

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

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.

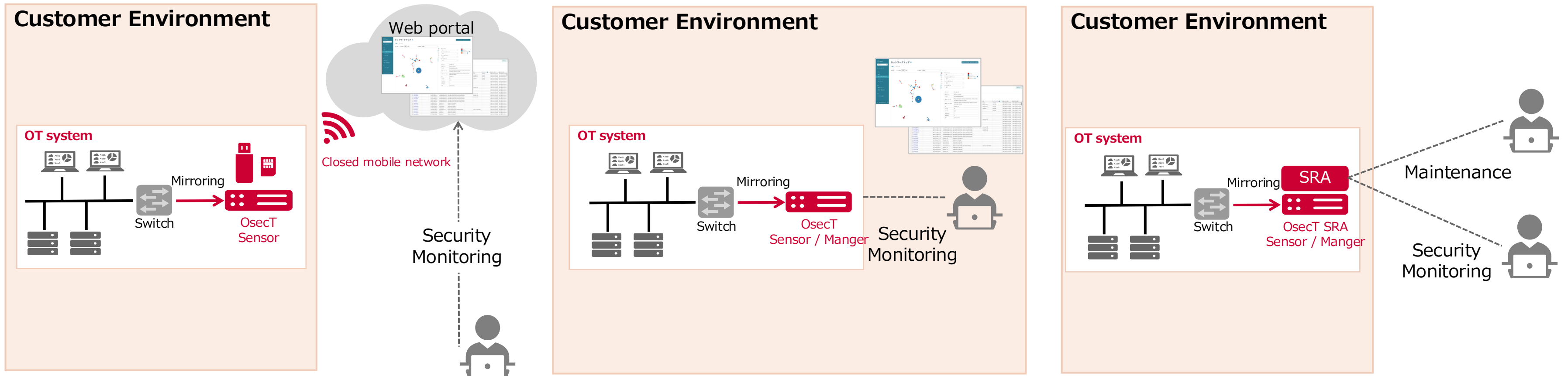
On-premises version

OsecT Edge

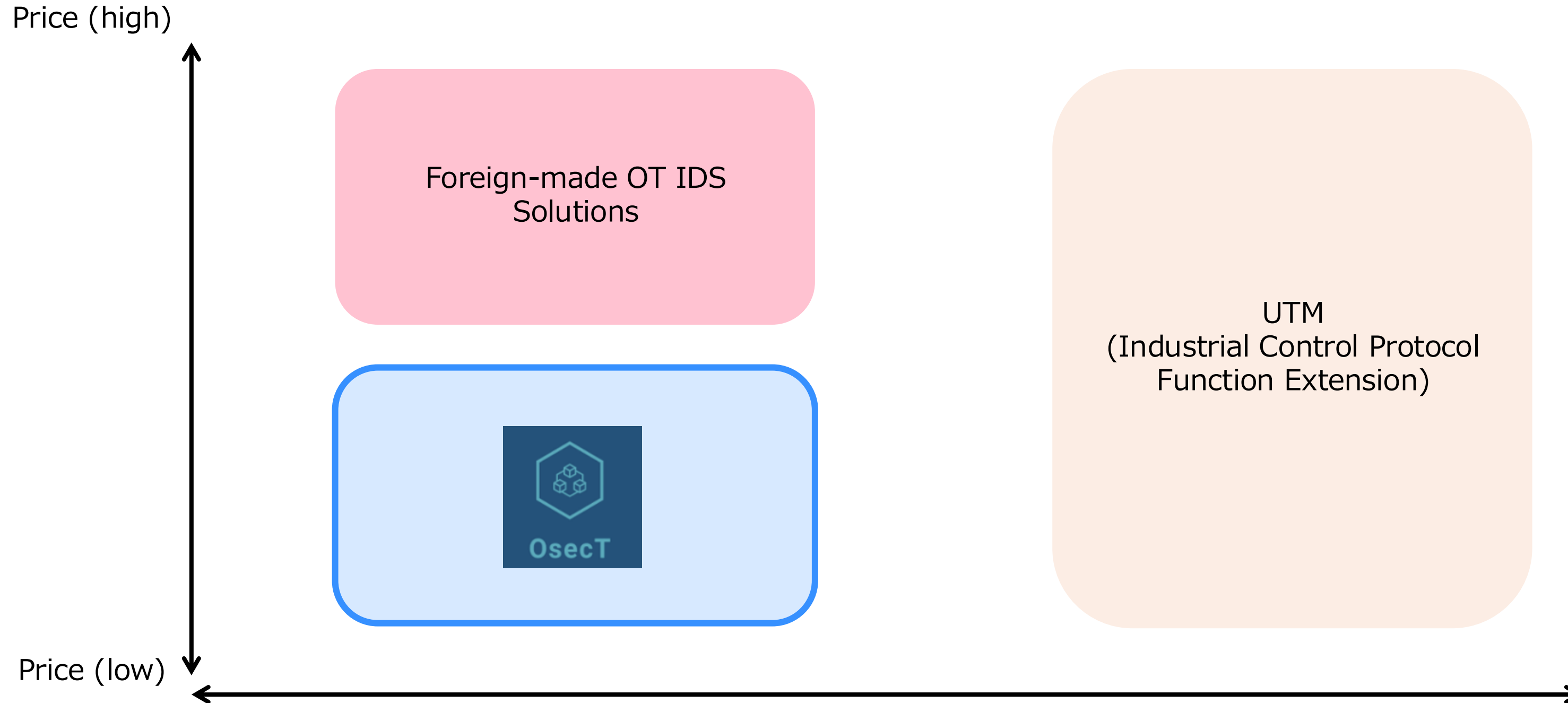
- Provided as an on-premises solution that completes security monitoring within the customer's environment, similar to conventional IDS products.
- Suitable for systems where cloud services cannot be used, or when security monitoring needs to be fully contained within the internal network.

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.

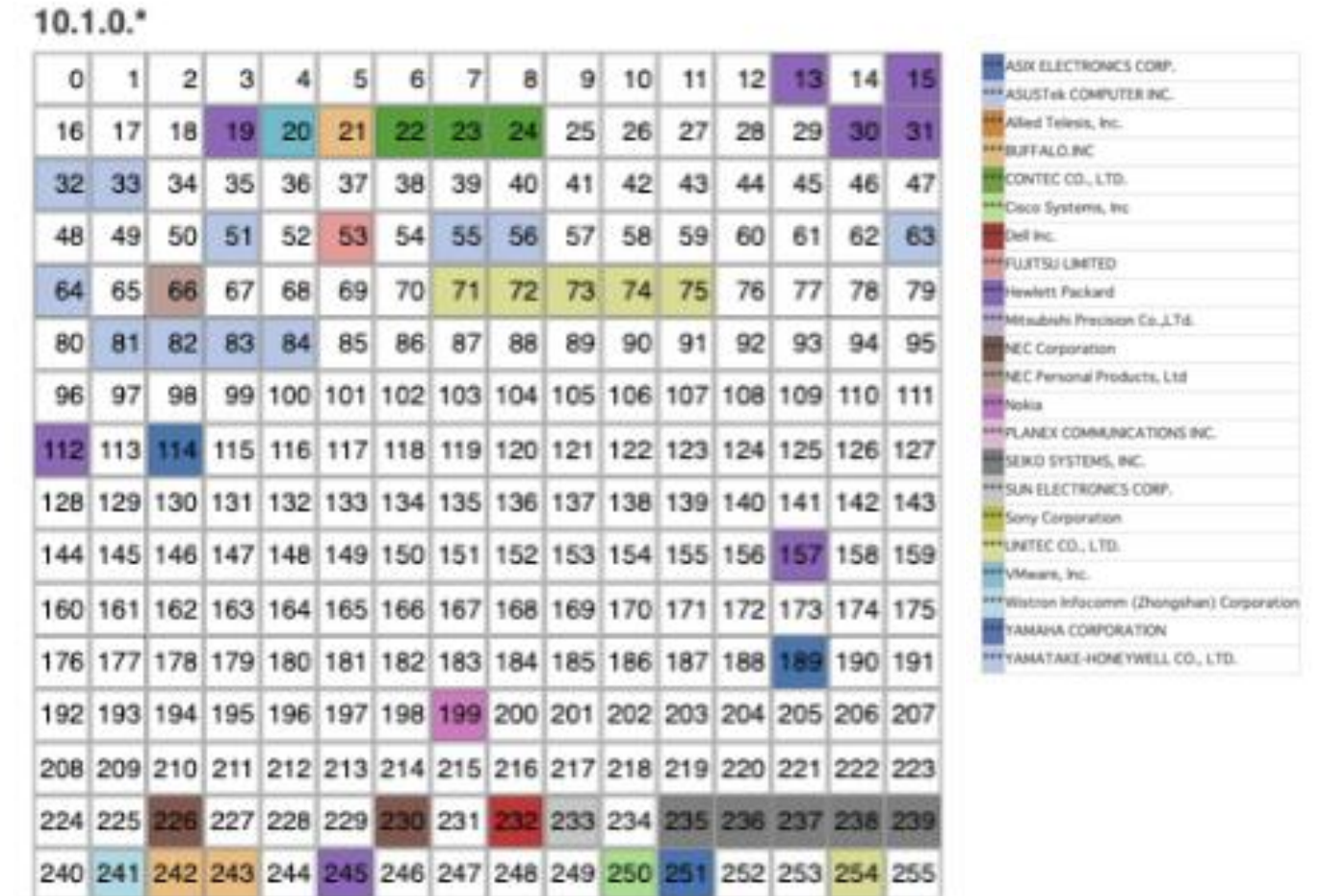
- Automatically generate an overview of host information
- Host overview can be exported as a CSV file and used as a register

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

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

Host Matrix



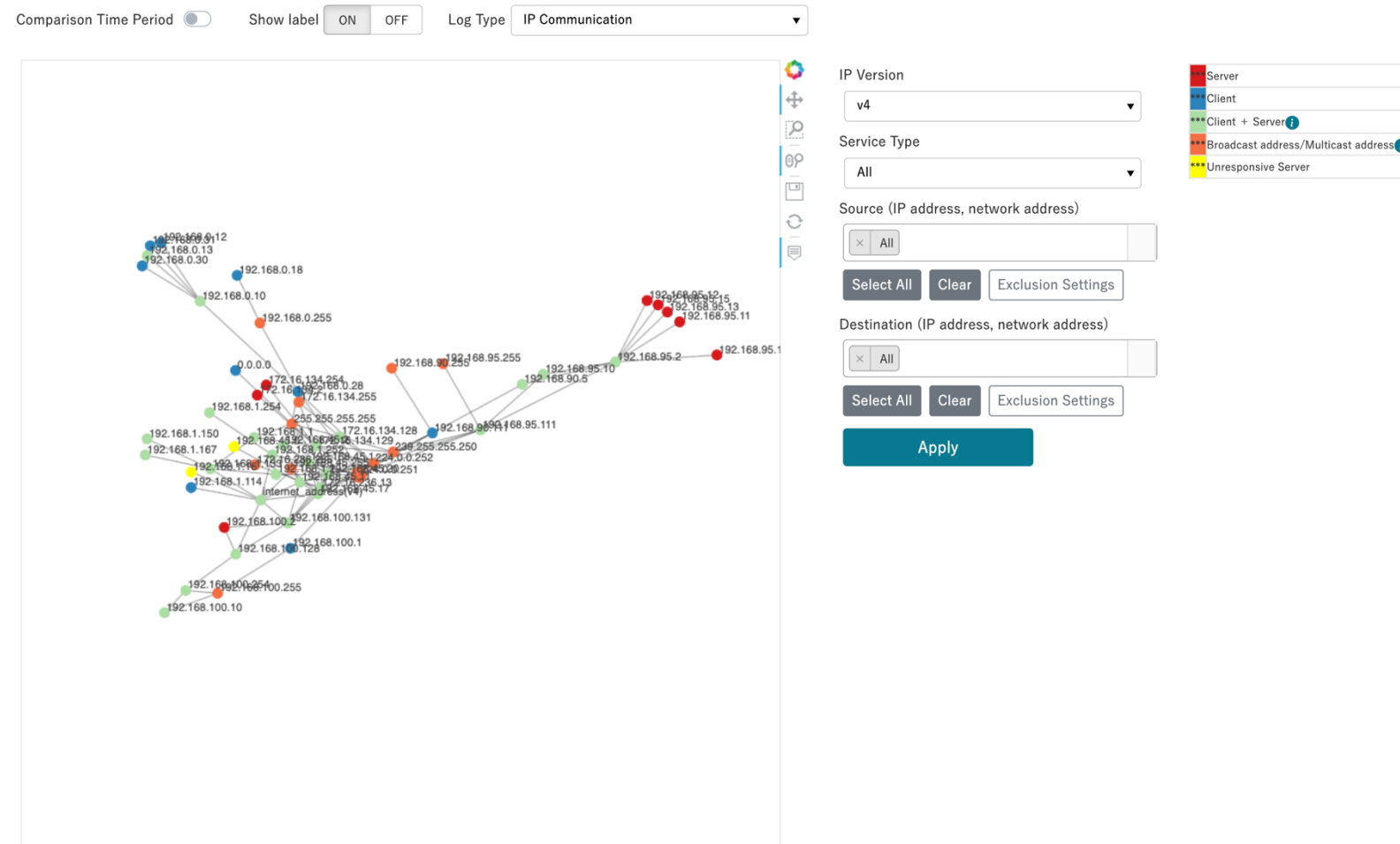
Visualization -Host · Network-

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.

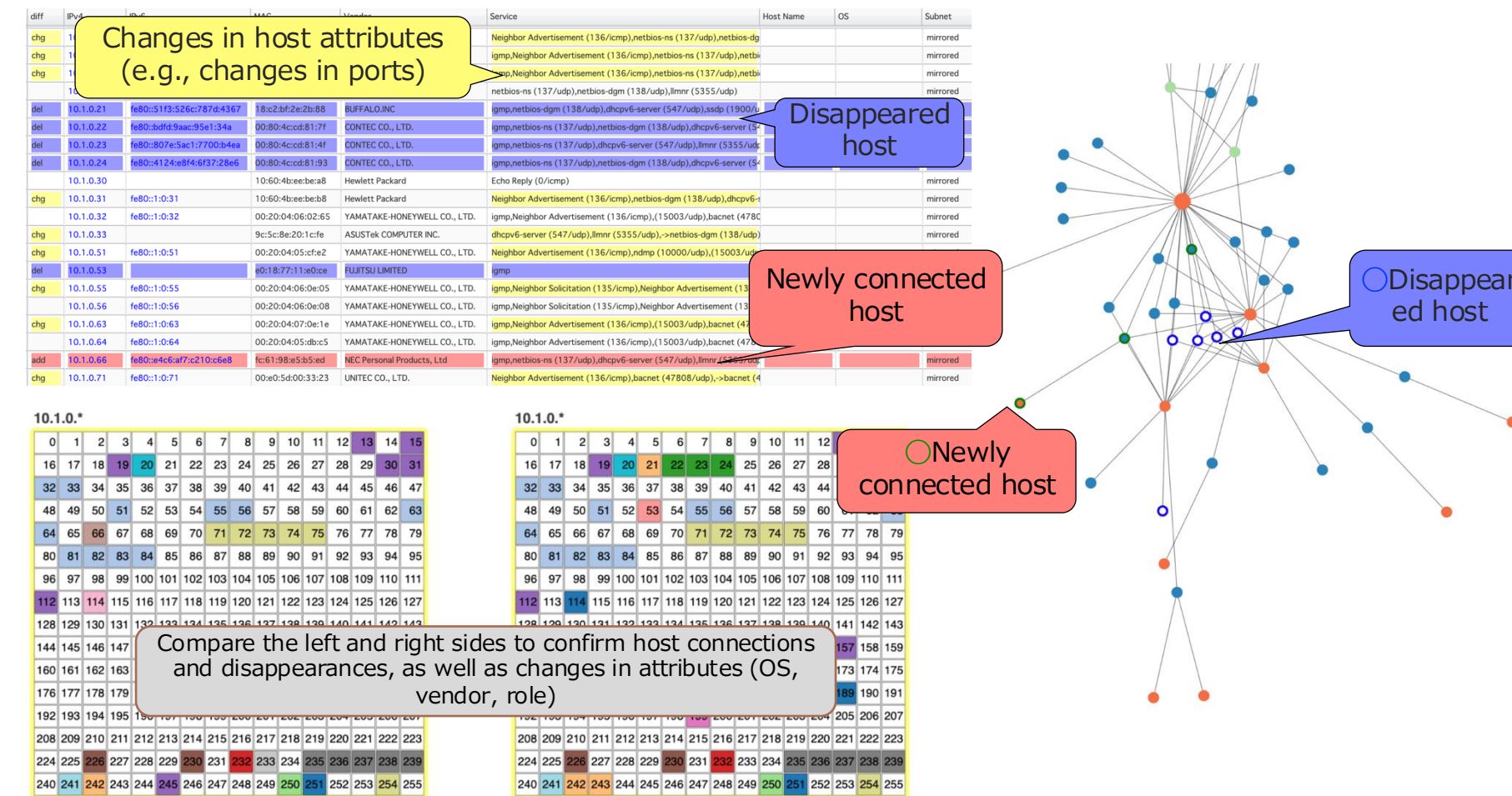
- Visualize host communication relationships in a map format
- Data being displayed can be exported as an image

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

Network Map



Difference Analysis



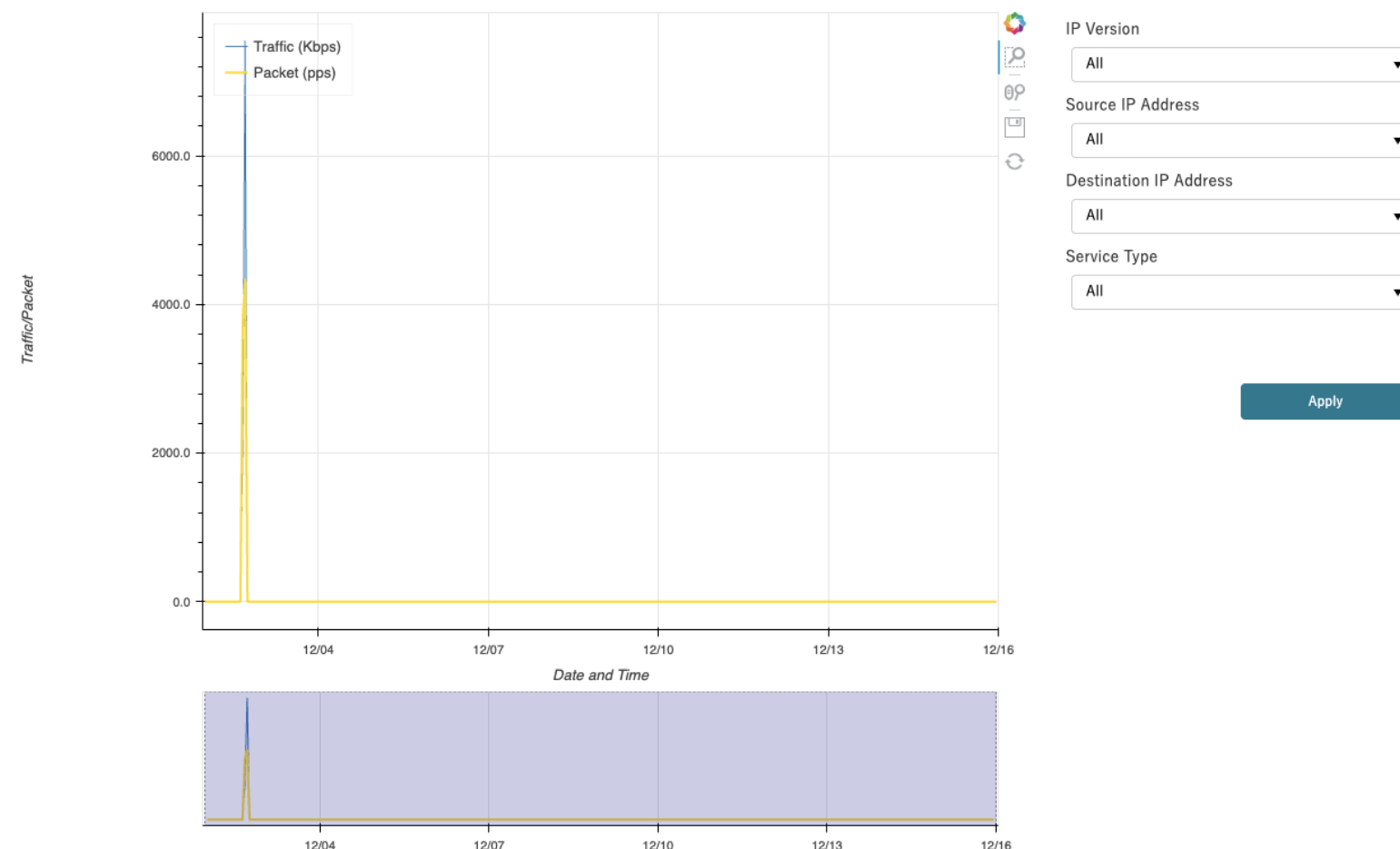
Visualization -Network-

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.

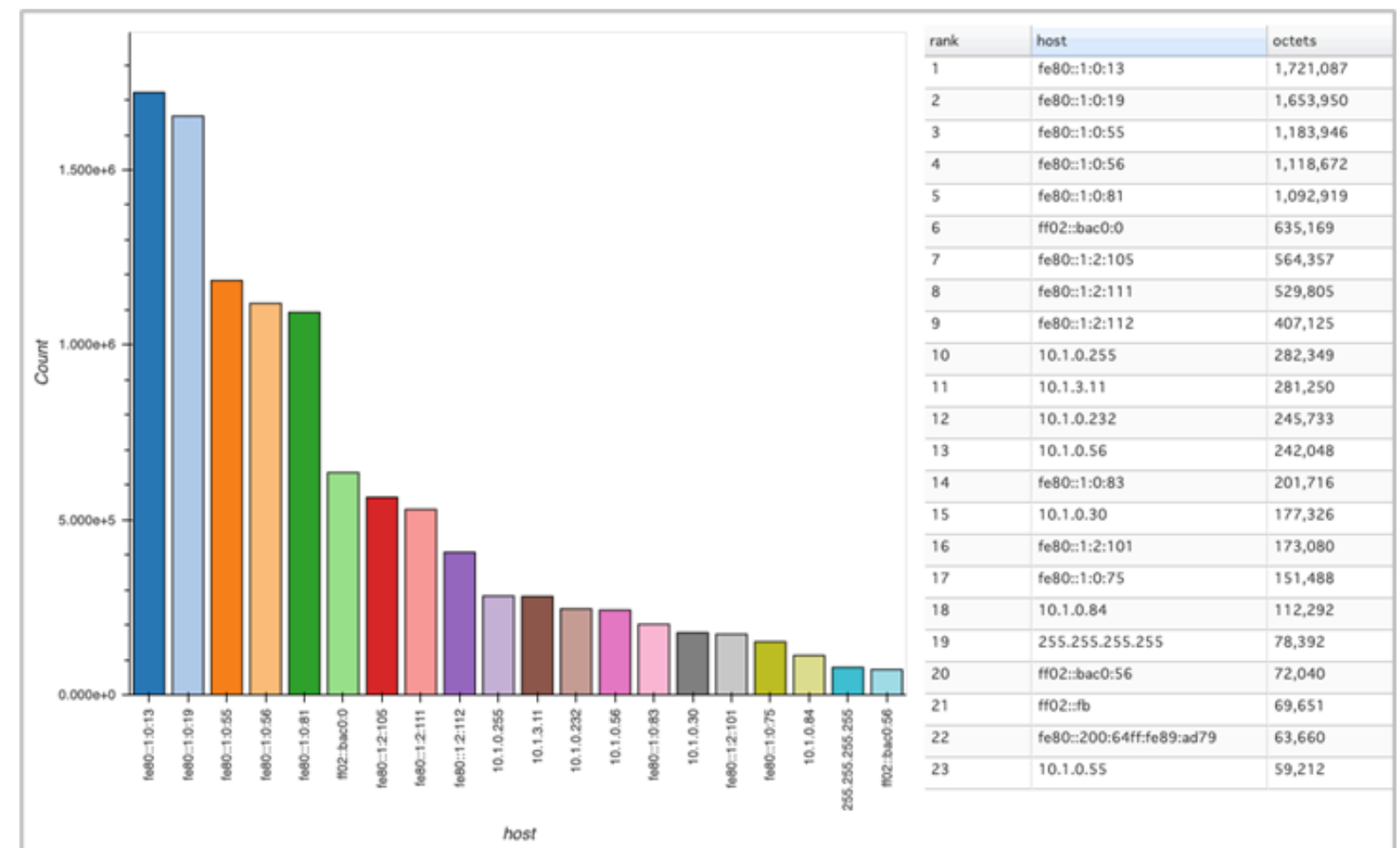
- Visualize network load (bandwidth usage)
- Detect bandwidth congestion caused by loops, etc.

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

Traffic



Ranking



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 Connected Hosts

Detection of Vulnerable Hosts

Detection Alert

All New Hosts Vulnerable Hosts IP Communication IP Traffic IP Statistics OT Behavior (IP) OT Behavior (Ethernet) OT Communication Suricata

✓ Detection Completed

Register to learned list

Detection Date and Time	IP Address	MAC Address	Vendor	Destination IP Address : Service (port)	Source IP Address : Service (port)
2023/12/13 09:32:10	fe80::1894:7c:ff:fe5b:3fad	1a:94:7c:5b:3fad		#02:~2:Router_Solicitation (133/icmp)	
2023/12/12 17:23:49	192.168.222.128	00:0c:29:34:a5:b9	VMware, Inc.	192.168.222.255:bacnet* (47808/udp)	10.0.218.174:bacnet* (47808/udp)
2023/12/12 17:23:49	10.0.218.174	00:50:56:c0:00:08	VMware, Inc.	192.168.222.128:bacnet* (47808/udp)	
2023/12/12 17:23:48	internet_address(v4)	00:0c:29:7e:18:29	VMware, Inc.	192.168.143.254:Echo_Reply (0/icmp), ms-wbt server* (3389/tcp), http-alt* (8080/tcp)	192.168.143.254 (81119/tcp)
2023/12/12 17:23:48	192.168.154.1	00:0c:29:00:82:ad	VMware, Inc.	192.168.154.254:Destination_Unreachable (3/icmp)	
2023/12/12 17:23:48	192.168.153.1	00:0c:29:c0:dd:bc	VMware, Inc.	192.168.153.254:Destination_Unreachable (3/icmp)	
2023/12/12 17:22:58	192.168.153.254	00:0c:29:4e:24:ea	VMware, Inc.	internet_address(v4):domain* (53/udp)	192.168.153.1:Destination_Unreachable (3/icmp)
2023/12/12 17:22:58	192.168.154.254	00:0c:29:cf:da:21	VMware, Inc.	internet_address(v4):domain* (53/udp)	192.168.154.1:Destination_Unreachable (3/icmp)
2023/12/12 17:22:54	192.168.140.254	00:0c:29:ed:92:1f	VMware, Inc.	internet_address(v4):(13177/tcp), (37073/tcp), (43399/tcp), (57168/tcp)	internet_address(v4):sip* (5060/tcp), rfb* (5900/tcp)
2023/12/12 17:22:54	internet_address(v4)	00:0c:29:cd:7b:11	VMware, Inc.	192.168.140.254:sip* (5060/tcp), rfb* (5900/tcp)	192.168.140.254:(13177/tcp), (37073/tcp), (43399/tcp), (57168/tcp)

Showing 1 to 10 of 222 rows | 10 rows per page

Detection Alert

All New Hosts Vulnerable Hosts IP Communication IP Traffic IP Statistics OT Behavior (IP) OT Behavior (Ethernet) Suricata

✓ In Learning & Detection Process

Add to detection exclusion list

Detection Date and Time	IP Address	MAC Address	Vendor	Destination IP Address : Service (port)	Source IP Address : Service (port)	Host Name	OS
2024/12/02 17:06:50	172.16.236.13	00:0c:29:71:12:2e	VMware, Inc.	172.16.236.255:netbios-ns* (137/udp), netbios-dgm* (138/udp), 192.168.45.1:syslog* (514/udp), 192.168.45.11:Echo_Reply (0/icmp), domain* (53/udp), kerberos* (88/tcp), rtp* (123/udp), epmap* (135/tcp), ldap* (389/tcp), microsoft-ds* (445/tcp), (49671/tcp), (49676/tcp), 192.168.45.17:Echo_Reply (0/icmp), epmap* (135/tcp), netbios-ns* (137/udp), (49676/tcp), (49693/tcp), 192.168.45.20:Echo_Reply (0/icmp), epmap* (135/tcp), netbios-ns* (137/udp), (49172/tcp), 192.168.100.131:http* (80/tcp), 224.0.0.251:mDNS* (5353/udp), 224.0.0.252:llmnr* (5355/udp)	192.168.100.131: (8484/tcp)	VAGRANT-2008R2	Windows Server 2008R2
2024/12/02 17:06:50	192.168.45.20	00:0c:29:c2:25:f9	VMware, Inc.	192.168.45.1:netbios-dgm* (138/udp), syslog* (514/udp), 192.168.45.2:bootps* (67/udp), 192.168.45.11:domain* (53/udp), kerberos* (88/tcp), epmap* (135/tcp), netbios-ns* (137/udp), netbios-dgm* (138/udp), netbios-ssn* (139/tcp), ldap* (389/tcp), (49667/tcp), microsoft-ds* (445/tcp), (49667/tcp), 192.168.45.255:netbios-ns* (137/udp), netbios-dgm* (138/udp), 192.168.100.131:http* (80/tcp), netbios-ns* (137/udp), 224.0.0.252:llmnr* (5355/udp), 239.255.255.255:ssdp* (1900/udp), 255.255.255.255:bootps* (67/udp)	192.168.45.1:Destination_Unreachable (3/icmp), netbios-ns* (137/udp), netbios-ssn* (139/tcp), microsoft-ds* (445/tcp), 192.168.45.17:netbios-ns* (137/udp), netbios-ssn* (139/tcp), microsoft-ds* (445/tcp), 192.168.100.131:Destination_Unreachable (3/icmp)	WIN7-CLIENT-01	Windows 7
2024/12/02 16:13:43	192.168.100.10	70:58:12:23:c4:33	Panasonic Corporation AVC Networks Company	192.168.100.254:http-alt* (8080/tcp), 192.168.100.255:netbios-dgm* (138/udp)		CF-S10X02	Windows 7
2024/12/02 16:11:41	192.168.1.37	08:00:27:fb:de:c8	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WINNT4	WindowsNT 4.0
2024/12/02 16:11:41	192.168.1.37	08:00:27:fb:de:c8	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WINNT4	WindowsNT 4.0
2024/12/02 16:11:41	192.168.1.37	08:00:27:fb:de:c8	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WINNT4	WindowsNT 4.0
2024/12/02 16:11:41	192.168.1.37	08:00:27:fb:de:c8	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WINNT4	WindowsNT 4.0
2024/12/02 16:11:41	192.168.1.35	08:00:27:b9:d0:0a	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WIN2K	Windows 2000
2024/12/02 16:11:41	192.168.1.35	08:00:27:b9:d0:0a	PCS Systemtechnik GmbH	192.168.1.255:netbios-dgm* (138/udp)		SNG-WIN2K	Windows 2000

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

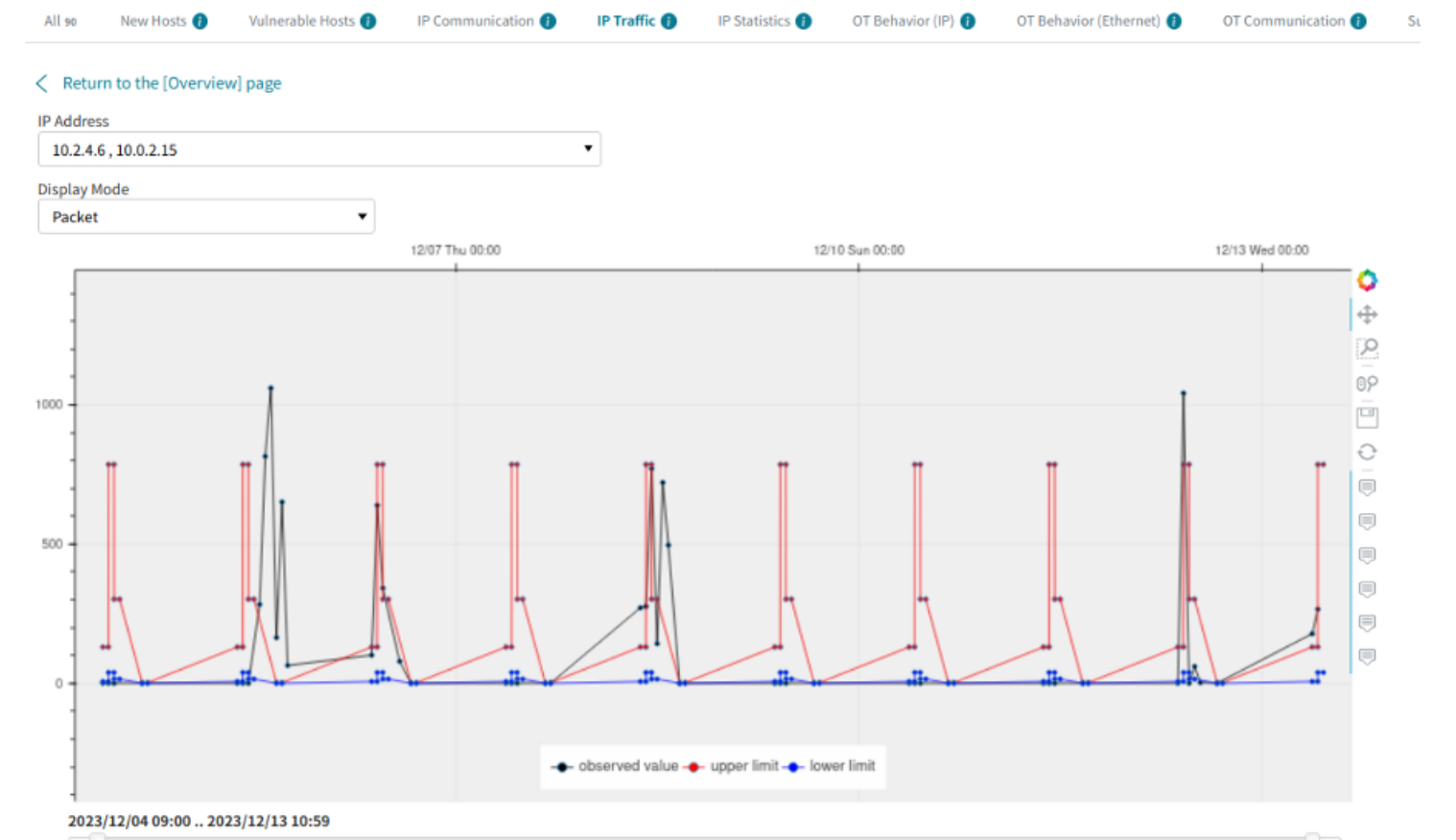
- Learn the traffic volume for each host pair during regular operations
- Automatically calculate thresholds for different time periods

Detection of Unusual IP Communication

Detection Date and ...	Source IP Address	Source Port	Destination IP Address...	Destination Port	Protocol
例: 1970/01/01 09:00:00	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

Detection of Unusual IP Traffic

Detection Alert



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

- Detect communications that match known attack patterns

Detection of OT Behavior

Detection Alert

All New Hosts Vulnerable Hosts IP Communication IP Traffic IP Statistics OT Behavior (IP) OT Behavior (Ethernet) Suricata

In Learning & Detection Process

Add to detection exclusion list

<input type="checkbox"/>	Detection Date and Time	Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	OT Protocol	Function
<input type="checkbox"/>	Example: 1970/01/01 09:00:00	Example: 192.168.2.0/24		Example: 192.168.2.0/24				
<input type="checkbox"/>	2024/12/02 19:50:33	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-slaveConfig
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-networkConfigTst
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-networkConfigMain
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-cyclicConfigRecvInfo
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-cyclicConfigRecvSubPayload
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-cyclicConfigTmSubPayload
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-cyclicConfigMain
Done	2024/12/02 17:15:56	192.168.3.1	45238	192.168.3.253	45238	udp	cclink_ie_tsn	slmp-notification
Done	2024/12/02 17:15:56	192.168.3.253	45238	192.168.3.255	45238	udp	cclink_ie_tsn	slmp-notification

Showing 1 to 10 of 10 rows

Detection of Signature

Detection Alert

All 90 New Hosts Vulnerable Hosts IP Communication IP Traffic IP Statistics OT Behavior (IP) OT Behavior (Ethernet) OT Communication Suricata

Add to detection exclusion list

<input type="checkbox"/>	Detection Date and Time	Source IP Address	Source Port	Destination IP Address	Destination ...	Protocol	Suricata	Threat Category	Severity
<input type="checkbox"/>	2023/12/12 08:54:46	a:a:a:a:a:a	20572	192.168.145.254	3394	6	ET SCAN MS Terminal Server Traffic on Non-standard Port	Attempted Information Leak	2
<input checked="" type="checkbox"/>	2023/12/12 08:54:46	a:a:a:a:a:a	20656	192.168.146.254	5647	6	ET SCAN MS Terminal Server Traffic on Non-standard Port	Attempted Information Leak	2
<input type="checkbox"/>	2023/12/12 08:54:46	a:a:a:a:a:a	19670	192.168.138.254	3039	6	ET SCAN MS Terminal Server Traffic on Non-standard Port	Attempted Information Leak	2

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

#...	IPv4 Addresses	IPv6 A...	MAC Address	Vendor	OS	First Seen	Last Seen	Register
1	10.0.0.100		b8:31:b5:36:86:95	Microsoft Corporation		2025-02-12 21:28:05	2025-02-12 21:59:57	Registered
2	192.168.0.100		b8...					

Showing 1 to 2 of 2 rows

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 Connected Hosts Detection

Detection Alert

All **New Hosts** | Vulnerable Hosts | IP Communication | IP Traffic | IP Statistics | OT Behavior (IP) | OT Behavior (Ethernet) | Suricata

In Learning & Detection Process

Register to learned list | Delete all alerts | CSV

Registration Details	Detection Date and Time	IP Address	MAC Address	Vendor	Destination IP Address : Ser...	Source IP Address : Service (...)
<input type="checkbox"/>	Example: 1970/01/01	Example: 192.0.2...	Example: 00:00:5e...		Example: https* (443/udp)	Example: https* (443/udp)
<input type="checkbox"/>	2024/12/02 09:05:06	172.16.134.128	00:0c:29:5f:70:ce			

Showing 1 to 1 of 1 rows

Notification Settings

When setting multiple email addresses, please separate them with comma (up to 5).
Example: aaa@example.com, bbb@example.com

Type	Notification Settings
New Hosts	Notify only new hosts not in the register
Vulnerable Hosts	Notify All
IP Communication	Notify All
IP Traffic	Notify All

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

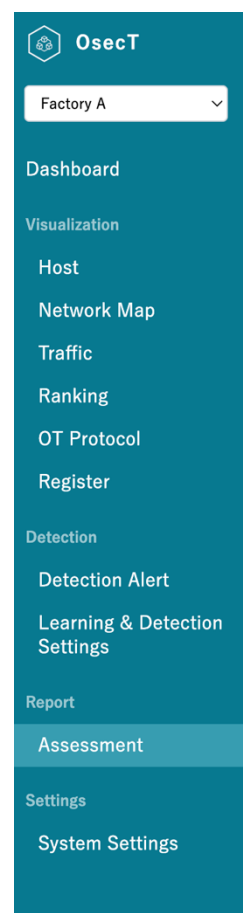
Output in an editable PowerPoint format

List hosts and those with unsupported OS versions

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

Assessment

Assessment Report File



Assessment Report

Report Download



Please accumulate data before downloading the report.

2. List of detected hosts

A total of 255 hosts were detected on the network.

The report displays information on 50 hosts. For the full information, please refer to the attached Excel file.

If there is any security risks

It is recommended to check them through

If any host that reasons may be

- The communication point.
- No communication
- Other reasons

9. List of hosts using VNC and RDP

3 hosts using VNC and RDP were detected. Hosts utilizing VNC or RDP may accept remote connections from external sources.

Hosts using (Remote connection)

The server's RDP, please using the is conducted

9. List of hosts using VNC and RDP (1/1)

IPv4 Address	IPv6 Address	MAC Address	Vendor	Connecting Service	Connected Service	Host Name	OS	First Seen	Last Seen
10.62.200.21		86:ea:71:38:7d:78	Unregistered(86:ea:71)	epmap* (135/tcp),netbios-ns* (137/udp),ms-wbt-server* (3389/tcp)			Windows 7/8	2024-12-24 15:09:46	2025-02-04 09:59:46
10.62.200.64		86:ea:71:38:7d:78	Unregistered(86:ea:71)	epmap* (135/tcp),netbios-ns* (137/udp),ms-wbt-server* (3389/tcp)			Windows 7/8	2024-12-24 15:09:53	2025-02-04 09:59:32
10.62.200.152		86:ea:71:38:7d:78	Unregistered(86:ea:71)	epmap* (135/tcp),netbios-ns* (137/udp),ms-wbt-server* (3389/tcp)			Windows 7/8	2024-12-24 15:10:19	2025-02-04 09:59:52

