensive monitoring is required to check for control command malfunctions, device failures, the presence of unauthorized protocols and traffic sessions to secure the stability of the facility at all times.

In the operational network, detecting malware from the endpoint is required by default. The presence of any unauthorized applications and removable devices must be checked as well. In the network domain, continuous detection of threats such as C2 IPs, malicious URLs, malware transmissions, and unauthorized traffic is required.

C. Response

Response refers to finding the most optimal countermeasure based on the identified and detected information to minimize the damage to operations. Responding to threats against ICS machines in the control network requires support from the facility manufacturers first due to their specialized nature.

However, when it comes to operational networks, proactive threat response is possible. If an endpoint security threat is detected, a malware scan and remediation can be performed to minimize damage. Also, the entire security posture can be enhanced through device controls and vulnerability patches. Against network security threats, it is a standard practice to divide networks through segmentation to improve the efficiency of monitoring and threat response. Enhancing access control by protecting the OT environment through network air-gapping between IT and OT is also effective.

If we briefly examine the security solutions required to establish the security capability for each step mentioned above, anti-malware, whitelist-based application and device control solutions, and patch management solutions are needed. In the network domain, an intrusion detection system (IDS) for identifying assets and detecting threats is default, along with solutions such as OT-dedicated firewall and unidirectional data transfer. Finally, ICS machines require a solution that analyzes abnormalities based on deep packet inspection (DPI) analysis for various industrial protocols.

In order to operate IT & OT converged security with its various components, it is essential to go beyond point products and pursue systematic interoperation based on the unified security framework.

Our Unified OT Security Framework: Definition and Benefits

In July 2021, AhnLab acquired NAONWORKS, a company specializing in OT security and industrial protocol analysis, in response to the expanding demand for unified OT security. Starting with the gateway solutions for OT protocol standardization in 2017, NAONWORKS has provided the "CEREBRO" series, security solutions customized for OT and ICS, powered by OT protocol identification and analysis technology and open architecture-based edge computing platforms.

AhnLab's excellent IT security capabilities were further enhanced with the acquisition of NAONWORKS, allowing AhnLab's security threat detection, response, and analysis technologies to be integrated with NAONWORKS' industrial protocol analysis technology to establish a unified OT security framework. The following is a summary of our unified OT security framework architecture for each OT layer.

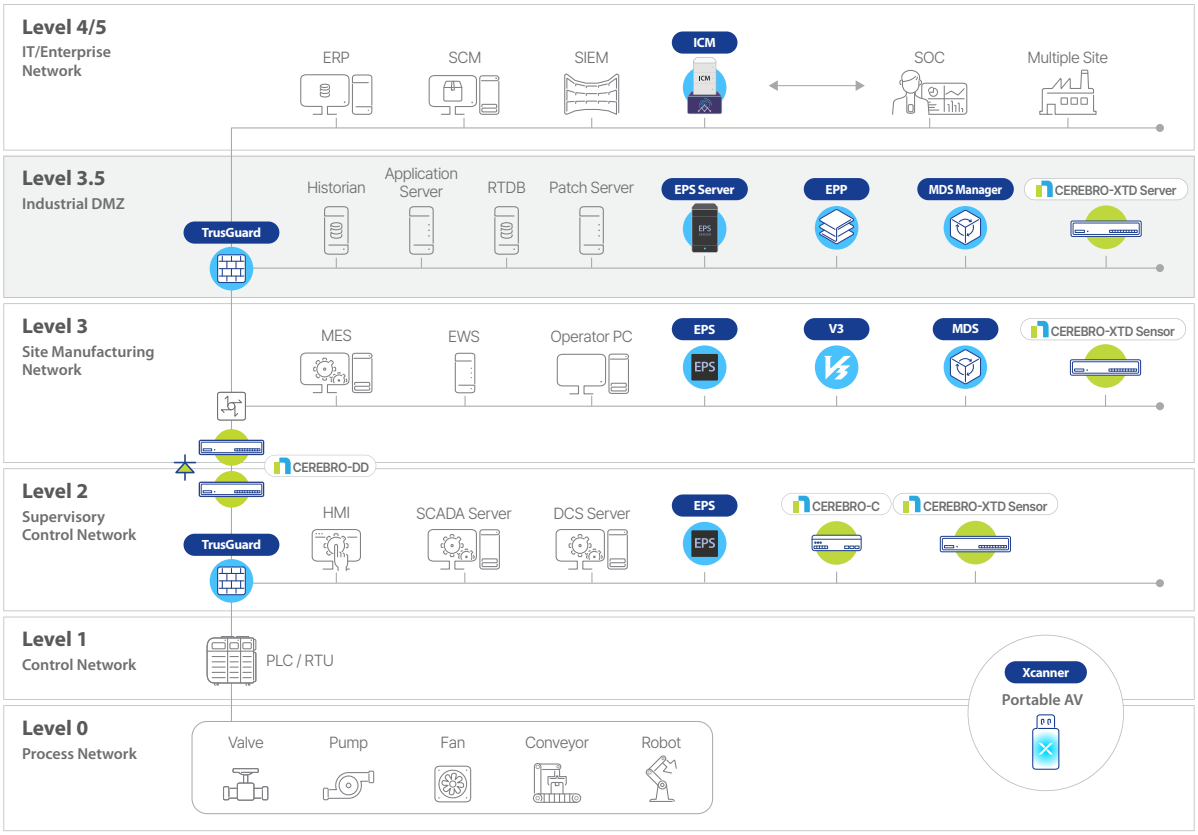

Figure 4. AhnLab's unified OT security framework

From a user perspective, the greatest value that comes with the AhnLab unified OT security framework is that an integrated security process of "identification > detection > response" can be materialized across all levels of the OT environment. AhnLab and NAONWORKS solutions create synergy while performing the necessary roles within the security framework. Also, integration is continuously enhanced from a platform perspective to improve the efficiency of user management across endpoint-network domains. The following figure is a summary of our unified OT security framework components and their roles in each security stage.

	Level 1 Monitoring & Identification	Level 2 Threat Detection	Level 3 Response	Level 4 Follow-up Actions
AhnLab ICM	• Unified Log Monitoring	• Log Analysis • In-depth Analysis Report	• Managing Lockdown Exceptions • Checking Agent Policy Status	• Checking Remediation Status • Applying Rest API Security Policy
AhnLab EPS	• Equipment Asset Identification	• Known Malware Detection	• Malware Scan • Blocking Unauthorized Process • Blocking Device Execution	• Lock Mode Activation • AhnReport Analysis Request
AhnLab Xcanner			• Malware Scan/Clean on PCs	
AhnLab MDS		• Un/Known Malware Detection • Network Anomalies Detection • Detect Behavior Analysis Evasion	• MDS Detection Verification • Pinpoint Analysis	
AhnLab TrusGuard		• Network Threat Detection • Unauthorized Traffic Detection	• Blocking ACL-based Unauthorized Sessions • Blocking Malicious Traffic	• Firewall Policy Settings • Network Segmentation
CEREBRO-XTD	• OT Asset Identification • Traffic Identification by Asset	• Malware Propagation Detection • Malicious Traffic Detection	• Threat Detection/Response Alert	
CEREBRO-C	• Protocol Identification		• Protocol Conversion	
CEREBRO-DD	• Protocol Identification		• Unidirectional Data Transfer	

Figure 5. Security components and their roles at each level

In summary, AhnLab can provide a variety of solutions to protect OT environments in the endpoint and network domains, while NAONWORKS has solutions for industrial protocol analysis and unidirectional data transfers, with the synergy between the solutions maximized through joint development.

Roles of Solutions within the Framework

Then, exactly what sorts of roles do these solutions in the unified OT security framework perform? The information from Figure 5 will be looked at in detail for each solution.

AhnLab EPS

AhnLab EPS is our flagship OT endpoint security solution, used in various global and Korean manufacturing production factories for semiconductors, displays, and automobiles. Using AhnLab EPS' web-based management system allows efficient unified management of OT devices that are scattered throughout each facility. Additionally, it minimizes threats to the OT environment by only allowing authorized processes and devices to be run based on a whitelisting technology. As the administrator does not need to create a separate application allowlist, flexible management is possible without the burden of drudgery policy configuration.

EPS Intelligent Whitelist-based **EPS**	VS.	 Blacklist-based **Traditional Security Solution**
Proactive prevention	Response	**Post-response**
Only authorized applications allowed	Application Execution	**Any applications allowed**
No change	Engine size	**Continuous increase**
Low	Resource Usage	**High**
Very high	Security Level	**Medium**
No engine update needed (Update needed in EPS server)	Engine Update	**Regular engine update needed**

Figure 6. Comparison between AhnLab EPS and AV solution

Operation stability is guaranteed through malware detection and analysis performed on the central management server of AhnLab EPS. It is notable for being consisted of an EPS agent installed on the device system and EPS server for policy management and centralized monitoring. It also supports agent operation in various legacy operating systems across Windows and Linux.

At the end of 2022, AhnLab released an exclusive security solution for large manufacturing equipment called AhnLab EPS Relay, which fundamentally relays OT assets and AhnLab EPS servers to enhance visibility and reinforce central management capabilities. With AhnLab EPS Relay, it is possible to secure visibility by viewing information such as the quantity and types of assets within the network and security statuses that could not be easily checked with existing OT security solutions that check assets only based on network packets and protocols.

CEREBRO-XTD

CEREBRO-XTD was jointly developed by AhnLab and NAONWORKS to provide comprehensive visibility of OT networks and detect security threats and abnormal behaviors in real time. As OT environments prioritize availability, it enhances operational stability by using the passive monitoring method to avoid affecting facility operations.

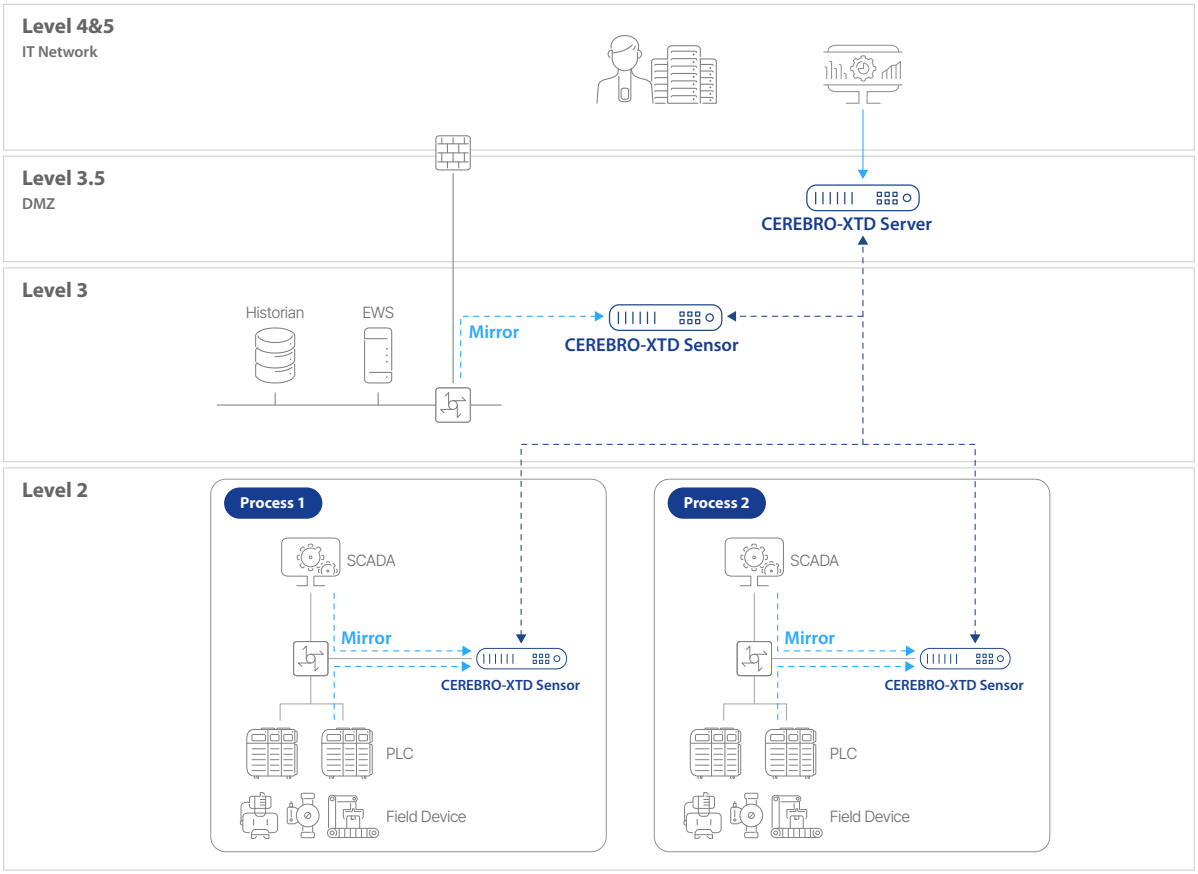

Figure 7. CEREBRO-XTD operation structure

CEREBRO-XTD features the ability to integrate with AhnLab's endpoint security products, providing endpoint visibility along with malware detection and remediation. It can also identify multiple OT protocols and deliver detection and analysis capabilities for abnormal control logic with the DPI analysis technology.

Typically, OT solutions in the market only provide asset status up to the network domain. However, CEREBRO-XTD can be integrated with AhnLab EPS to not only provide network data but also detailed information about actual devices, such as the operating system versions, patch statuses and workstations connected to the OT network.

In addition, the scope of malware scans can be expanded when integrated with AhnLab Xcanner. When malware propagation or malicious traffic exploiting vulnerabilities is detected for the first time, a second malware scan can be executed on suspicious systems located in the endpoint domain. Also, unlike other OT solutions which only provide security threat detection within the network, CEREBRO-XTD can proactively respond to threats as it performs malware scans for threats at their sources.

Another feature is threat tracking, which traces back the distribution path of detected threats to provide more information. This feature identifies the previous distribution points from where the attack was propagated, allowing users to track the propagation and movement paths of the attack. With this feature, users can systematically respond to threats by checking how the threats are connected, such as the distribution path of the detected threat event and assets with initial threat occurrence.

AhnLab ICM

When operating multiple security products, one must alleviate security complexity and improve efficiency through a comprehensive collection and monitoring of various events from multiple security products. In this regard, AhnLab ICM provides a unified management for OT environments.

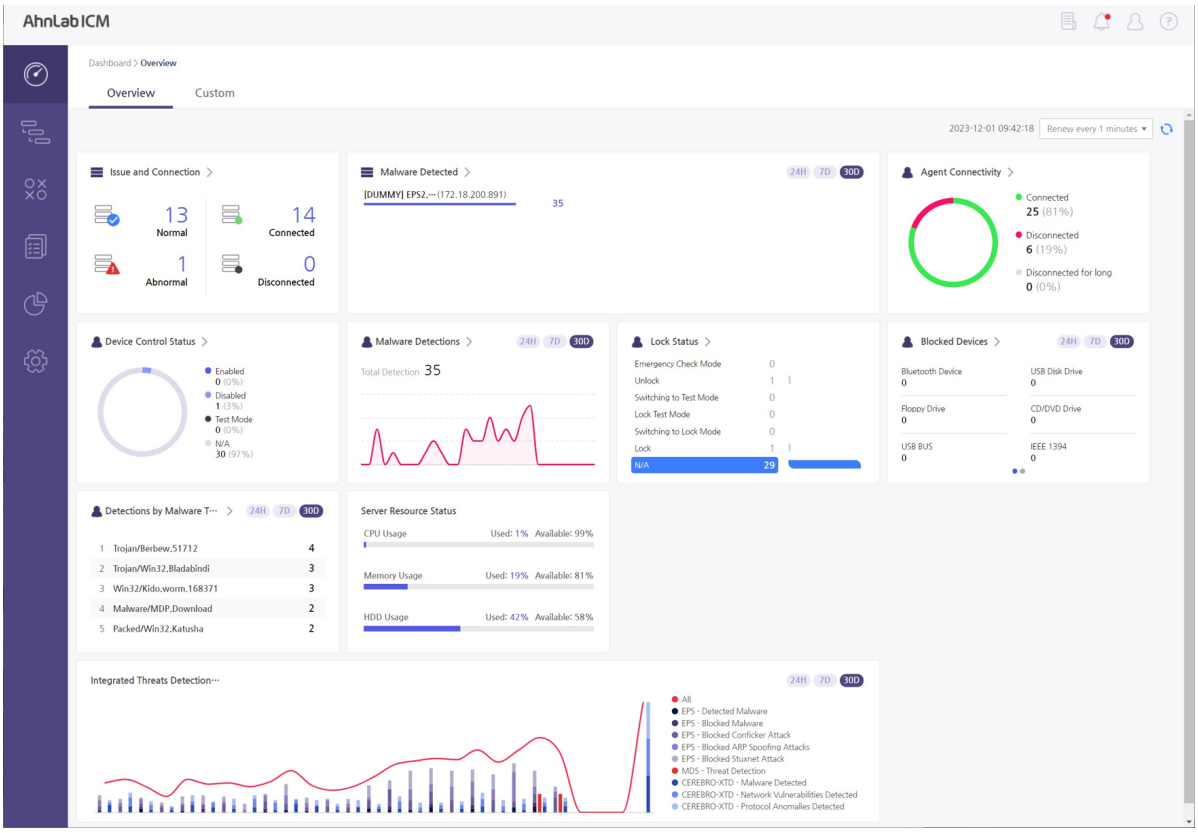

Figure 8. AhnLab ICM dashboard

Users can perform system monitoring and log analyses with an intuitive interface. Also, the system can be managed more effectively such as by taking appropriate actions through various reports and notification features and by reducing the total cost of ownership (TCO) for management. AhnLab ICM currently has the endpoint solutions AhnLab EPS, Xcanner, MDS, and the network solution CEREBRO-XTD for unified management with its scope expected to increase in the future. It also provides additional content analysis of collected threat information from various security solutions by integrating with AhnLab TIP, our threat intelligence platform.

AhnLab Xcanner

Considering the characteristics of OT environments, there are systems where agents cannot be installed. For such systems, the portable AV solution like AhnLab Xcanner can be used to perform malware scans and remediations. As the demand is rising for security measures for malware-infected systems in which real-time response is difficult, it helps the administrators to treat infected systems effectively. AhnLab Xcanner can also integrate with AhnLab EPS to allow the EPS server administrator to execute AhnLab Xcanner remotely and perform additional malware scans and remediations.

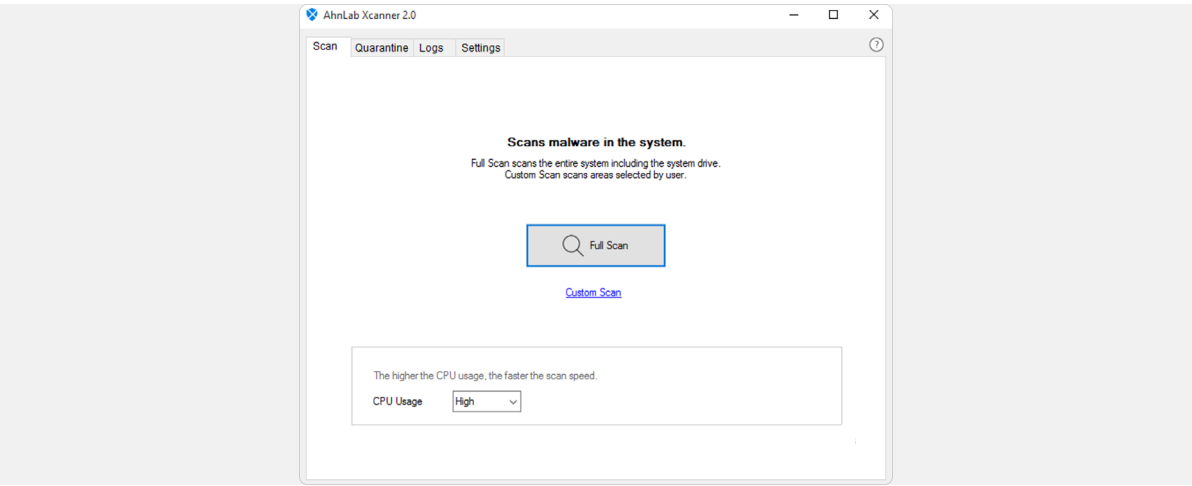

Figure 9. AhnLab Xcanner screen

The scan and remediation options can be configured on AhnLab Xcanner to allow responding appropriately based on operational situations. Users can also make effective use of the tool by setting certain folders and files to not be scanned. Additionally, since AhnLab Xcanner minimizes conflicts by not needing to remove existing security agents, scanning and remediation can be performed without causing a burden to the operation .

AhnLab MDS

As cyber threats continue to evolve, there has been a rise in APTs along with new and emerging variants of malware. Therefore, it has become paramount to be able to analyze and respond to unknown malware in addition to those already known.

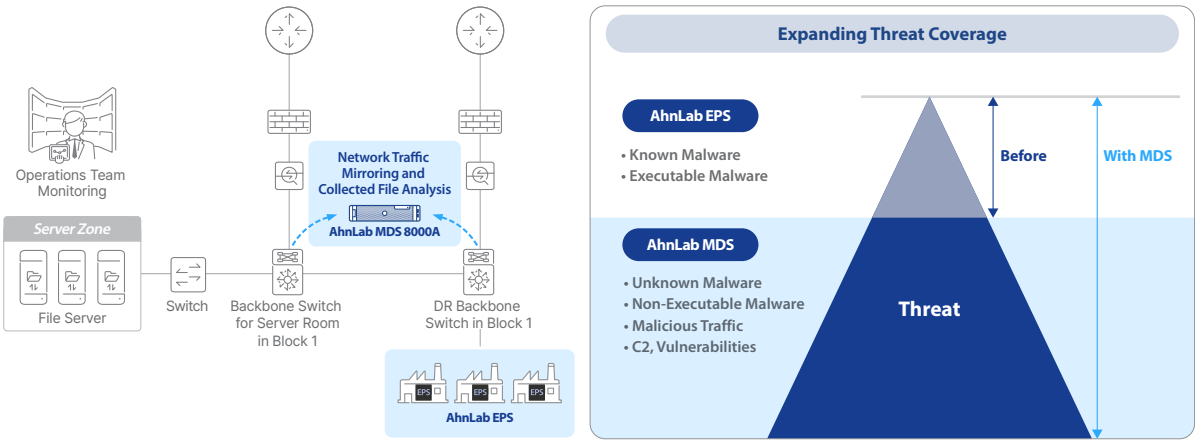

Figure 10. Expanding threat coverage by integrating AhnLab EPS and AhnLab MDS

AhnLab MDS, our sandbox-based APT solution, collects and analyzes files within the network traffic and performs dynamic analyses on unknown malware. Since it can also detect and analyze the attacker's C2 IP connections, AhnLab MDS provides monitoring for various security threats such as the path of malware spread within OT networks, C2, and vulnerabilities as well as offering remediation and response for infected devices.

All in all, when integrated with AhnLab EPS, AhnLab MDS can expand the overall threat response coverage to both known and unknown malware strains.

AhnLab TrusGuard

Our next-generation firewall takes on a crucial role in the OT network security. First, it is able to detect and block malicious traffic from the OT network perimeter and support secure communications in the form of IPSec/SSL VPN, in addition to features such as network segmentation.

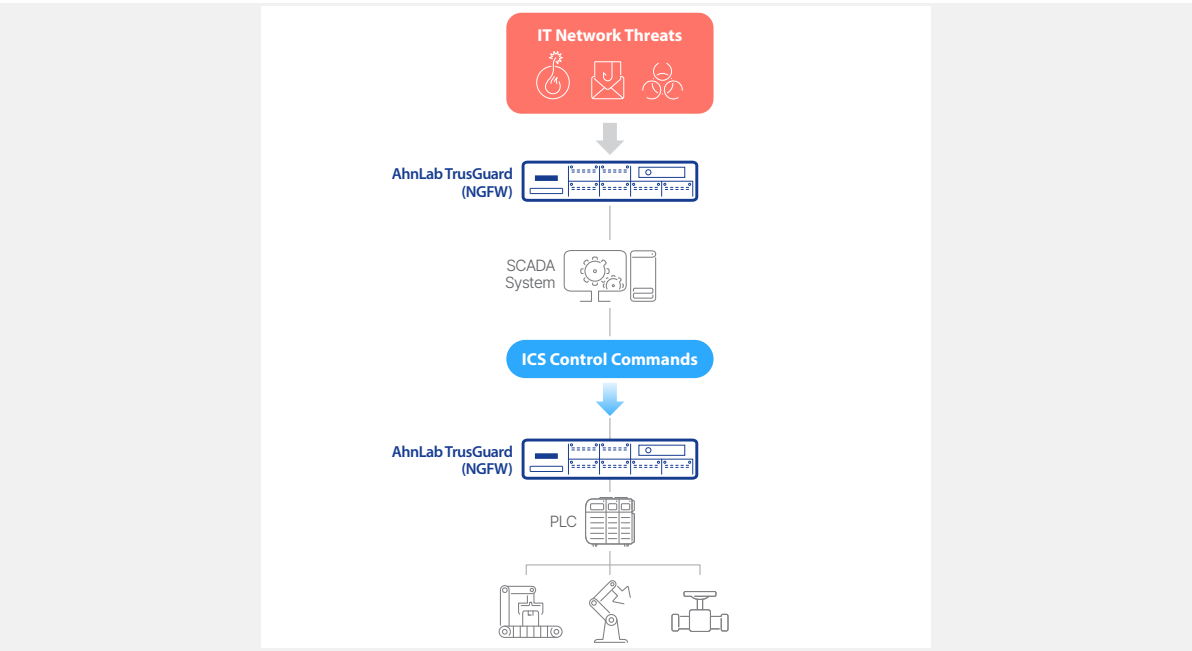

Figure 11. The role of AhnLab TrusGuard in OT security

Furthermore, NAONWORKS' ICS protocol analysis technology can be applied to AhnLab TrusGuard, allowing detailed control over industrial protocols within the OT network. More specifically, it is possible to identify and control individual protocols such as Modbus and DNP3 as well as function codes for more precise control.

CEREBRO-C

CEREBRO-C from NAONWORKS is an industrial protocol gateway for the unified management of OT networks. The security of the control network is enhanced by converting and delivering various ICS protocols into secure standard protocols such as OPC-UA and MQTT.

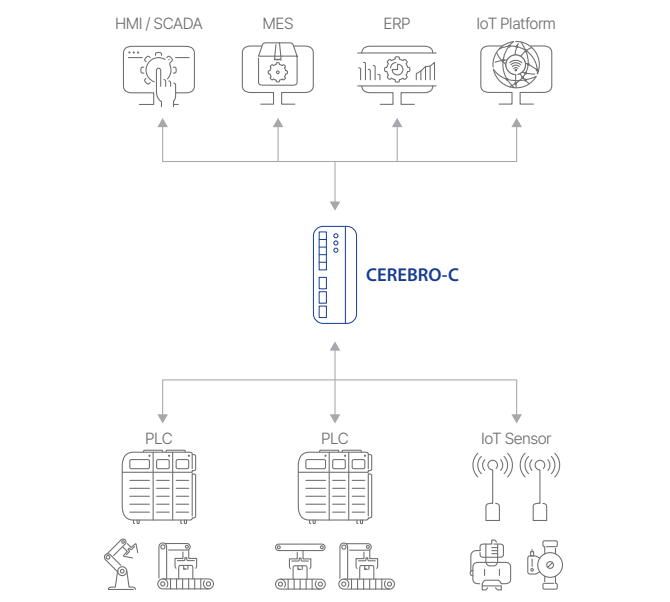

Figure 12. CEREBRO-C operation structure

CEREBRO-C features incredible compatibility with various device connections such as Fieldbus and Ethernet, integration with upper-level system interfaces, and support for Windows, Linux, container platforms, etc. If a new system is being built for data collection, integration, and device management, CEREBRO-C can solve integration issues from having different communication protocols without changing the existing network configuration.

CEREBRO-DD

One of the most important aspects of OT security is network air-gapping. This measure is put in place to prevent data leakage from OT networks and block malicious access such as malware from external networks. However, with the growing emphasis on the integration between OT and IT, there has been an increasing demand for secure data transfers between air-gapped networks.

The ability to connect data between networks with different security levels while also preventing external threats from accessing secure areas such as OT environment is available through physical one-way communications. CEREBRO-DD is a unidirectional data transfer solution that establishes a secure data transfer environment from OT to IT, providing complete protection of OT networks.

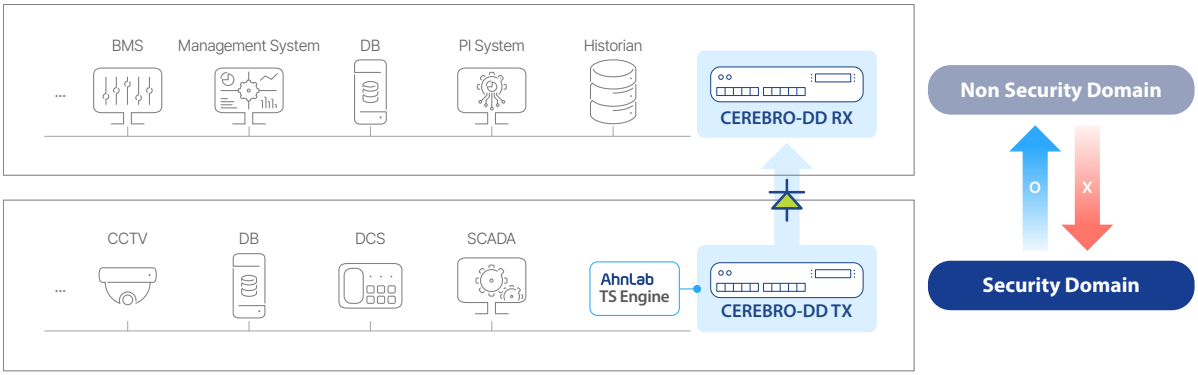

Figure 13. CEREBRO-DD concept (TX: transmitter server/RX: receiver server)

CEREBRO-DD utilizes undisclosed protocols for the one-way communication to improve security. It also applies AhnLab's anti-malware engine to perform comprehensive scans. Data stability is secured by performing policy, signature, and malware scans when transmitting data.

Conclusion

The security threats against OT environments are escalating on a daily basis. The scale of damage is greater compared to IT environments, and breach incidents can lead to social issues or significant losses for organizations. As a result, the interest in OT security is increasing every year. However, due to having different characteristics compared to traditional IT environments, it is difficult to implement security solutions into OT environments without compromising operations, a reason why many companies still refrain from taking proactive actions. Yet as more OT security incidents occur with every passing year, now is the time to actively consider OT security rather than passively observing.

OT security may still feel unfamiliar and technically challenging for readers. If so, just keep the following three points in mind.

#1. IT security must also be taken into consideration in order to protect OT environments.

Security threats against OT environments often originate from IT environments that are connected to the OT environment. If the OT domain is infiltrated, the damage can spread rapidly, hence the reason for IT & OT converged security.

#2. OT security requires the process of "identification > detection > response" by default.

There are rarely changes made to assets or networks in OT environments. Therefore, it is necessary to have a process that can make appropriate responses by securing the visibility of assets and detecting security threats through identification baselines.

#3. In order to secure OT environments, a unified OT security framework is necessary to cover all levels.

IT & OT converged security can be divided into the IT network, the OT operation network, and the OT control network. Each level requires specific security measures customized for its characteristics, and an OT security framework must be established by taking into consideration various management aspects and appropriate security solutions.

AhnLab has partnered with NAONWORKS to continuously improve its unified OT security framework to become the optimal OT security partner. As the importance of OT security becomes more prominent, we hope for more companies to establish a strong security system to create a safe business environment.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com