

OsecT: An IDS for OT



Introduction of OsecT



OsecT visualizes risks in industrial control systems and detects cyber threats and vulnerabilities, enabling early risk detection and preventing losses caused by factory shutdowns.

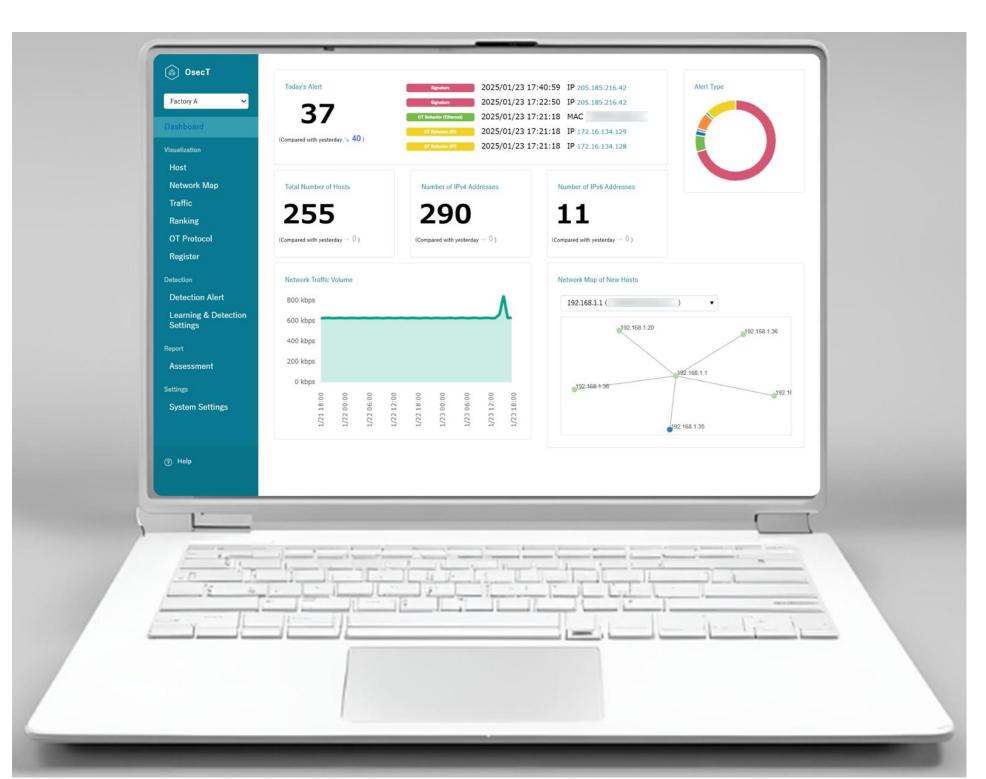
2 Main Functions

■ Visualization

Visualization of hosts and networks

Detection

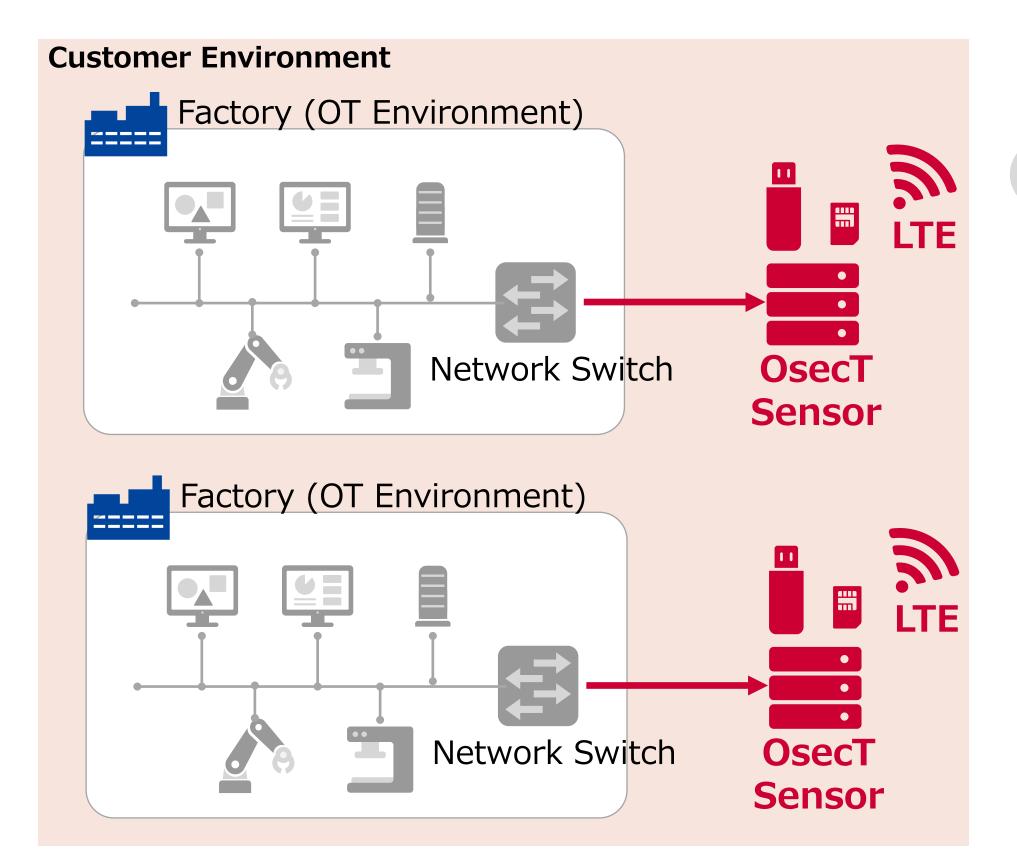
Detection of cyber threats through learning and analysis

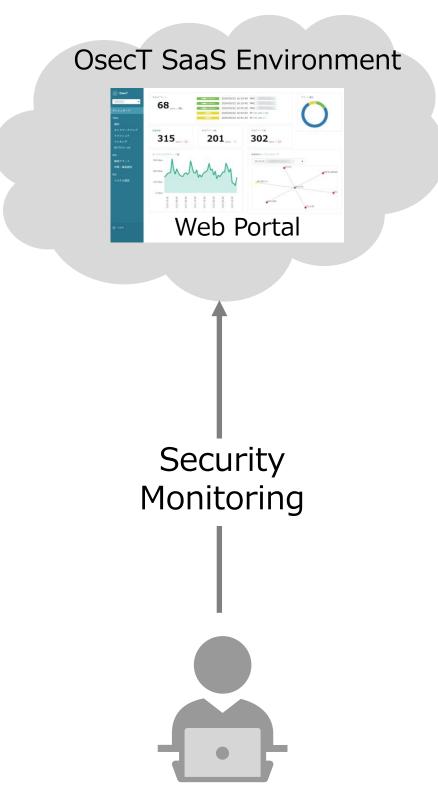


Structure of OsecT









Feature 1: Affordable as an IDS for OT



- Initial implementation cost is a fraction of that of competitor products (for the same number of units).
- Price is suitable for implementation even in small-scale network configurations.



First Year: \$8.800 (Initial: \$1,660, Monthly: \$595)

Second Year: \$7,140

※Price per set, excluding tax

Included in the cost:

- · Initial: Sensor hardware, LTE USB Dongle, SIM card
- Monthly: Web Portal usage, communication costs

Not included in the cost:

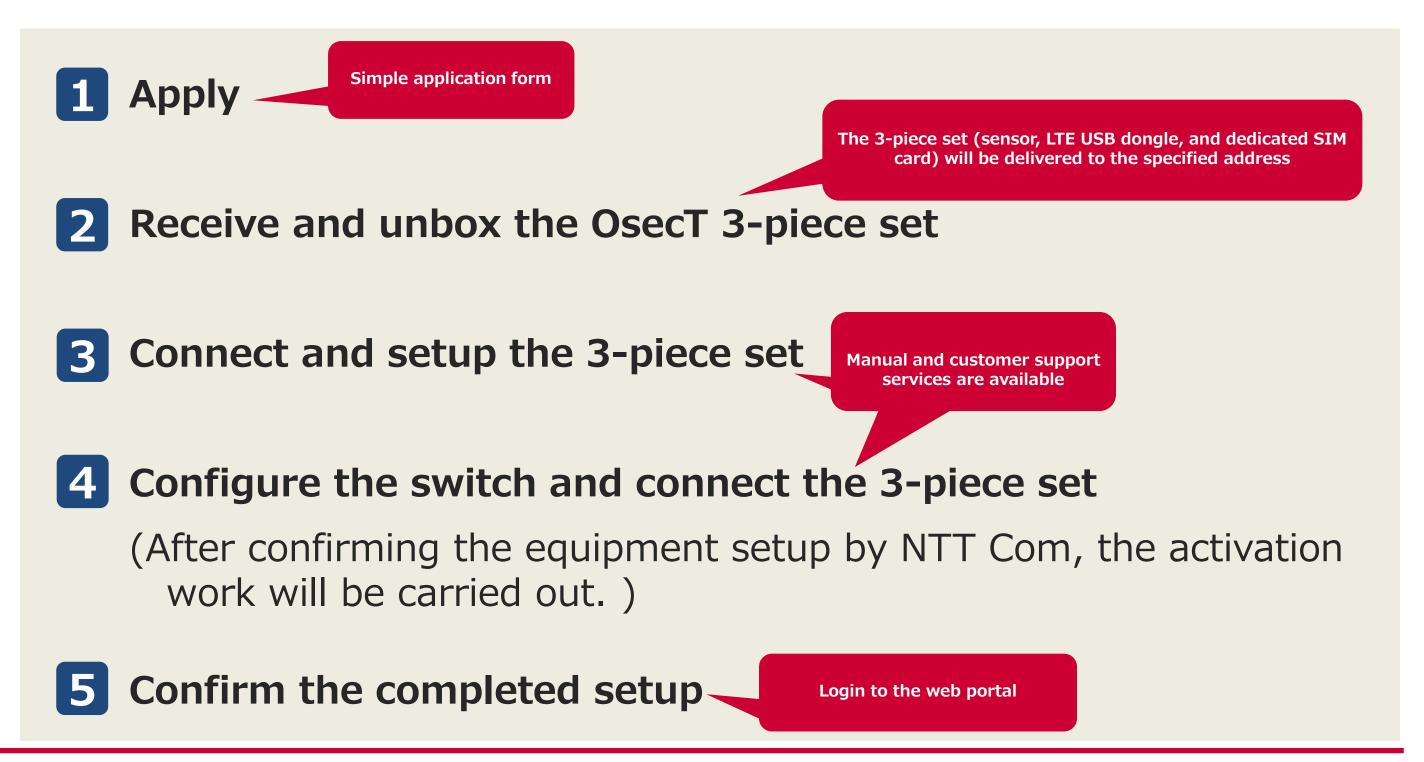
Implementation support, security operations/support, etc.

Feature2: Easy Implementation



- Simply connect the sensor device to the mirror port of a network switch
- Since OsecT sensor uploads the collected information using NTT's closed mobile network, no network design or VPN device installation is required



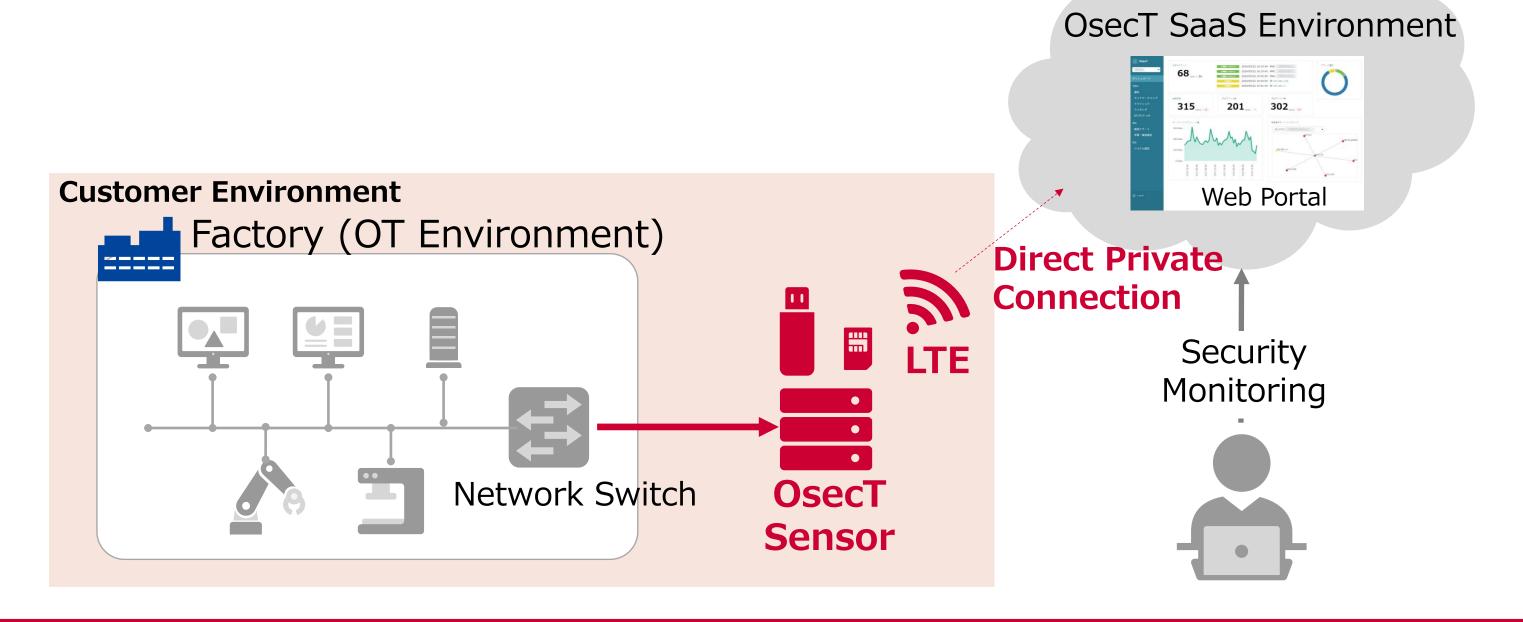


Feature 3: No Security Management Required



The web portal is centralized on SaaS

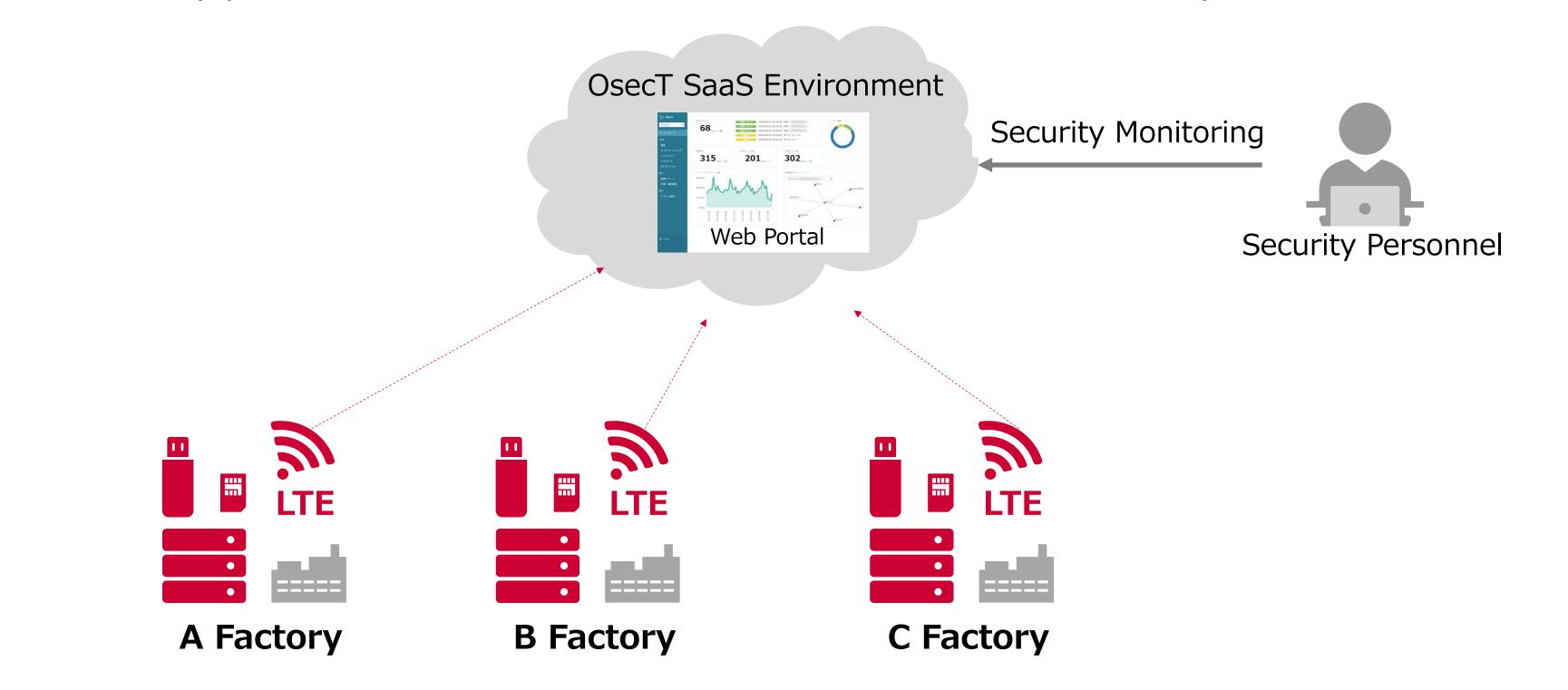
Communication from the sensor to SaaS uses our private network, so ASM (Attack Surface Management, management of areas that could be targeted by external attacks) is not required.



Feature 4: SaaS-based Service



- The security monitoring status can be checked on the OsecT SaaS environment's web portal.
- Security personnel at remote locations can also monitor each factory.





Introduction of OsecT Functions

Visualization -Host-

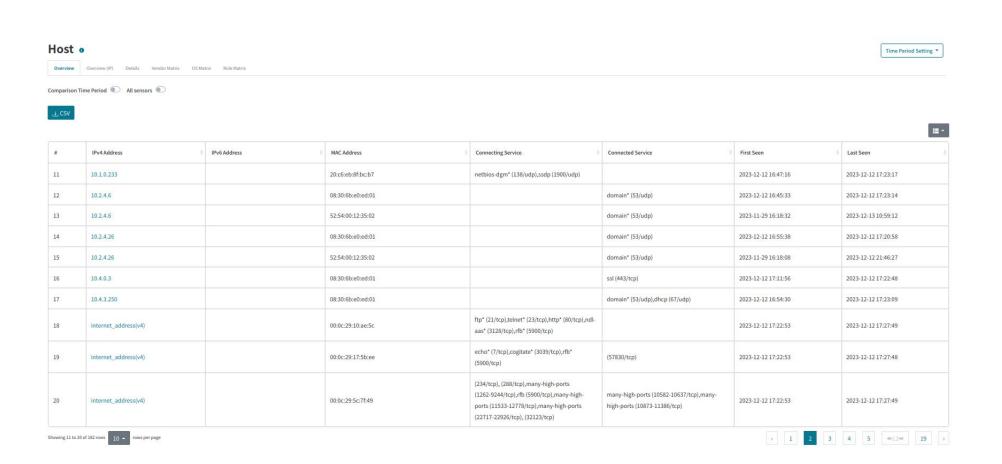


By visualizing hosts, network maps, and the configuration differences between two periods from multiple perspectives, a comprehensive visual understanding of the OT network environment can be gained, allowing for host management and the identification of newly connected hosts. This helps enhance security measures and improve response capabilities in case of an emergency.

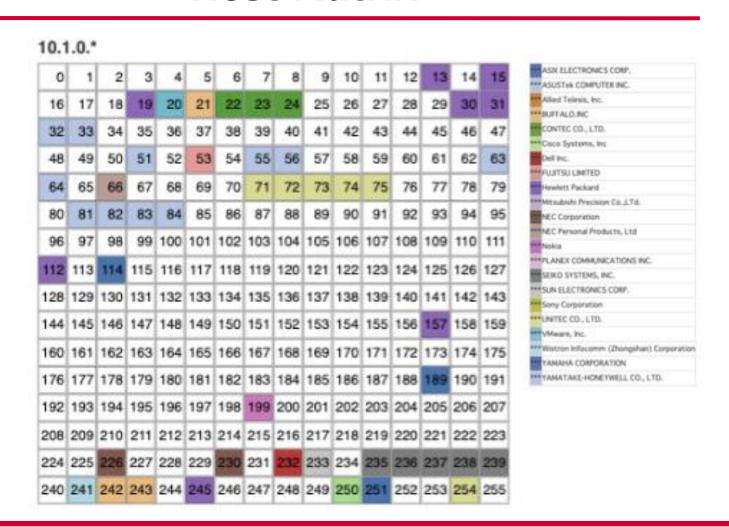
- Automatically generate an overview of host information
- Host overview can be exported as a CSV file and used as a register

- Visualize active hosts in a 16x16 matrix format
- Color-coding by vendor, OS, and role enables an at-a-glance analysis

Host Overview



Host Matrix



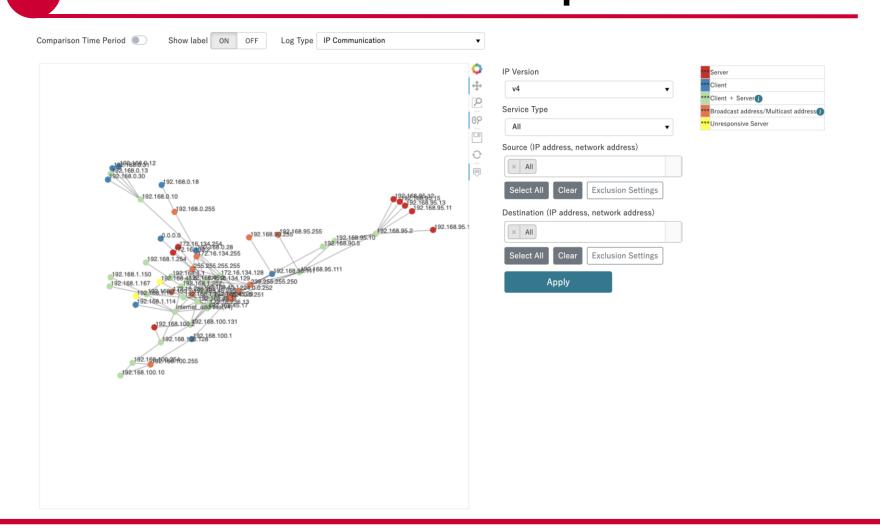
Visualization -Host · Network-



By visualizing hosts, network maps, and the configuration differences between two periods from multiple perspectives, a comprehensive visual understanding of the OT network environment can be gained, allowing for host management and the identification of newly connected hosts. This helps enhance security measures and improve response capabilities in case of an emergency.

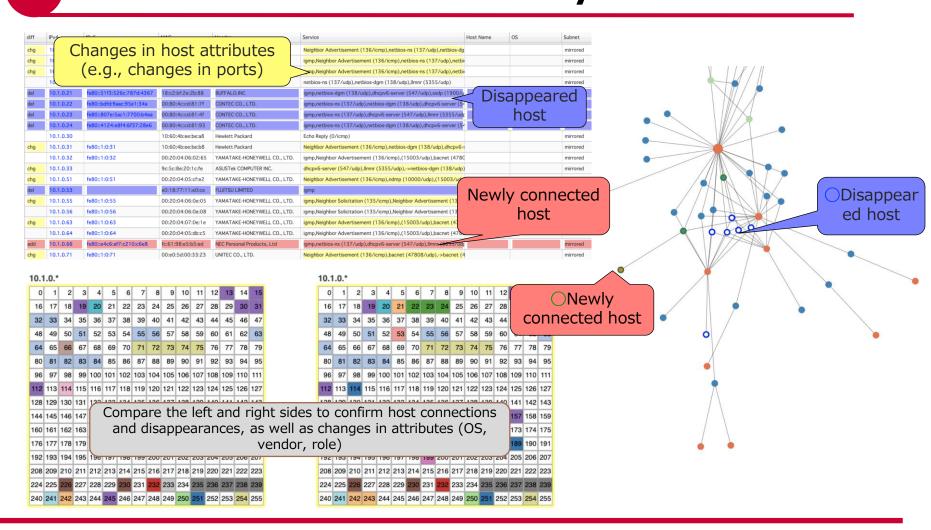
- Visualize host communication relationships in a map format
- Data being displayed can be exported as an image

Network Map



- Visualize configuration differences in hosts and networks between two periods
- Identify newly connected hosts

Difference Analysis



Visualization -Network-



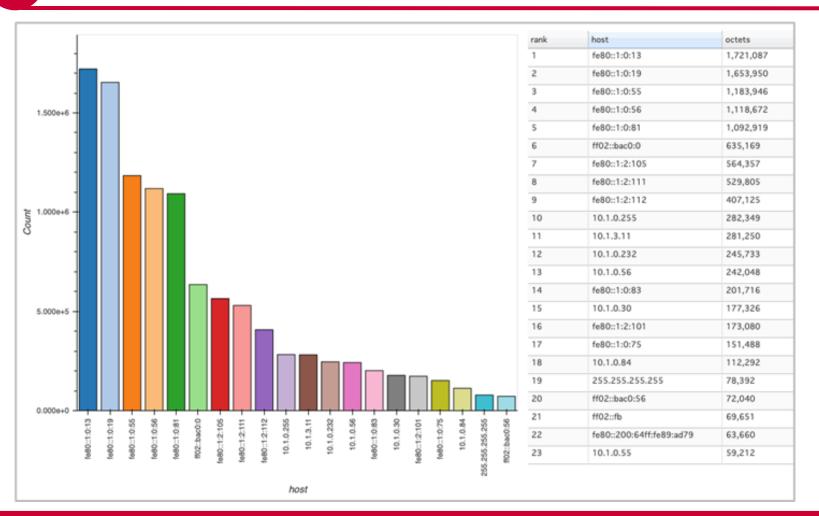
Trends such as host and service traffic volume and the number of connected hosts are visualized, and high-impact hosts within the network are identified, helping to enhance security measures and improve response capabilities in case of an emergency.

- Visualize network load (bandwidth usage)
- Detect bandwidth congestion caused by loops, etc.

- Visualize the number of connected hosts, hosts with high traffic, and services
- Gain insights into trends in the OT network



Ranking



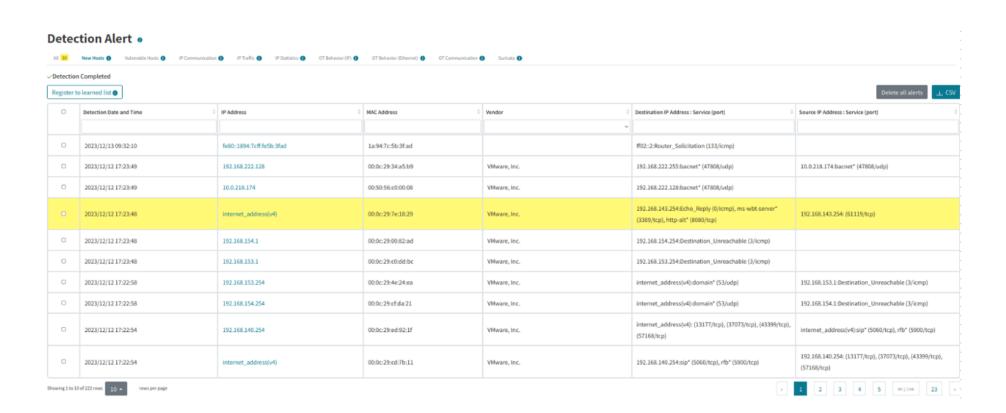
Detection - Prevention-



By detecting newly connected hosts, unknown communications, and hosts using unsupported OS, and sending alert notifications, we help customers take proactive measures for risk management and prevention.

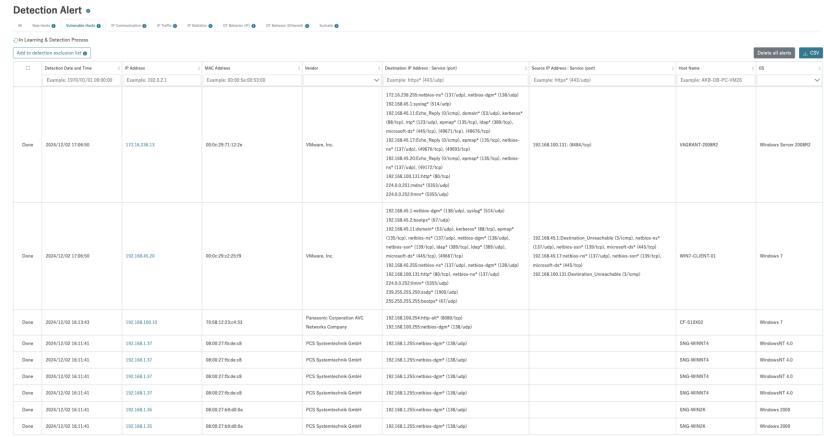
- Automatically learn host addresses within the network
- Quickly detect rogue hosts without missing any





- Automatically detect hosts using unsupported OS
- Detect high-risk hosts early without overlooking

Detection of Vulnerable Hosts



Detection -Early Identification of Anomalies-



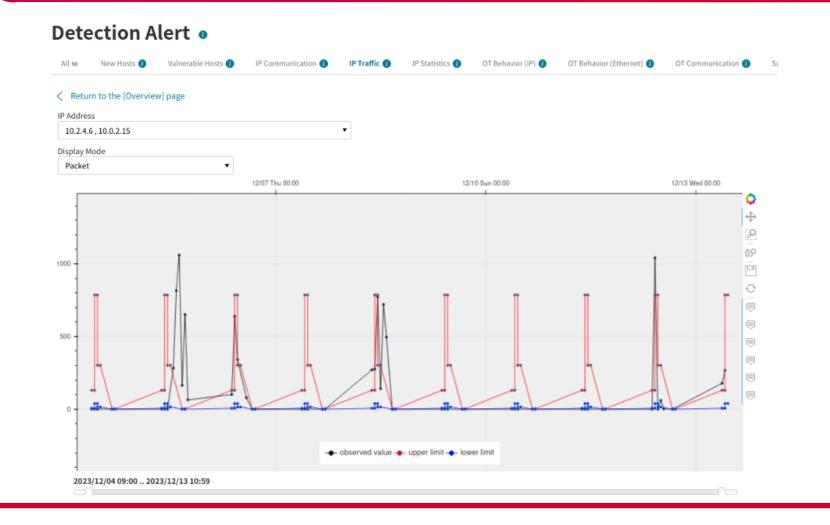
In the event of anomalies like malware infections, detecting their behavior (such as unexpected communications or changes in traffic volume) and sending alert notifications can help customers take prompt action and minimize the impact.

- Automatically learn communication data within the network
- Quickly detect unknown communications without missing any
- **Detection of Unusual IP Communication**

Detection Date and ···	Source IP Address	Source Port	Destination IP Addres···	Destination Port	Protocol
例: 1970/01/01 09:00:(例: 192.0.2.1	~	例: 192.0.2.1	~	<u> </u>
2025/02/13 16:58:43	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:54:16	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:49:42	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:45:16	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:40:42	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:36:16	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:31:42	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:27:16	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:22:43	100.121.126.96	25421	10.64.15.51	1812	udp
2025/02/13 16:18:17	100.121.126.96	25421	10.64.15.51	1812	udp

- Learn the traffic volume for each host pair during regular operations
- Automatically calculate thresholds for different time periods

Detection of Unusual IP Traffic



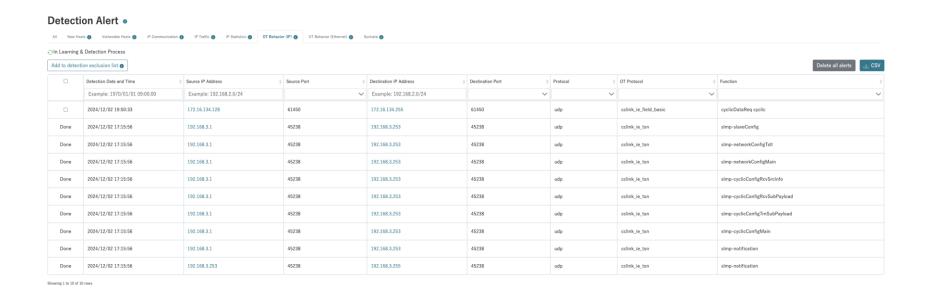
Detection -Early Identification of Anomalies-



By detecting and sending alerts for communications that match known high-risk patterns, we can help customers take prompt action and minimize the impact.

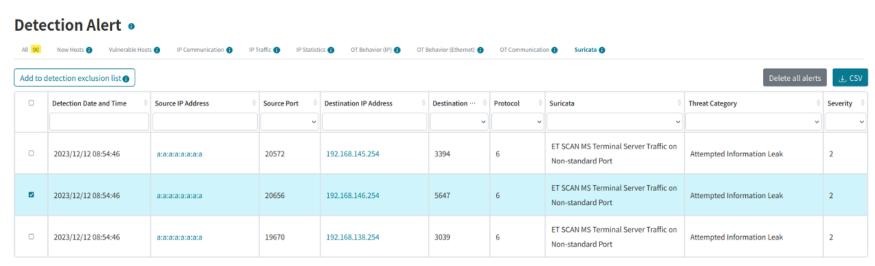
- Detect OT commands that affect the system
- Commands and hosts targeted for detection can be customized

Detection of OT Behavior



Detect communications that match known attack patterns

Detection of Signature



Showing 1 to 3 of 3 rows

Register Integration -Streamlined Host Management & Alert Response-

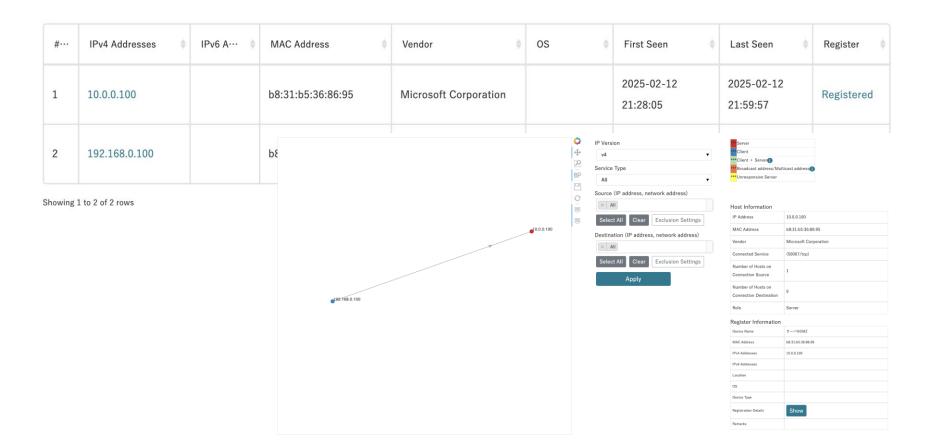


By importing register data from existing host management software, it can be integrated with various OsecT functions, helping streamline operations such as host management and detection of suspicious hosts.

Integrate host register information with Host Overview/Network Map

Display additional information such as host installation locations and dates

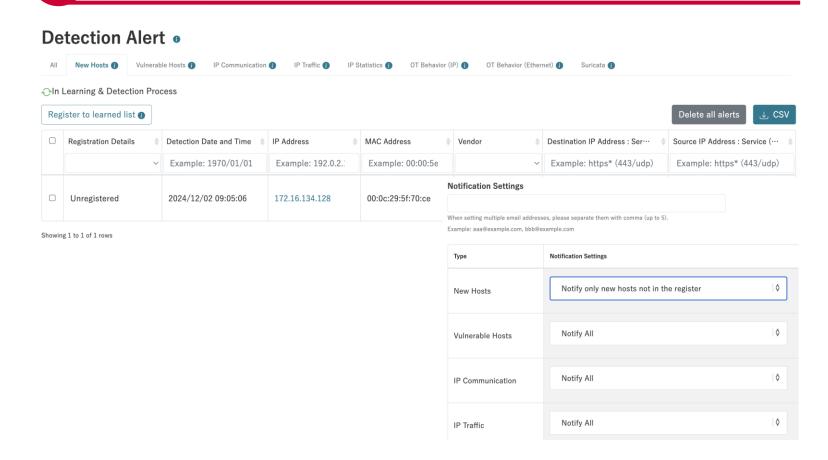
Integrate with Host Overview/Network Map



Integrate register data with New Host Detection function

Display register presence on the Alert UI
Set conditions for email notifications based on
host registration status in the register

Integrate with New Host Detection



Assessment

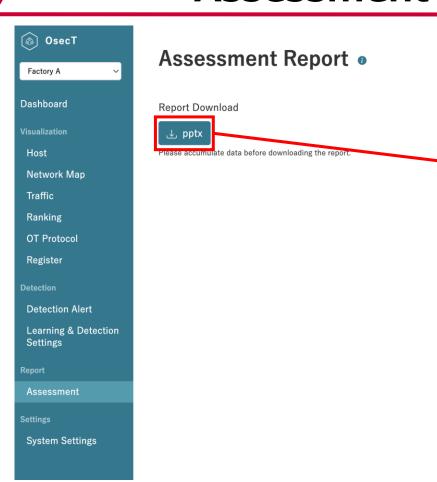


With just a single button, a visualization report of assets and risks connected to the network can be generated. The focused report helps prioritize actions for strengthening and enhancing security measures and improving response capabilities in case of an emergency.

Generate reports with just a single click

List hosts and those with unsupported OS versions

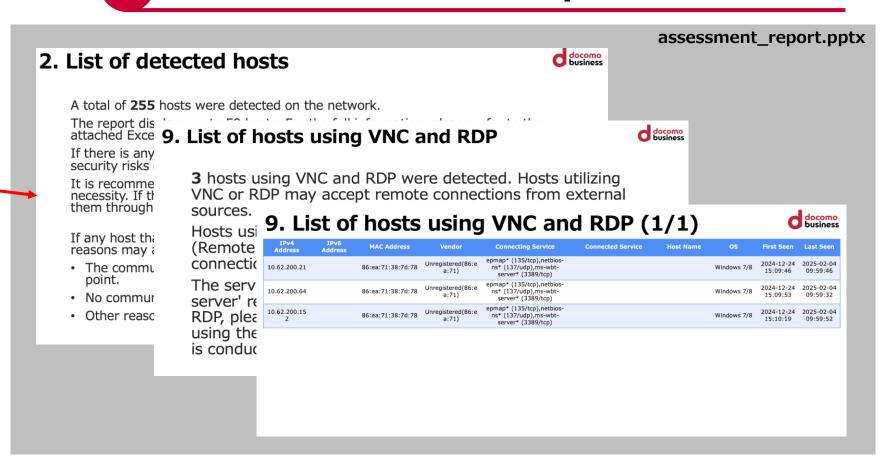
Assessment



Output in an editable PowerPoint format

Visualize traffic volume, plaintext communication, RDP communication, etc.

Assessment Report File





Service Details

Equipment provided (OsecT 3-piece set)



Sensor

Number: 1



Dell: Precision3240 Compact CTO BASE

Item	Specification			
Size	Height:188.1mm, Width:70.2mm, Depth:178.65mm			
Min. weight	1.71kg			
CPU	Intel Xeon W-1250			
OS	Ubuntu Server 20.04 LTS			
SSD	M.2 256GB PCIe NVMe Class 35 SSD			
Memory	8GB 1X8GB DDR4 2666MHz or 2933MHz (2933MHz requires Intel Core i7 or above) SoDIMM ECC Memory			
NIC	Built-in: Intel Ethernet Connection I219-LM 10/100/1000 Additional: Intel Ethernet Server Adapter I210-T1			
Power	7.4mm, 240W AC adapter			

LTE USB Dongle

Number: 1

SIM Card

Number: 1





Service Menu



The following functions are available for use.

Menu category	Function Name	Explanation
Basic Service	Visualization of Hosts/Network	Based on traffic obtained from the mirror port of network devices, the communication status is visualized from various perspectives using the Web UI. Host Network Map Traffic Ranking OT Protocol Registration
	Threat/Vulnerability Detection	Learning is performed based on traffic obtained from the mirror port of network devices to detect threats and vulnerabilities. Detection alerts are sent by email, and the information of targeted hosts can be checked from each alert. • Detection Alert • Learning & Detection Settings
	System Settings	System settings can be made, including internet address visualization, data deletion settings, sensor and user management, and service name management for the visualization UIs. • Change Settings • System Log • Sensor Management • User Management • Service Name Management
	Maintenance	 OsecT Sensor Maintenance Software Maintenance (OsecT Core, OsecT Sensor) Signature Updates (Once a day)



Function 1 Host/Network Visualization (1/3)



Function Categories	Function Name	Explanation	
1. Hosts	1-1. Overview	 All hosts in the network (information: IP address, MAC address, etc.) can be seen. The list of host information can be downloaded in CSV file format. By cross-referencing this list with the customer's management register, unintentionally connected hosts can be identified." 	
	1-2. Overview (IP)	 Hosts (IP addresses) can be searched by log type (IP communication, name resolution, etc.) and host type (client, server, etc.). 	
	1-3. Details	Detailed information for each host can be seen.	
	1-4. Vendor Matrix	 The MAC vendors of hosts are color-coded and displayed in a 16x16 format to provide a view of the entire network. 	
	1-5. OS Matrix	 The OS of hosts are color-coded and displayed in a 16x16 format to provide a view of the entire network. The OS is estimated from the packets sent by the host. The estimation accuracy can also be verified. 	
	1-6. Role Matrix	 The roles (e.g. client, server) of hosts are color-coded and displayed in a 16x16 format to provide a view of the entire network. The role is estimated from the status of the connection. 	
2. Network	2-1. Hosts	 All hosts can be seen in a network map of their connections. It is possible to check if unintended hosts are communicating with each other. 	
	2-2. Services	 The communication status of each service in the network can be checked on the network map. It is possible to check if any communication is occurring due to unintended services. 	

Function 1 Host/Network Visualization (2/3)



Function Categories	Function Name	Explanation
3.Traffic	3-1.Traffic	 Traffic information is displayed in a time series graph. It is possible to check if a host is infected and generating abnormal traffic.
4.Ranking	4-1.Traffic Volume of Host	 The ranking of hosts is displayed in order of traffic volume. The ranking order can be used to assess whether the traffic volume of a host is reasonable.
	4-2.Number of Connected Hosts	 The ranking of hosts is displayed in descending order of the number of connections. The ranking order can be used to assess whether the number of connections of a host is reasonable.
	4-3.Importance of Hosts	The ranking of hosts is displayed in order of importance.
	4-4.Traffic Volume of Service	The ranking of services is displayed in order of traffic volume.
	4-5.Number of Hosts by Service	 Service information is displayed in a ranking order based on the number of connected hosts.
	4-6.Number of Hosts by Vendor	 The ranking of MAC vendors is displayed in descending order of number of connections. The IP addresses for each MAC vendor can also be checked.
5.OT Protocol	5-1.Overview (IP)	 Information (source IP address, destination IP address, protocol name, etc.) of IP-based OT protocol in the control system network is analyzed and visualized.
	5-2.Overview (Ethernet)	 Information (source MAC address, destination MAC address, protocol name, etc.) of non IP-based OT protocol in the control system network is analyzed and visualized.



Function 1 Host/Network Visualization (3/3)



Function Categories	Function Name	Explanation
6.Registration	6-1.Overview	 Information from the customer's host register (IP address, MAC address, host name, installation location, etc.) can be imported. The only supported file format for import is CSV, and the format, including the items and order, cannot be changed from the default settings. Information of the imported host register is displayed in a list format.
	6-2.Details	 Information for all fields in the imported register is displayed for each host.
	6-3.Register Integration	 Information from the imported host register can be linked, displayed, and configured with existing visualization and detection functions. Host Overview: Display whether each host has a register or not. Host Details: Display host information, communication details, and register information. Network Map: When hovering over nodes on the map, register information will be displayed along with host information. Detection Alerts: Display whether the register is present in new host detection alerts. Learning & Detection Settings: Email notifications for new hosts not found in the register can be set.

Function 2 Threat/Vulnerability Detection (1/2) decomo



Function Categories	Function Name	Explanation	
1.Detection Alert	1-1.New Hosts	Detect newly connected hosts (IP addresses) and outputs alerts.	
	1-2. Vulnerable Hosts	Detect hosts using unsupported operating systems and outputs alerts.	
	1-3.IP Communication	 The combination of Layer 3/4 information is learned as a normal communication, and any communication outside the learning period is detected, outputting an alert during the detection period. Some OT protocols have a fixed source port number and a variable destination port number. To identify such services, the destination port number can be learned in a range (e.g., 49203-65477) and the source port number can be set as a fixed value. 	
	1-4.IP Traffic	 Based on the traffic volume for each host pair, threshold values are automatically set and calculated for every day of the week. Detection and alert output occur when these threshold values are exceeded. 	
	1-5.IP Statistics	 Summary statistics are calculated for each host every 5 minutes from communication logs. Based on these summary statistics, normal communication is learned for each host through confidence interval analysis and principal component analysis. In detection, the same summary statistics are used and compared with the model created during learning to perform anomaly detection and alert output. 	
	1-6.OT Behavior (IP)	 OT protocol information (source IP address, destination IP address, OT protocol name, function) is registered in the detection exclusion list as normal communication. During the detection period, communication outside the exclusion list is detected and alerts are generated. 	
	1-7.OT Behavior (Ethernet)	 OT protocol information (source MAC address, destination MAC address, OT protocol name, function) is registered in the detection exclusion list as normal communication. During the detection period, communication outside the exclusion list is detected and alerts are generated. 	
	1-8.Signature	 Detect and output alerts for communications matching known signatures such as CVE. 	



Function 2 Threat/Vulnerability Detection (2/2) docomo



Function Categories	Function Name	E	xplanation
2. Learning & Detection Settings	2-1.New Hosts	•	The list of learned host information (IP addresses, MAC addresses) can be viewed, allowing for the registration of new hosts and the removal of unnecessary information.
Detection Settings	2-2.Vulnerable Hosts	•	To avoid unnecessary alerts., host information can be registered in the detection exclusion list.
	2-3.IP Communication	•	The list of learned IP communication information (source/destination IP addresses, source/destination port numbers, protocols) can be viewed, allowing for the registration of new communication information, removal of unnecessary data, and modification of the learned list.
	2-4.IP Traffic	•	The list of traffic for each learned host pair can be viewed. Additionally, the selection of host pairs for detection and the deletion of learned information are possible.
	2-5.IP Statistics	•	The learning status (confidence intervals, principal components) for each host can be checked. Detection mode (no/week/strong) can also be configured for each host.
	2-6.OT Behavior (IP)	•	OT protocol communication information (source IP address, destination IP address, OT protocol, function) set in the detection exclusion list can be viewed. New OT protocol communication information can be added, and target functions to be detected can be configured.
	2-7.OT Behavior (Ethernet)	•	OT protocol communication information registered (source MAC address, destination MAC address, OT protocol name, and function) set in the detection exclusion list can be viewed. New OT protocol communication information can be added, and target functions to be detected can be configured.
	2-8. Signature	•	To avoid unnecessary alerts, a combination of source IP address and signature can be registered in the detection exclusion list.
	2-9. Learning & Detection Status	•	The learning and detection modes, status, and setting data for each detection function can be viewed in a list.

Function³ Assessment



Function Categories	Function Name	Explanation
1. Assessment	1-1. Assessment	 This feature generates an assessment report. Based on OsecT's visualization and detection information, a report evaluating the status of the OT network and providing improvement suggestions is generated and exported in PowerPoint format.