OsecT: An IDS for OT

Updated on Apr 7th, 2026

This document describes the specifications for services within Japan, and specifications for services outside Japan may differ.

Japan-made OT-IDS 「OsecT」

OsecT is an OT-focused Intrusion Detection System (IDS) developed by NTT Docomo Business, based on advanced technologies from NTT Laboratories. These include traffic flow analysis techniques cultivated through DDoS countermeasures in large-scale ISP/Tier1 networks, as well as risk visualization technologies used to support the communications infrastructure for the Tokyo 2020 Olympic and Paralympic Games.

OT Network Visualization

Connected hosts and communications, analyzed from various perspectives, can be viewed through the OsecT SaaS portal.

Early Detection of Cyber Threats

Cyber threats such as suspicious hosts and unknown communications can be detected at an early stage with automated alert notifications.

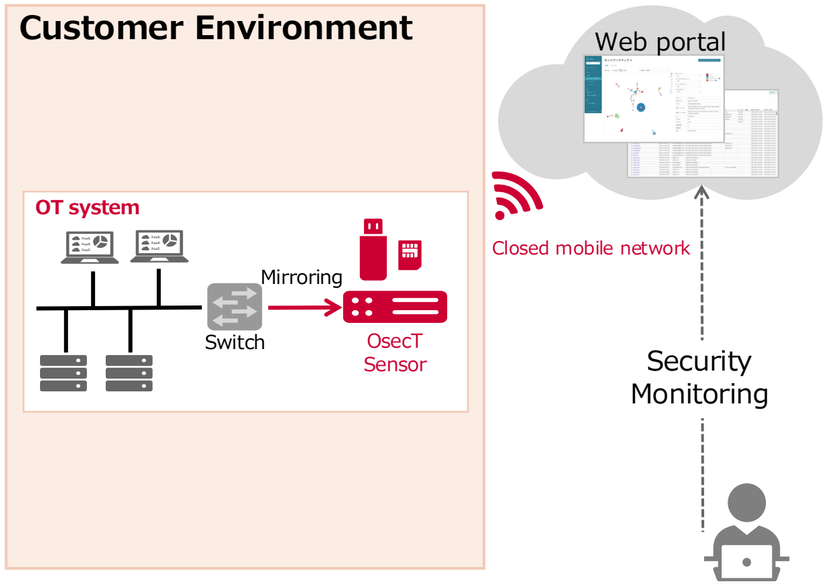
Structure of OsecT

docomo Business

SaaS version

OsecT Basic

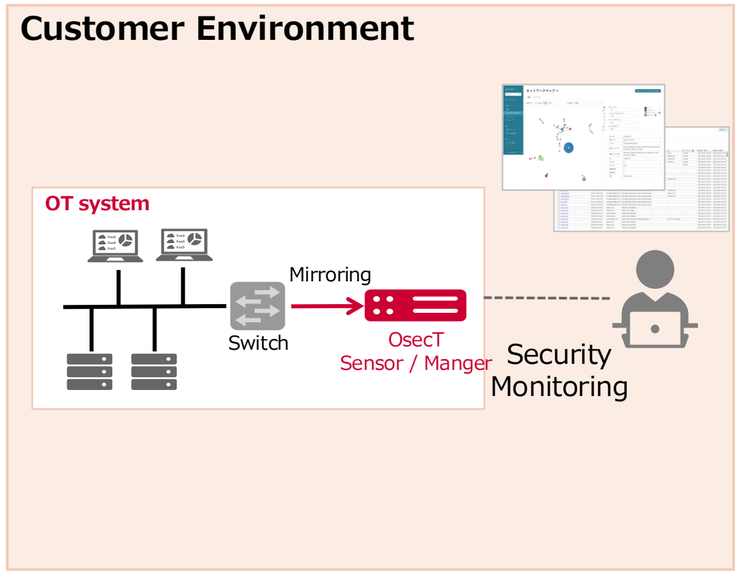
- Security monitoring data is uploaded from the OsecT sensor to the cloud via LTE (private network).
- Security monitoring is performed by accessing the web portal interface.



On-premises version

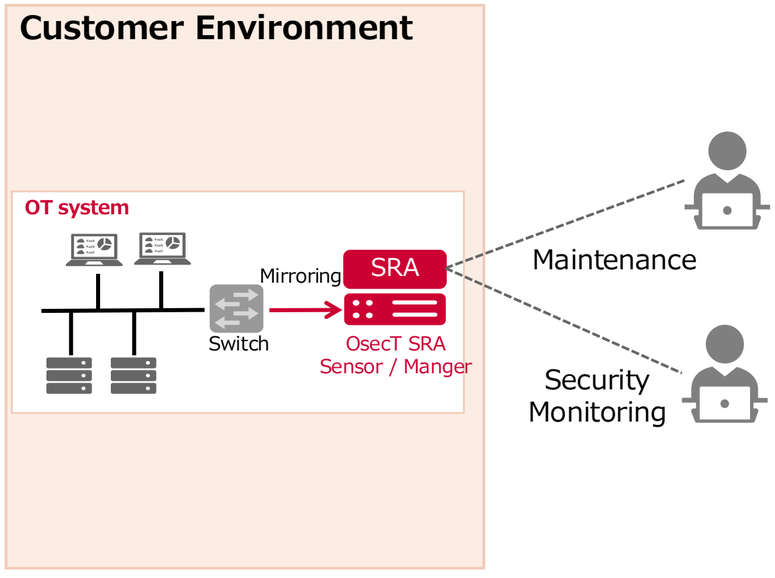
OsecT Edge

- Provided as an on-premises solution that completes security monitoring within the customer's environment, similar to conventional IDS products.
- Suitable for systems where cloud services cannot be used, or when security monitoring needs to be fully contained within the internal network.



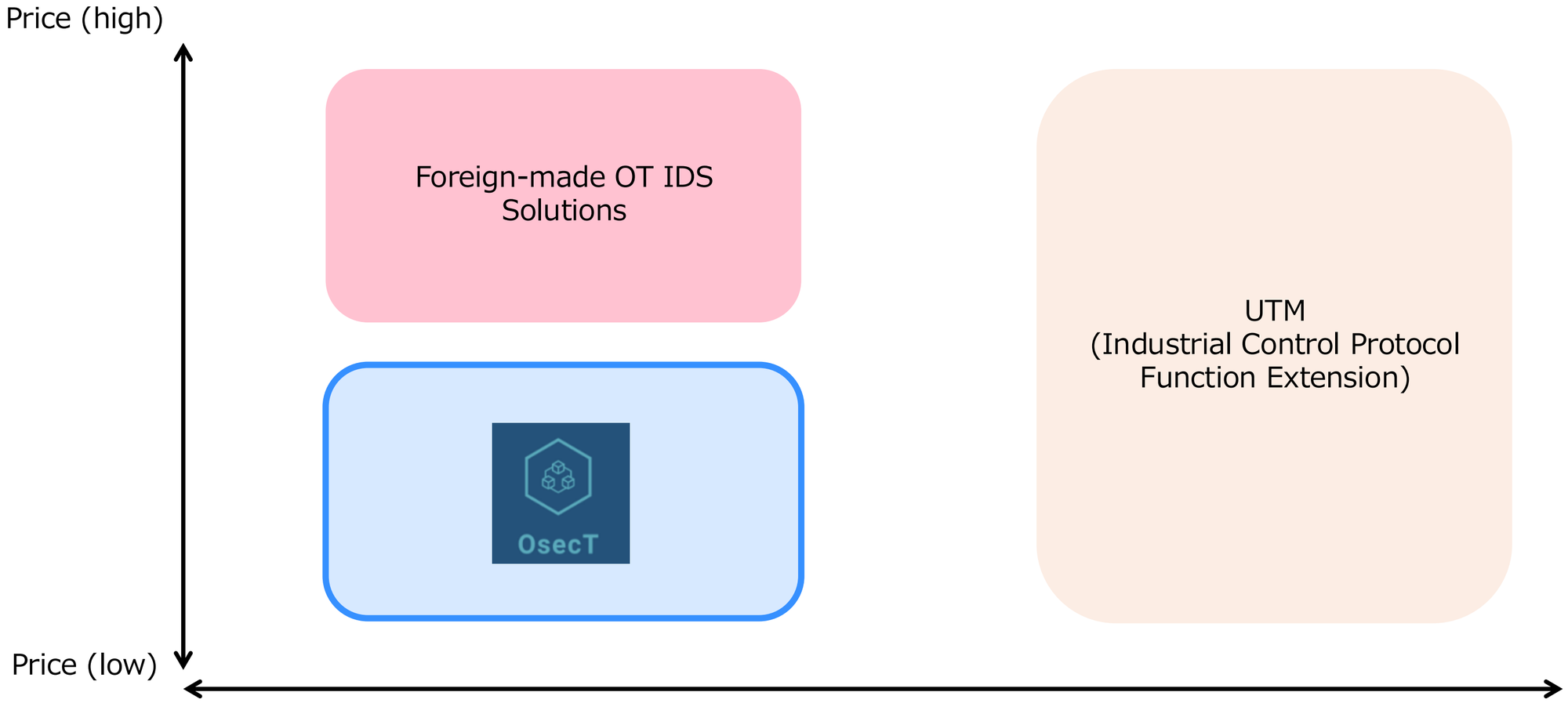
OsecT SRA

- The OsecT on-premises version is equipped with a Secure Remote Access (SRA) feature. In addition to "visualization" and "detection," it provides "secure remote access" in a one-stop solution on the same hardware.
- In addition to monitoring OsecT through the SRA function, it can also be used for remote maintenance of OT systems.



OsecT

Positioning in the OT IDS Market



IDS for OT Systems

- Passive monitoring, incorporating limited active scanning functions
- Core features: network visualization and anomaly detection
- Supplementary signature-based detection also provided

IDS for IT Systems

- Core feature: signature detection

*UTM : Unified Threat Management

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.

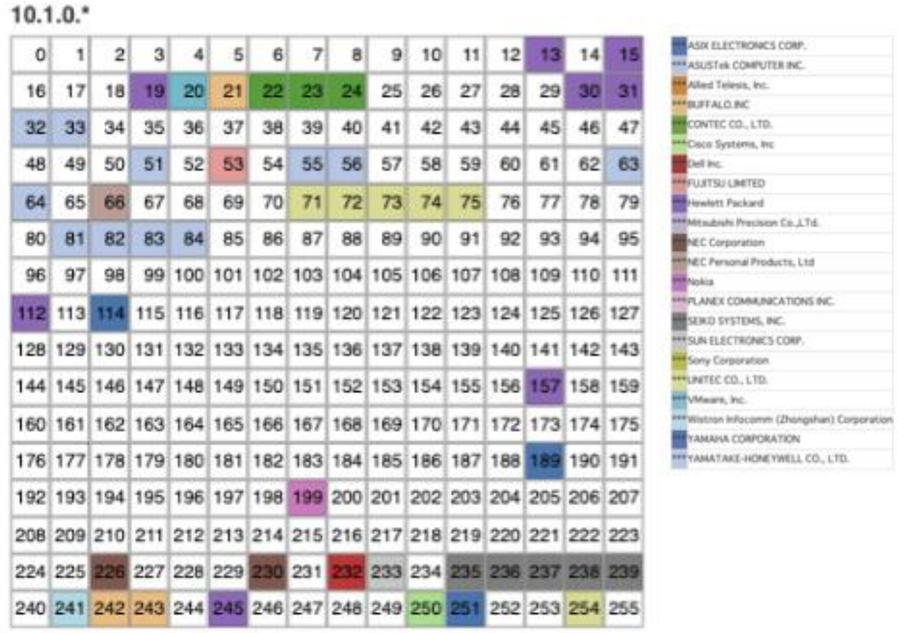
- **Automatically generate an overview of host information**
- **Host overview can be exported as a CSV file and used as a register**

Host Overview

#	IPv4 Addresses	IPv6 Addresses	MAC Address	Vendor	Host Name	Host Type···	OS	Same S···	First Seen	Last Seen	Register
11	10.90.4.134		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
12	10.90.4.135		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
13	10.90.4.136		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
14	10.90.4.137		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
15	10.90.4.138		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
16	10.90.4.139		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
17	10.90.4.140		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
18	10.90.4.141		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
19	10.90.4.142		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered
20	10.90.4.143		00:0c:29:62:f4:31	VMware, Inc.		PC			2024-12-02 17:08:41	2024-12-02 17:18:22	Unregistered

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

Host Matrix

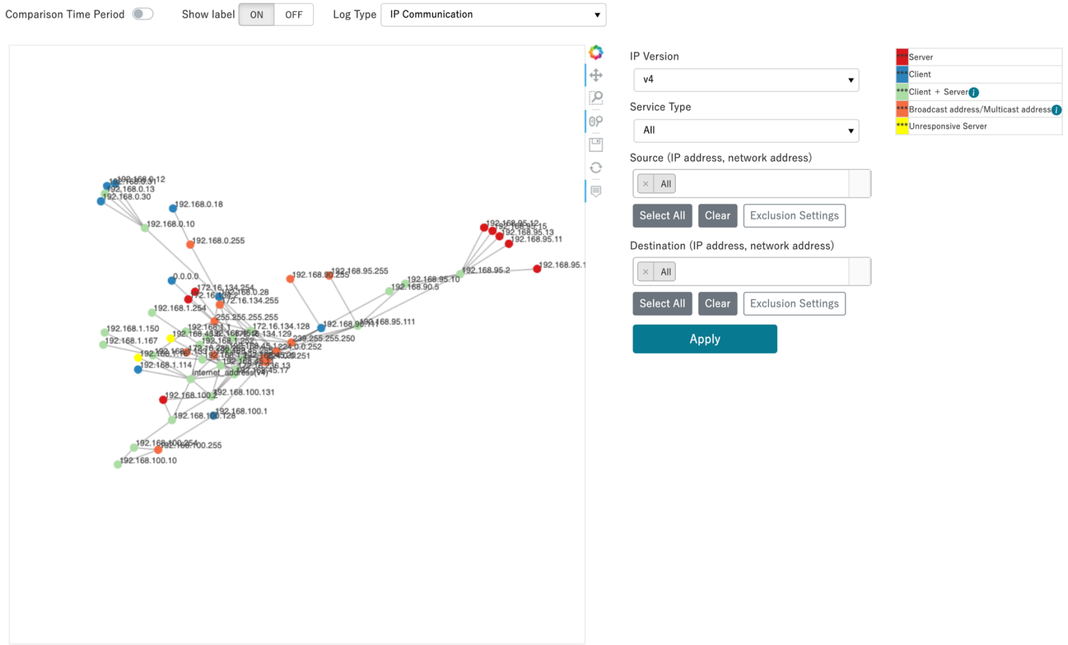


Visualization -Host・Network-

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.

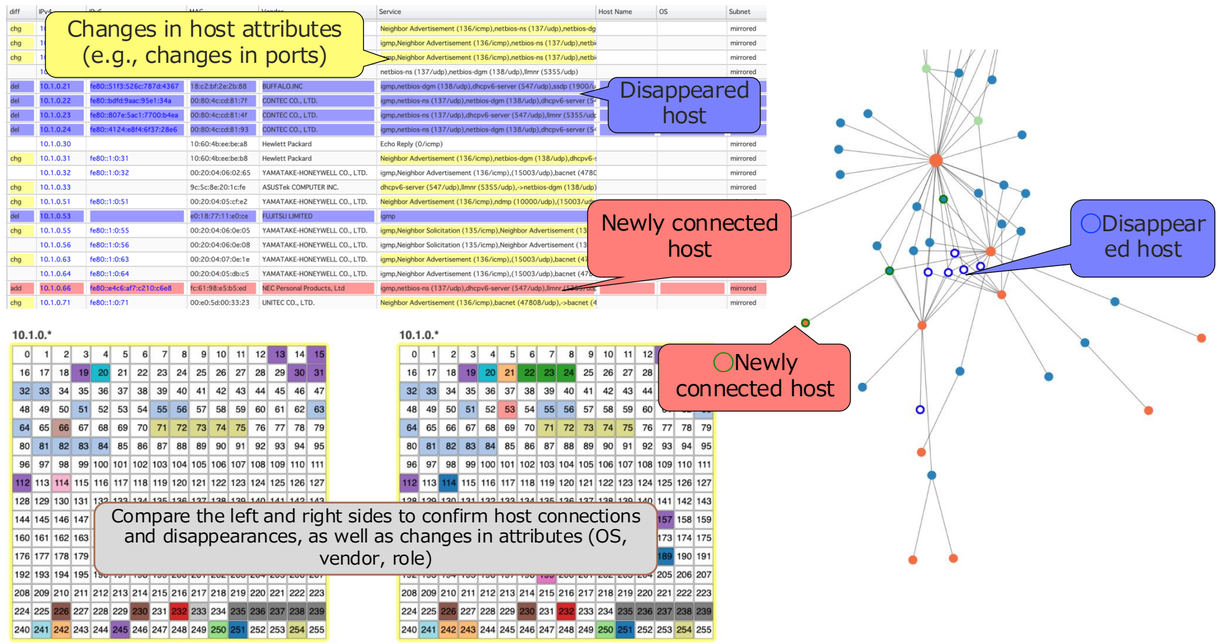
- **Visualize host communication relationships in a map format**
- **Data being displayed can be exported as an image**

Network Map



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

Difference Analysis



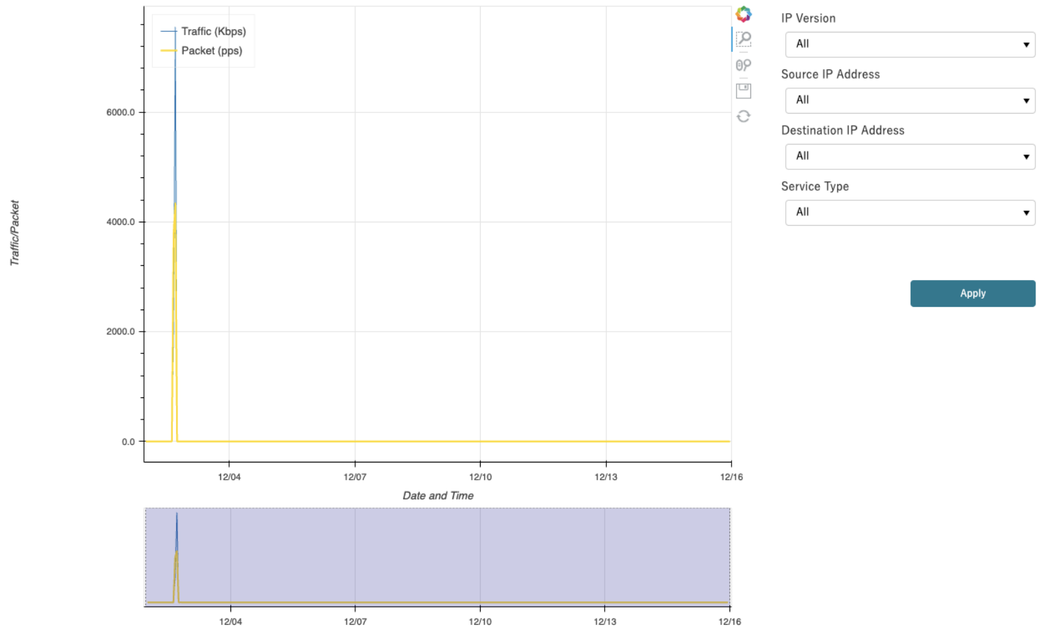
Visualization -Network-

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.

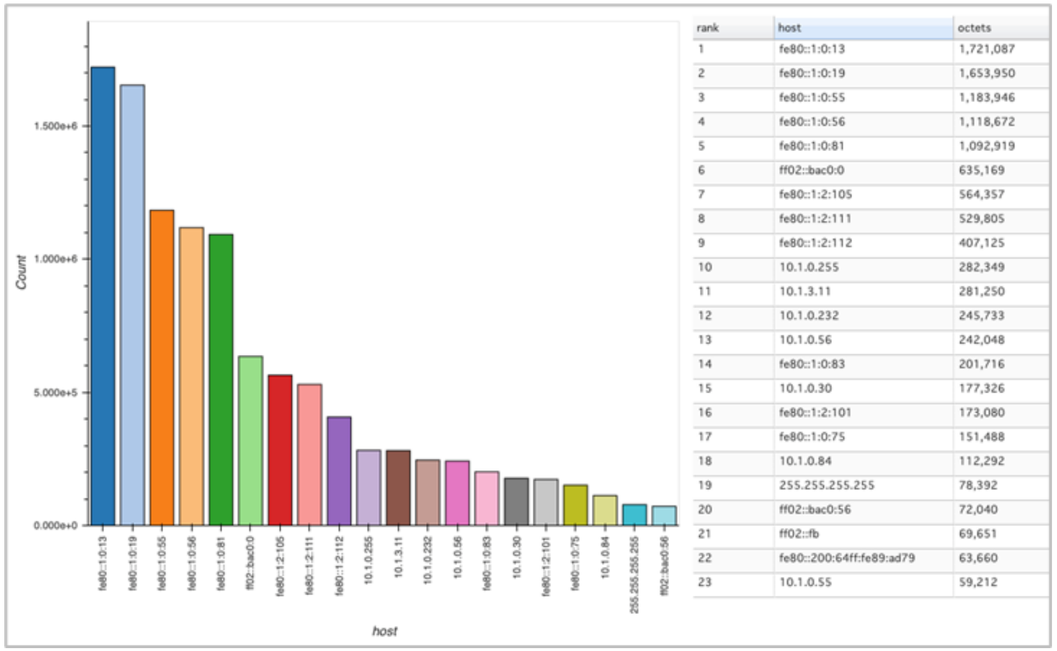
- **Visualize network load (bandwidth usage)**
- **Detect bandwidth congestion caused by loops, etc.**

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

Traffic



Ranking



rank	host	octets
1	fe80::1:0:13	1,721,087
2	fe80::1:0:19	1,653,950
3	fe80::1:0:55	1,183,946
4	fe80::1:0:56	1,118,672
5	fe80::1:0:81	1,092,919
6	ff02::bac0:0	635,169
7	fe80::1:2:105	564,357
8	fe80::1:2:111	529,805
9	fe80::1:2:112	407,125
10	10.1.0.255	282,349
11	10.1.3.11	281,250
12	10.1.0.232	245,733
13	10.1.0.56	242,048
14	fe80::1:0:83	201,716
15	10.1.0.30	177,326
16	fe80::1:2:101	173,080
17	fe80::1:0:75	151,488
18	10.1.0.84	112,292
19	255.255.255.255	78,392
20	ff02::bac0:56	72,040
21	ff02::fb	69,651
22	fe80::200:64ff:fe89:ad79	63,660
23	10.1.0.55	59,212

Detection -Prevention-

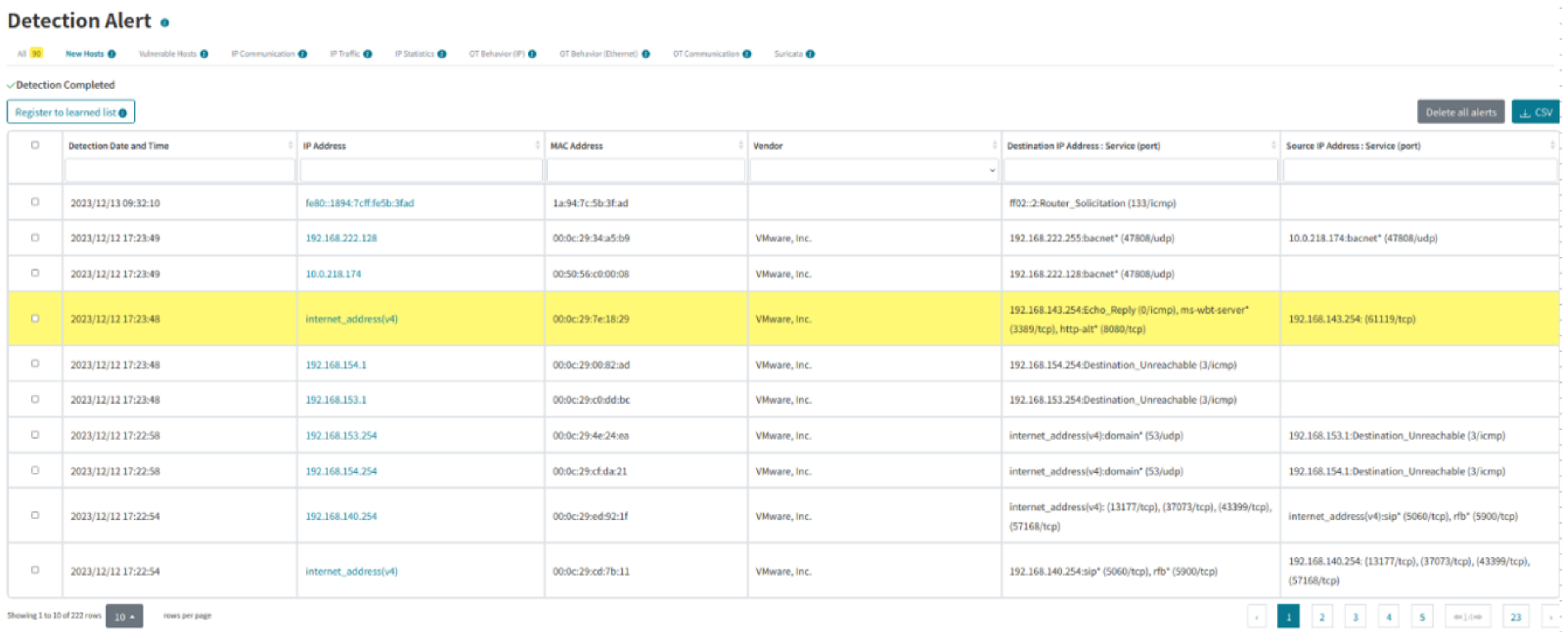
NTT docomo Business

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.

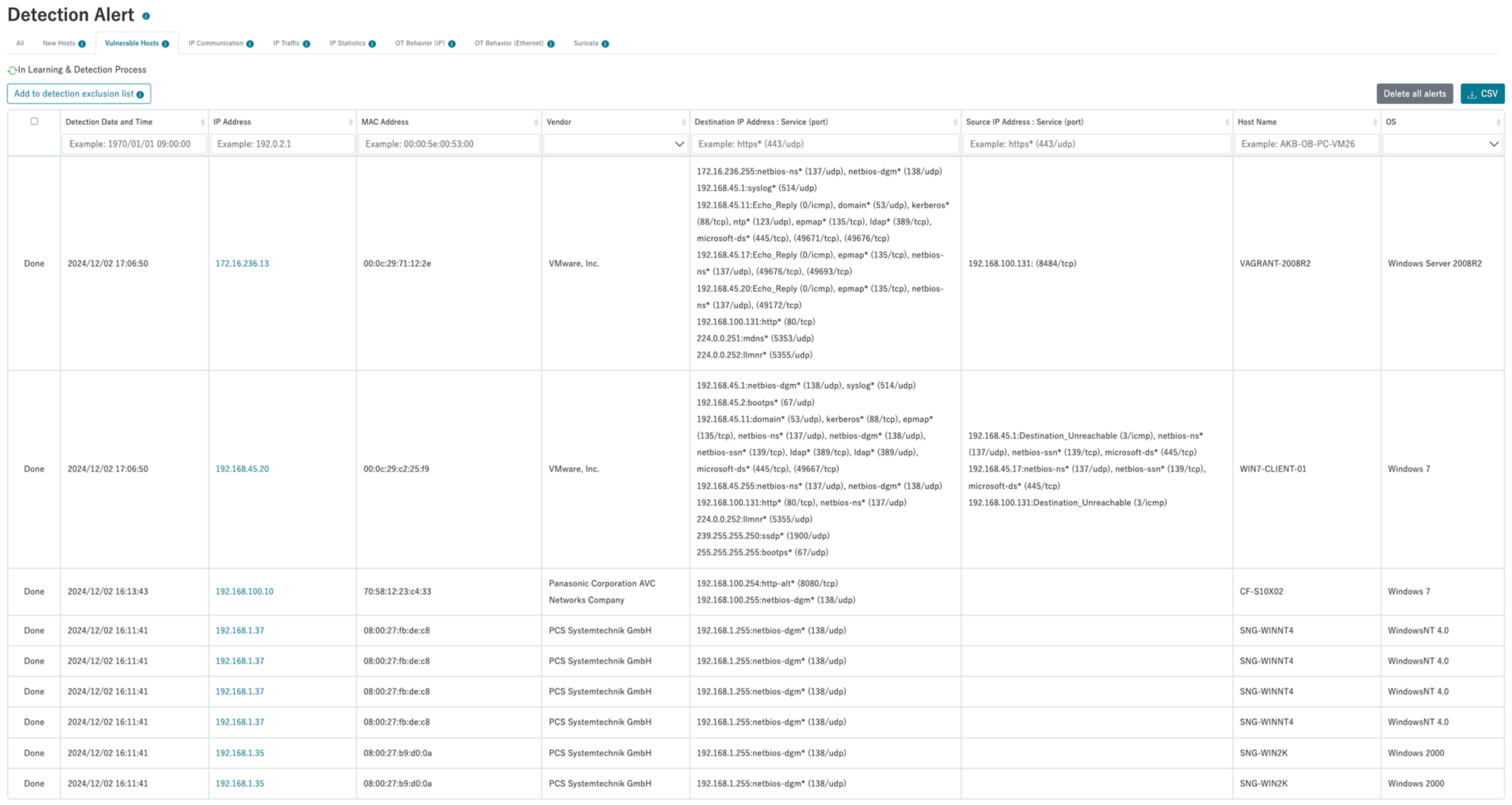
- **Automatically learn host addresses within the network**
- **Quickly detect rogue hosts without missing any**

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

Detection of Connected Hosts



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.

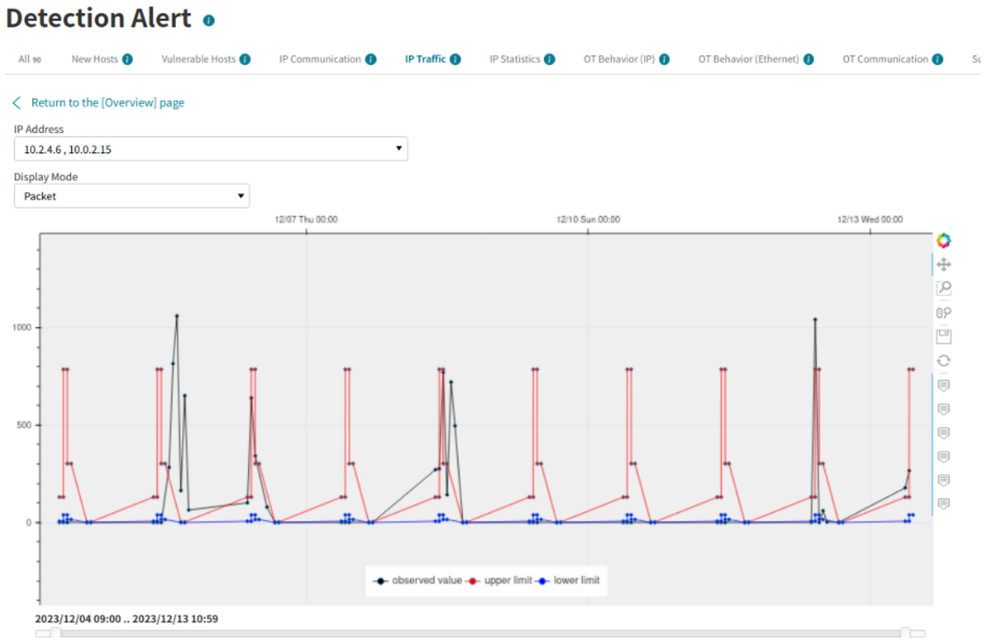
- **Automatically learn communication data within the network**
- **Quickly detect unknown communications without missing any**

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		
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

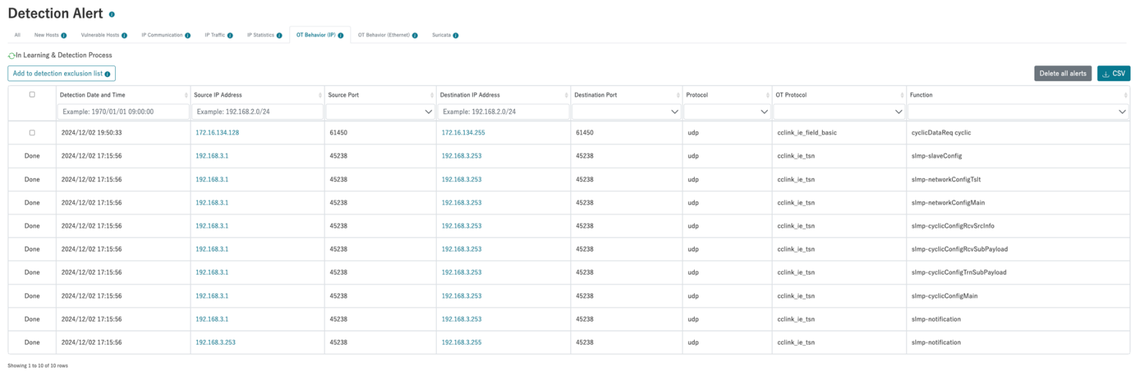


Detection -Early Identification of Anomalies-

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

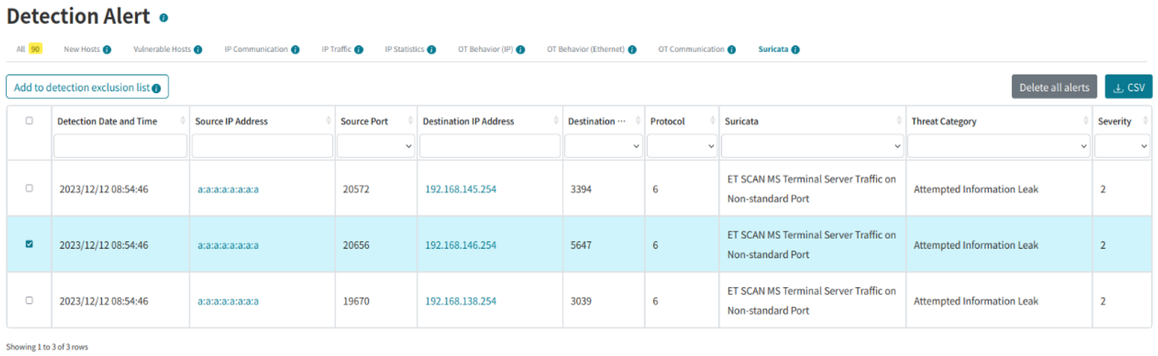
- **Detect OT commands that affect the system**
- **Commands and hosts targeted for detection can be customized**

Detection of OT Behavior



- **Detect communications that match known attack patterns**

Detection of Signature



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.

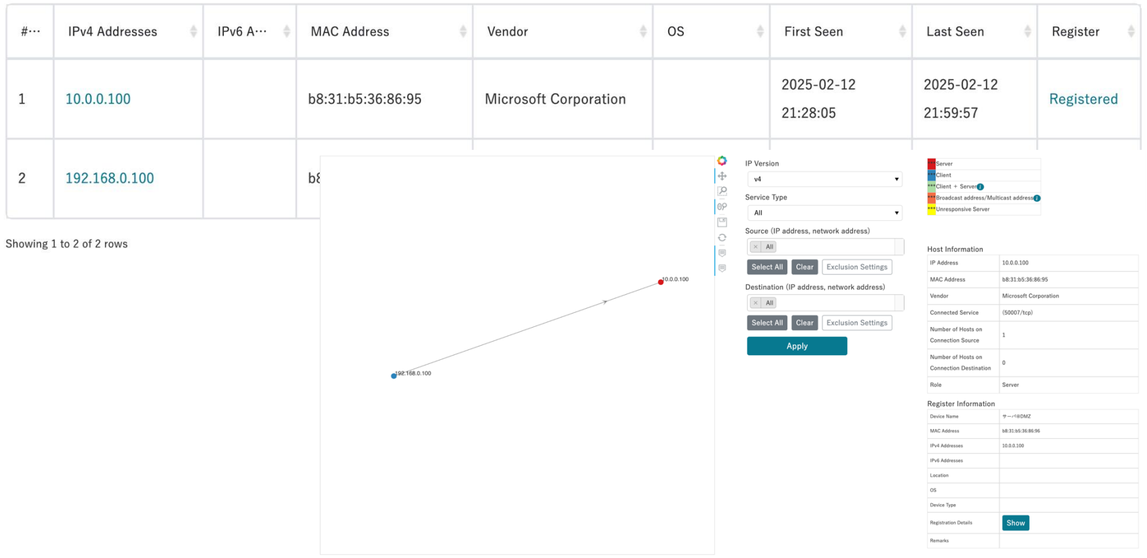
Integrate host register information with Host Overview/Network Map

Display additional information such as host installation locations and dates

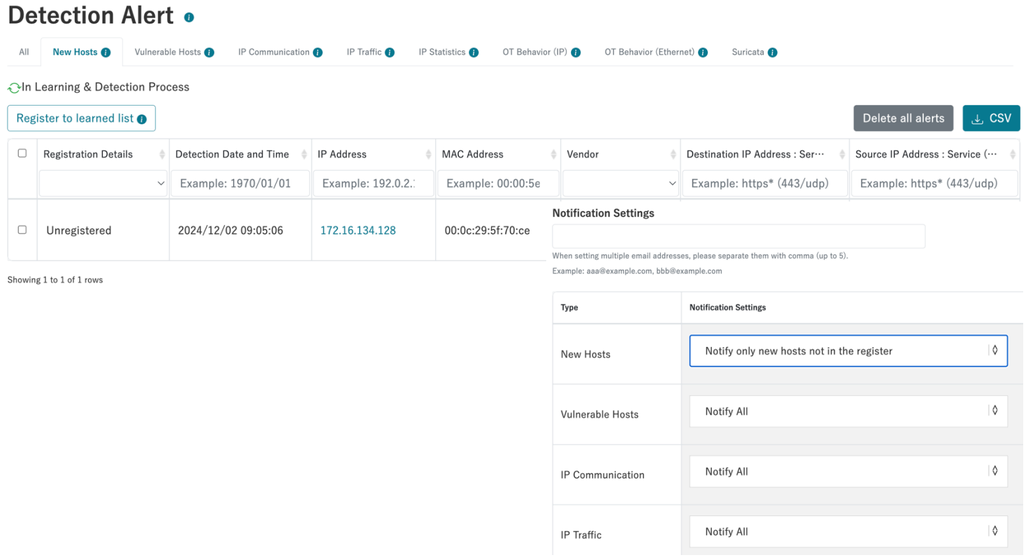
Integrate register data with Connected Host Detection function

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

Integrate with Host Overview/Network Map



Integrate with Connected Hosts 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.

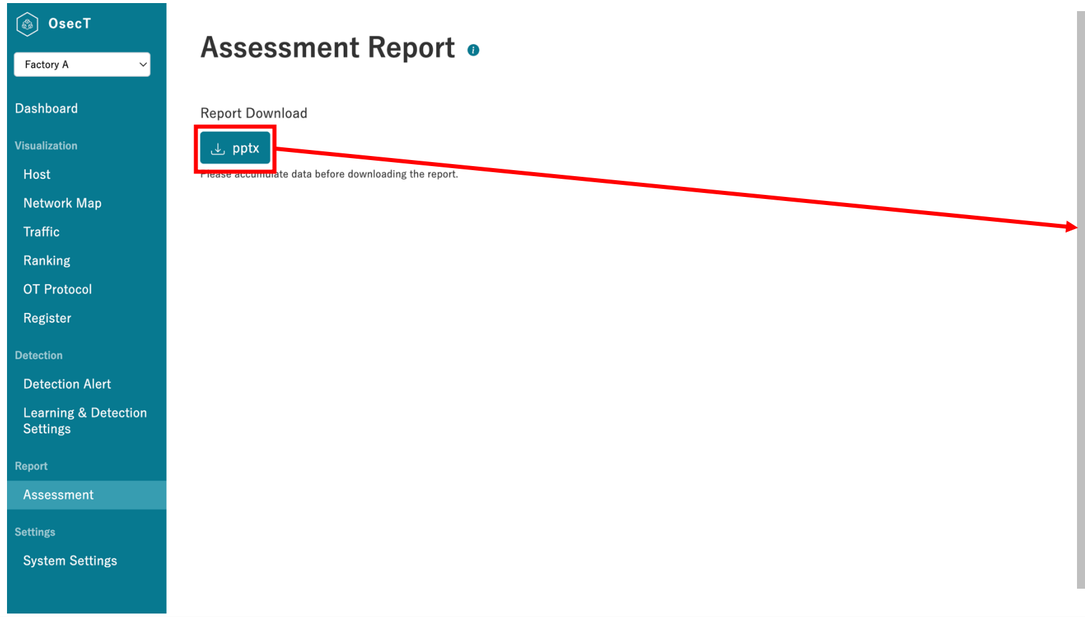
Generate reports with just a single click

Output in an editable PowerPoint format

List hosts and those with unsupported OS versions

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

Assessment



Assessment Report File