



Development and demonstration of network security system using AI for maritime autonomous surface ship

IMO KASS Symposium

2024.05.14(Tue)
Penta Security Inc.

Index

I. Understanding the Significance of Cybersecurity in Maritime Operations

II. Development of AI-Based Network Security Solutions for Autonomous Ships

III. Practical Application: Demonstrating AI-Based Network Security Systems for Autonomous Ships

**IV. Anticipated Impact and Utilization Strategies of
AI-based Network Security Systems for Autonomous Ships**

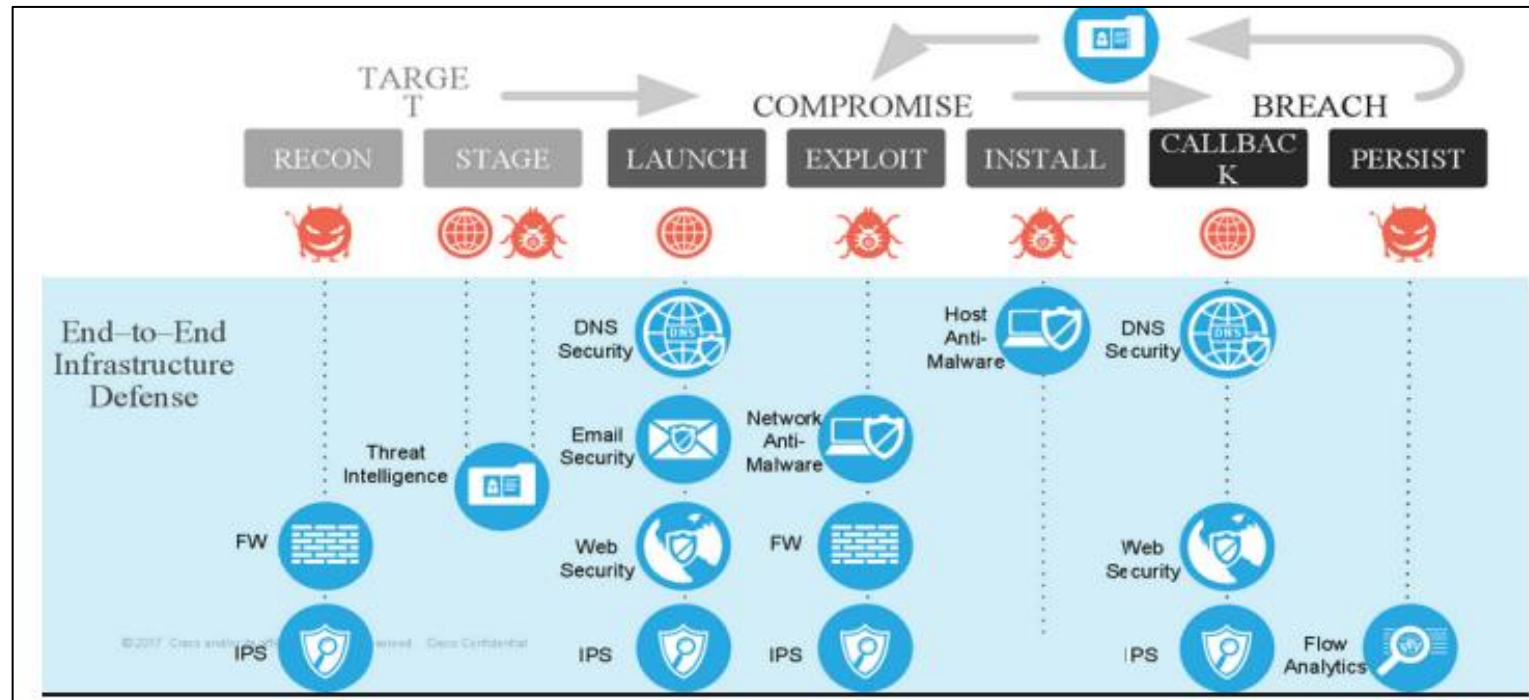
I. Understanding the Significance of Cybersecurity in Maritime Operations

1. Identifying Cybersecurity Threats
2. Cyber Attack Incidents
3. Cybersecurity Management for Autonomous Ships

Understanding the Significance of Cybersecurity in Maritime Operations

Identifying Cybersecurity Threats

- Maritime accidents are over six times more severe than road accidents
- The Fourth Industrial Revolution has increased connectivity between internal and external ship systems
⇒ **Increased exposure to cybersecurity threats**
- Attackers exploit vulnerabilities in ship networks to breach both IT and OT systems
- Attackers can gain unauthorized control over both ship IT and control system equipment.
⇒ **Application of Cyber Kill Chain-based response technology is necessary**



Cyber Kill Chain-based Response Technology

Understanding the Significance of Cybersecurity in Maritime Operations

Cyber Attack Incidents

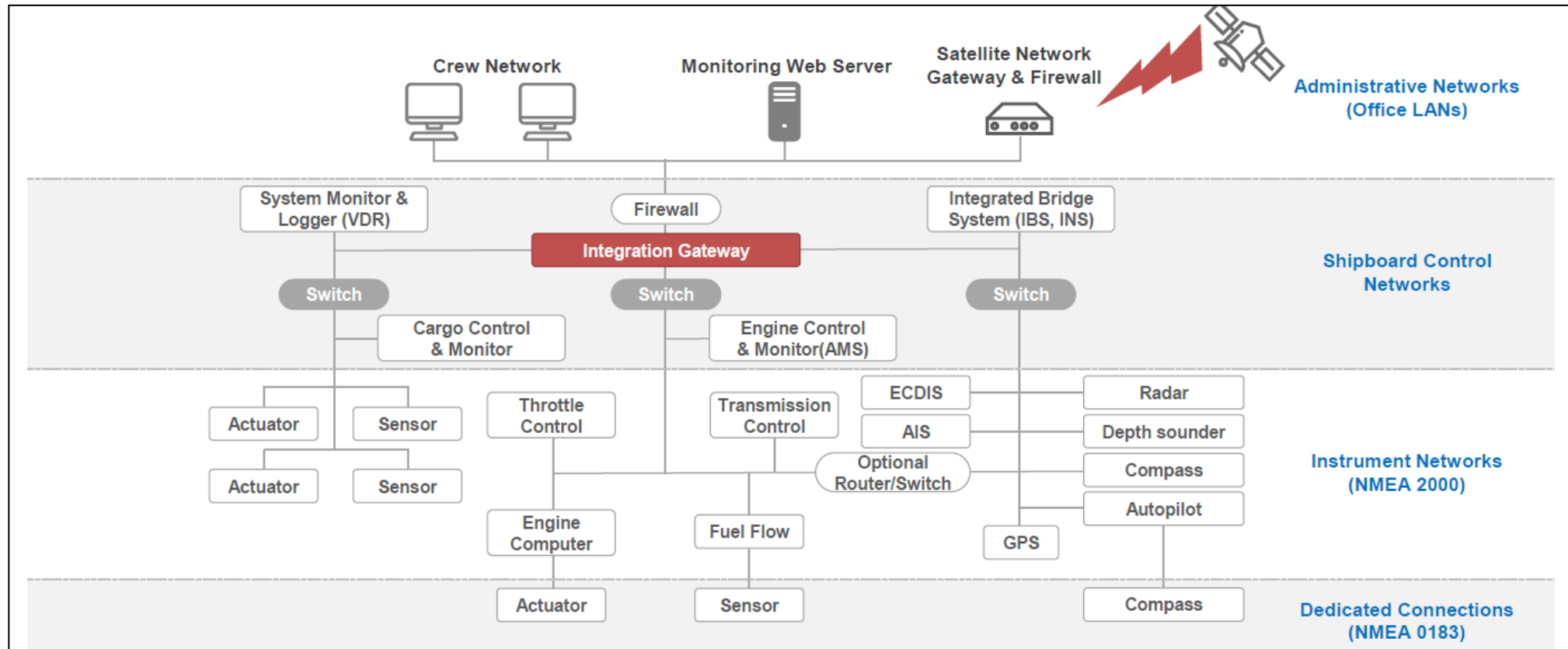
- Recent incidents have shown numerous cyber attacks targeting ships, shipping companies, and ports/harbors
- Substantial financial losses and severe human casualties are highlighted as consequences of cyber attacks

Year	Target	System	Attack Type	Consequences
2017	MAERSK	Terminal IT System	Ransomware	System outage for 3 weeks, resulting in losses of 300 billion
2017	Container Ship	Ship Navigation System	Malware	Loss of Control for 10 hours
2017	Clarkson	Company IT System	Insider Threat	Attempted Company data breach
2018	Shipping Company	Company Email	Spear Phishing	Estimated annual losses of 100 billion
2018	COSCO Shipping	IT System	Ransomware	Delayed cargo transportation
2018	Port of Barcelona	Port IT System	Ransomware	System shutdown And forensic investigation
2018	Port of San Diego	Port IT System	Ransomware	System shutdown And forensic investigation
2019	Automobile Carrier	Ship IT System	Ransomware	Targeted system formatting
2019	British Maritime Co.	Company IT System	Ransomware	Stock price decline, forensic investigation
2020	CMA CGM	Company IT System	Ransomware	Network system downtime for 2 weeks
2021	Transnet SOC	Port IT System	Ransomware	All port operations suspended
2022	Sembcorp Marine	Company IT System	Unauthorized Network Access	Data breach suspected
2022	Voyager Worldwide	Company IT System	Suspicious Cyber Attack	All system down
2023	Port of Lisbon	Company IT System	Ransomware	Internal data breach

Understanding the Significance of Cybersecurity in Maritime Operations

Current Status of Cybersecurity Implementation

- Most older ships lack any installed security equipment
- Modern ships primarily have firewall equipment installed, with other security technologies often absent
⇒ Persistent exposure to cybersecurity
- The policies of these devices are mostly set to default even when firewall equipment is installed.



Understanding the Significance of Cybersecurity in Maritime Operations

Cybersecurity Management for Autonomous Ships

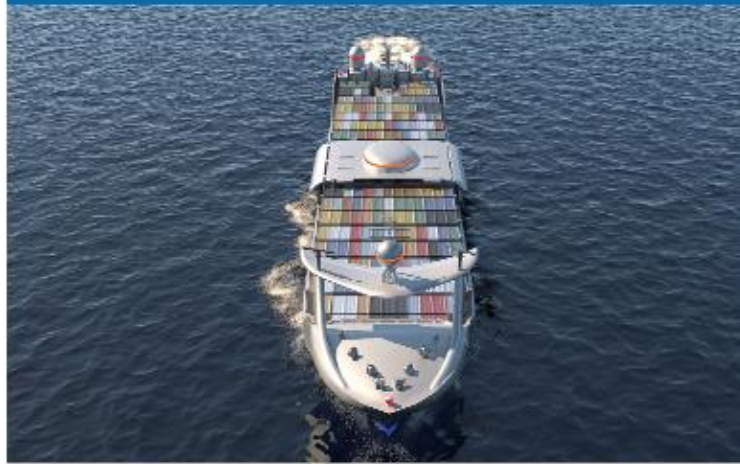
- Autonomous ships require technology capable of automatically responding to diverse attacks in the absence of security specialist
 - Necessary technologies include AI-based network anomaly detection and automatic policy updates based on detection results

Smart Ship



Comprehensive technology that applies advanced equipment and ICT to ships of meaning

Partial Autonomous Ship



Integrating IOT, platform, and control technology into existing ships The system replaces the role the crew was playing Vessels that can be operated with only minimum crew

Fully Autonomous Ship



Fully autonomous operation that can be operated without human intervention
Ship

II. Development of AI-Based Network Security Solutions for Autonomous Ships

1. Technical Development and System Architecture
2. AI-based Network Security Device
3. Deployment of Integrated Security Management System

Development of AI-Based Network Security Systems for Autonomous Ships

Technical Development Objectives

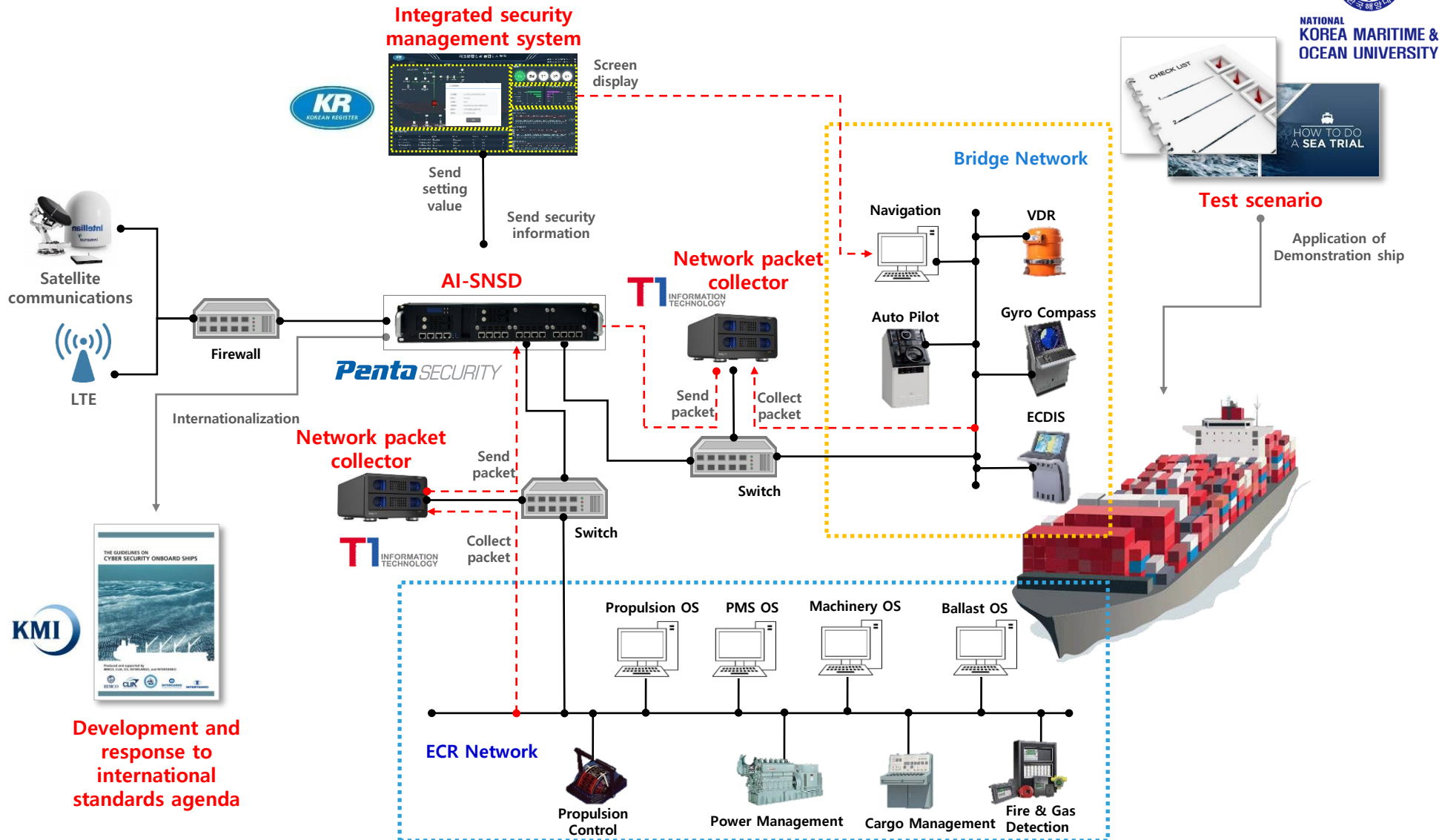
- Development of AI-based Ship Network Security Device (AI-SNSD) and Network Packet Collector
- Development of Integrated Security Management System for Autonomous Ships
- Development of technical standards and related agendas, including Cybersecurity Type Approval Documentation for Autonomous Ship
- Establishment of a verification environment for AI-SNSD and conducting tests on demonstration ships

Detailed Technical Development Objectives

<p>Penta Security</p> <p>AI-SNSD development</p>	<ul style="list-style-type: none"> ▪ Development of packet filtering technology based on firewall policies ▪ Development of attack detection and prevention features based on IDS/IPS ▪ Development of AI-based ship network anomaly detection and automatic 	<ul style="list-style-type: none"> ▪ AI-SNSD ▪ Manual 	<ul style="list-style-type: none"> ▪ All-in-One security device for ship-specific internal and external networks, aiming to reduce security system establishment costs ▪ Enhancing next-gen autonomous ship security with AI-based solutions.
<p>Korean Register</p> <p>Integrated security management system development</p>	<ul style="list-style-type: none"> ▪ Development of optimized remote cyber security management ▪ Visualization of integrated security technology ▪ Development of ICT asset management technology 	<ul style="list-style-type: none"> ▪ Integrated Security Management System (Software) ▪ Manual 	<ul style="list-style-type: none"> ▪ Establishment of a One-Stop security management system through the Integrated Security Management System
<p>Korea Maritime Institute</p> <p>Developing Cybersecurity related agendas</p>	<ul style="list-style-type: none"> ▪ Development of Integrated Cybersecurity Risk Management Framework for Autonomous Ships 	<ul style="list-style-type: none"> ▪ Response and Agenda development with International Organizations 	<ul style="list-style-type: none"> ▪ Establishment of proactive effects in identifying societal agendas regarding the functionality of next-generation autonomous ships
<p>KMOU</p> <p>Development of demonstration scenarios</p>	<ul style="list-style-type: none"> ▪ Development of demonstration scenarios for practical application ▪ Execution of tests based on demonstration scenarios 	<ul style="list-style-type: none"> ▪ Demonstration Scenario ▪ Demonstration Result Report 	<ul style="list-style-type: none"> ▪ Advancement of the realization and commercialization of autonomous ship cybersecurity through the demonstration scenarios
<p>T1IT</p> <p>Network packet collector development</p>	<ul style="list-style-type: none"> ▪ Collection of network packets from subnetworks not communicating with L3 ▪ Support network packet collectors for installation and testing of existing ships 	<ul style="list-style-type: none"> ▪ Network Packet Collector 	<ul style="list-style-type: none"> ▪ Securing a network analysis system in various ship network environments through network packet data collection

Development of AI-Based Network Security Systems for Autonomous Ships

Architecture



Development of AI-Based Network Security Systems for Autonomous Ships

AI-SNSD Overview

Category	Details
Type	2U (L)610mm,(W) 475mm, (H)85mm
CPU	Intel Xeon Processor Silver 4210 * 2
Memory	96GB (16GB * 6EA)
SSD	256GB + 1TB



AI-SNSD

Category	Details
Type	2U (L)712mm,(W) 439mm, (H)89mm
CPU	Intel Xeon Processor Silver 4208
Memory	128GB (16GB * 8EA)
SSD	96TB



Archiver Device

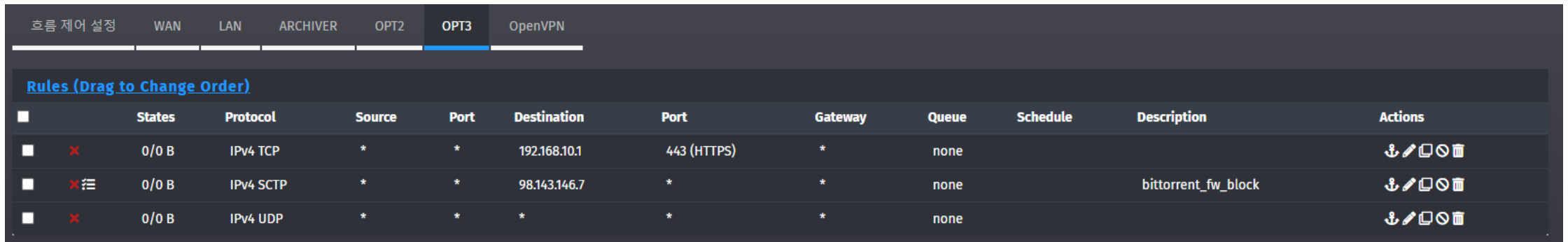
(Log Storage and Integrated Security Management System Installation)

Key Features	Function
Firewall	Block harmful packets incoming from external and internal sources based on policy (IP, Port, Protocol-based filtering).
IDS (Intrusion Detection System)	Detects packets containing harmful signatures incoming from external and internal sources.
IPS (Intrusion Prevention System)	Block harmful packets detected by IDS.
L3 Switch	Unique functions of L3 switch such as VLAN, NAT, Port Forwarding.
Logging/Monitoring	Monitor the status information and security function logs of AI-SNSD, and integration with the Integrated Security Management System.
AI-based Ship Network Anomaly Detection	<ul style="list-style-type: none"> - Analyze packets collectible at L2 and L3 switch levels using AI-based technology to detect signs of network anomalies. - Automatic IDS/IPS policy update.
SSL VPN	Virtual private network function for accessing ship's internal network from external network.
Anti Virus	Detects and blocks access to malicious websites and download of malicious files.

Development of AI-Based Network Security Systems for Autonomous Ships

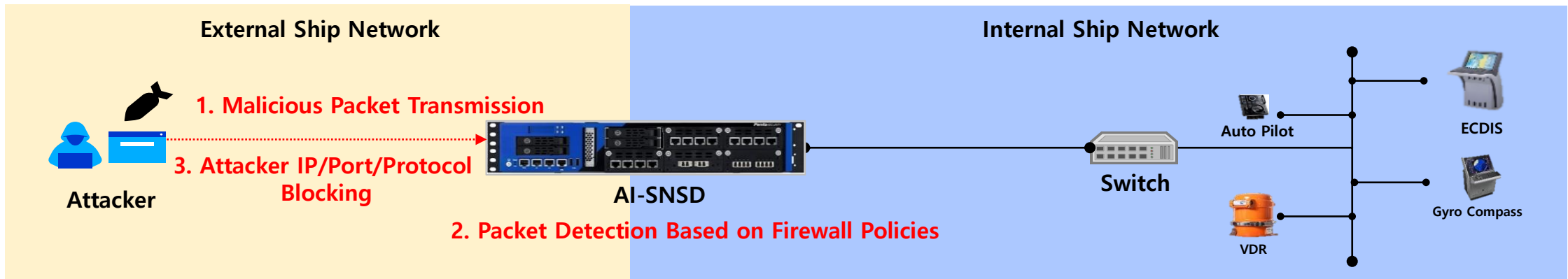
Features of AI-SNSD – Firewall

- Creation of firewall policies based on 5-tuple including Source IP/Port, Destination IP/Port, Protocol
- Support for both IPv4 and IPv6 systems
- Ability to create and apply firewall policies per interface



The screenshot shows the configuration interface for the AI-SNSD firewall. The 'OPT3' tab is selected. Below the navigation tabs, there is a section titled 'Rules (Drag to Change Order)'. The table below lists the configured rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	192.168.10.1	443 (HTTPS)	*	none			[Download] [Edit] [Copy] [Delete]
0/0 B	IPv4 SCTP	*	*	98.143.146.7	*	*	none		bittorrent_fw_block	[Download] [Edit] [Copy] [Delete]
0/0 B	IPv4 UDP	*	*	*	*	*	none			[Download] [Edit] [Copy] [Delete]

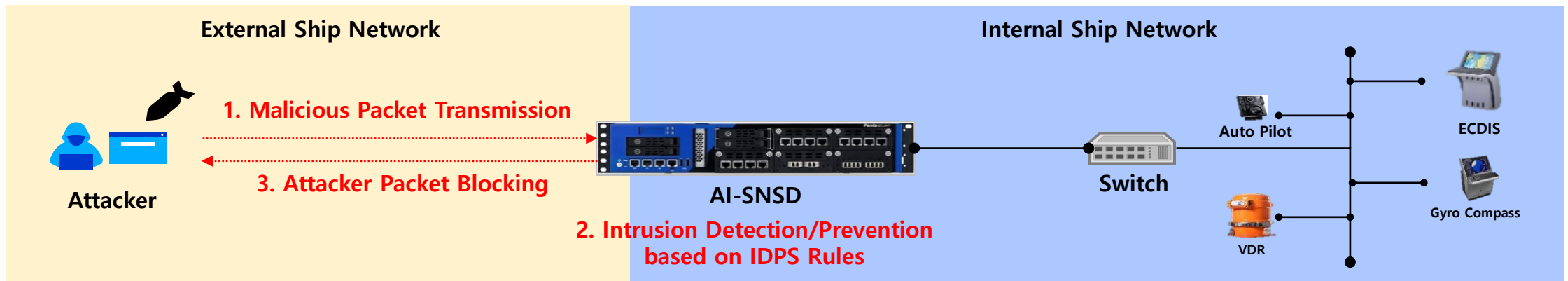


Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – IDS (Intrusion Detection System) / IPS(Intrusion Prevention System)

- latest Snort detection policies, Support for policy updates based on ETOpen detection policies
- Implemented 2,002 attack detection and blocking policies including Malware, Web Attack, DoS, Worm, Scada, Bot cc, Phishing, etc.

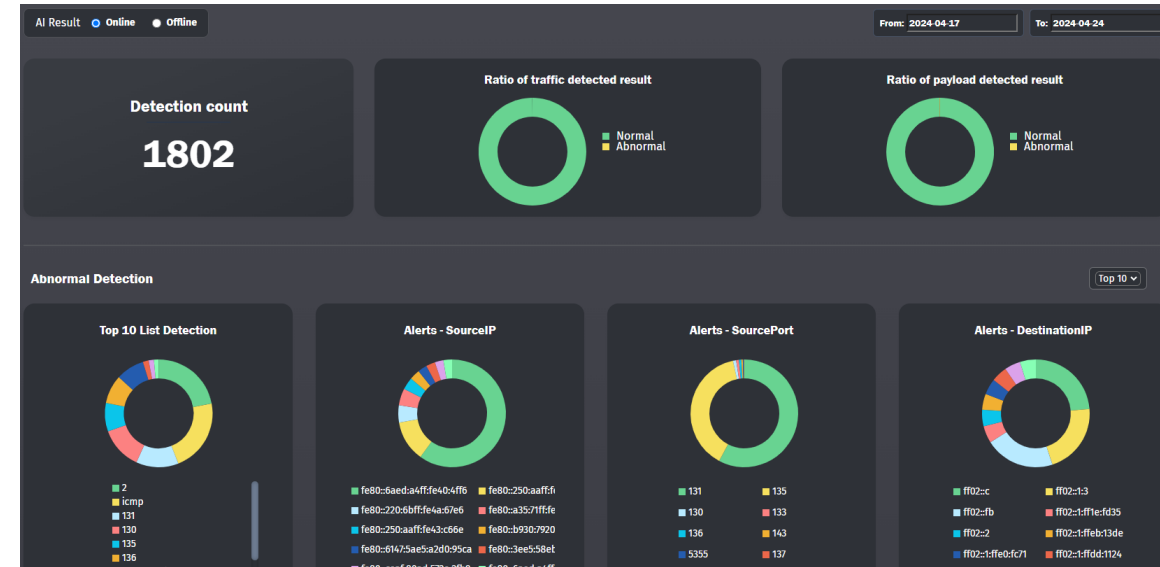
State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
🕒	⚠️	1	2240000	tcp	any	any	any	any	test rules 20240304 1208
🕒	✅	1	2026420	http	\$HOME_NET	any	\$EXTERNAL_NET	any	ET INFO Generic 000webhostapp.com POST 2018-09-27 (set)
⊗	⚠️	1	2044244	http	\$HOME_NET	any	\$EXTERNAL_NET	any	ET MALWARE Win32/Stealc Requesting browsers Config from C2
⊗	⚠️	1	2044246	http	\$HOME_NET	any	\$EXTERNAL_NET	any	ET MALWARE Win32/Stealc Requesting plugins Config from C2
⊗	⚠️	1	2049087	http	\$HOME_NET	any	\$EXTERNAL_NET	any	ET MALWARE Win32/Stealc/Vidar Stealer Style Headers In HTTP POST
🕒	⚠️	1	2404300	ip	\$HOME_NET	any	[103.82.243.5]	any	ET CNC Feodo Tracker Reported CnC Server group 1
🕒	⚠️	1	2404301	ip	\$HOME_NET	any	[158.220.95.214]	any	ET CNC Feodo Tracker Reported CnC Server group 2



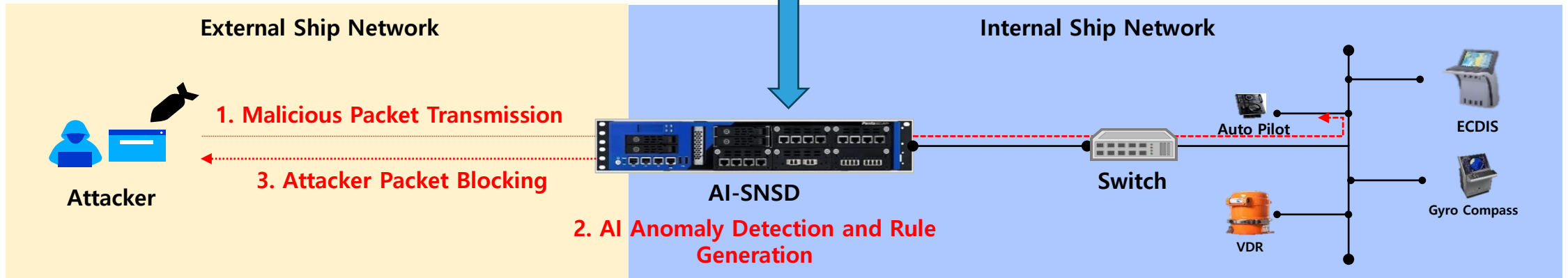
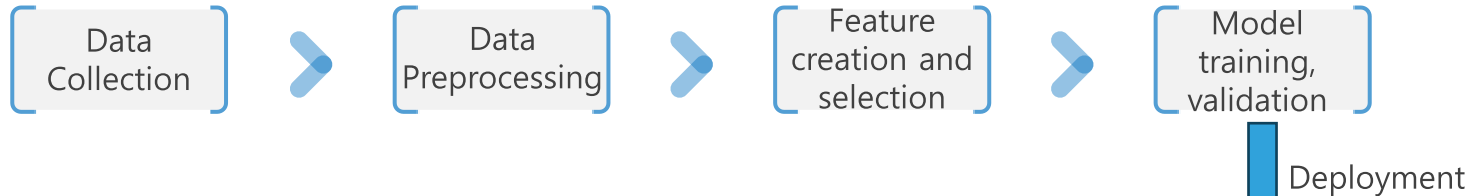
Development of AI-Based Network Security Systems for Autonomous Ships

Function of AI-SNSD – AI-based Anomaly Detection

- Collection of existing ship data for AI training
- Detect DoS, DDoS, and Scan attacks through network traffic analysis
- Detect SQL Injection, Cross-Site Scripting, Directory Traversal, Command Injection, Buffer Overflow through payload analysis of packet



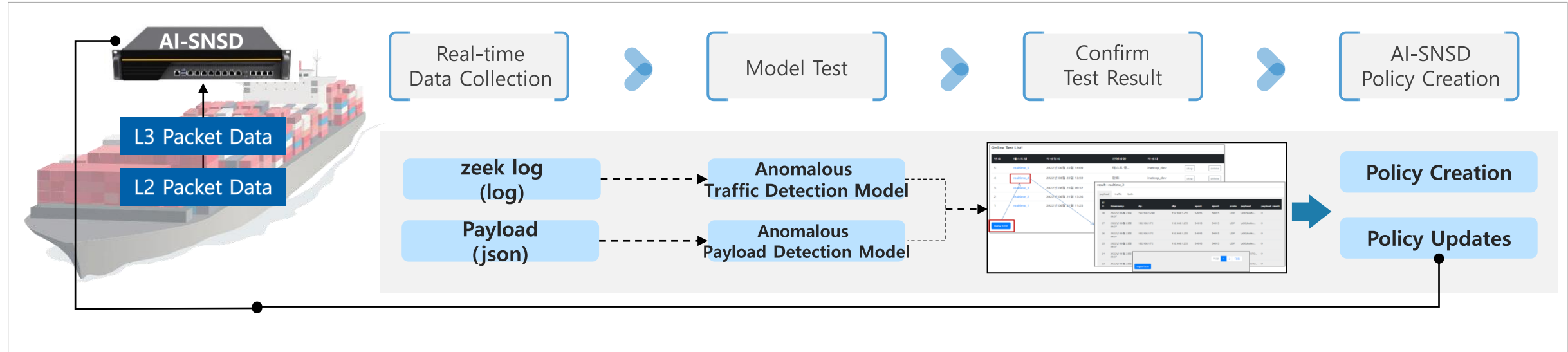
AI Model Creation Process



Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – AI-based Automatic Policy Updates

AI-based Threat Response Process



AI-SNSD Policy Creation Process

1. Anomalous Traffic Detection -> Block based on 5-tuple (srcip, dstip, srcport, dstport, protocol)

ex) alert udp \$EXTERNAL_NET any -> \$HOME_NET 1900 (msg:"Denial of Service / Xerox - Phaser 8400 / Printer"; classtype: Denial-of-Service_Null-Packet; dsize:0; sid:20000031;)

2. Anomalous Payload Detection -> Block based on malicious patterns

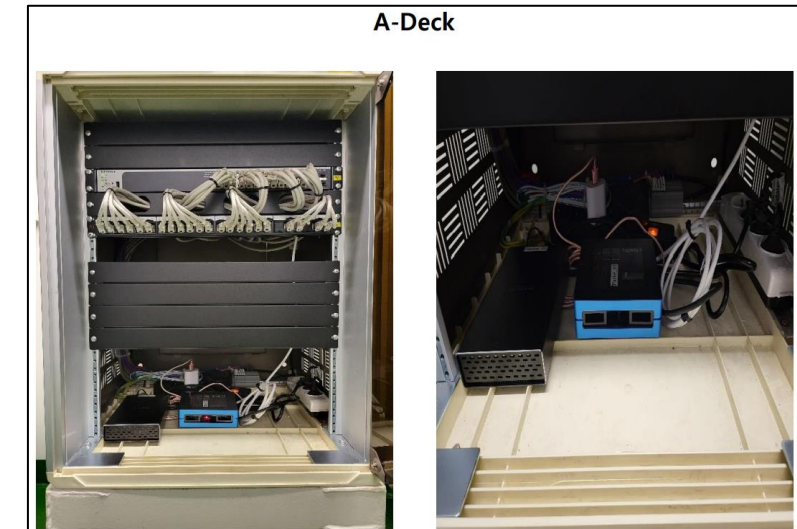
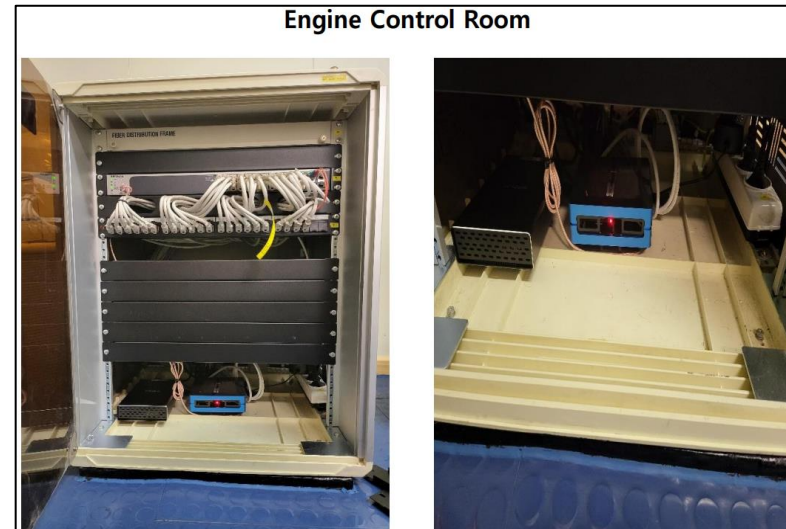
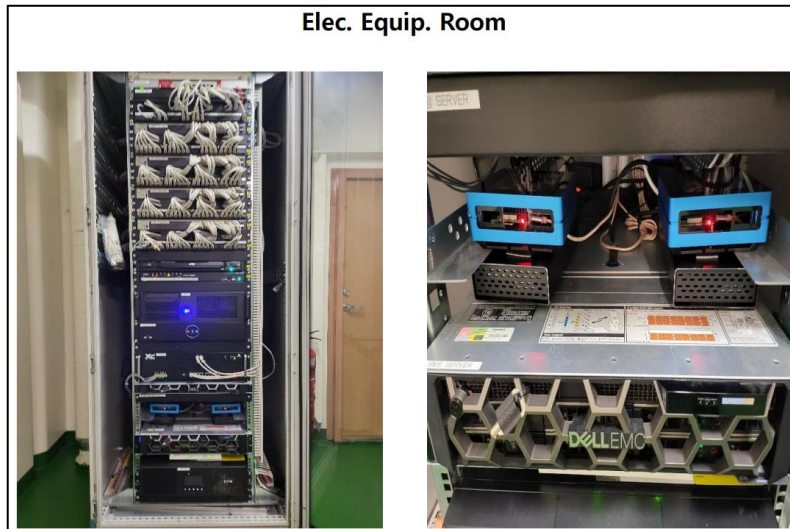
ex) alert tcp any any -> any 8000 (msg:"Command Injection / D-Link DWR-116 through 1.06, DWR-512 through 2.02."; content : "GET";http_method; content : "%7C";nocase; content : "cat%20";nocase; content : "passwd";nocase; classtype: Command-Injection_Request-Parameter; sid:20000090;)

Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – Data Collection and Analysis for AI Training

- Installation of network packet collectors on operating container ships for data collection (4 months).
- Network packet collectors are installed on an LNG vessel to collect data for a year.

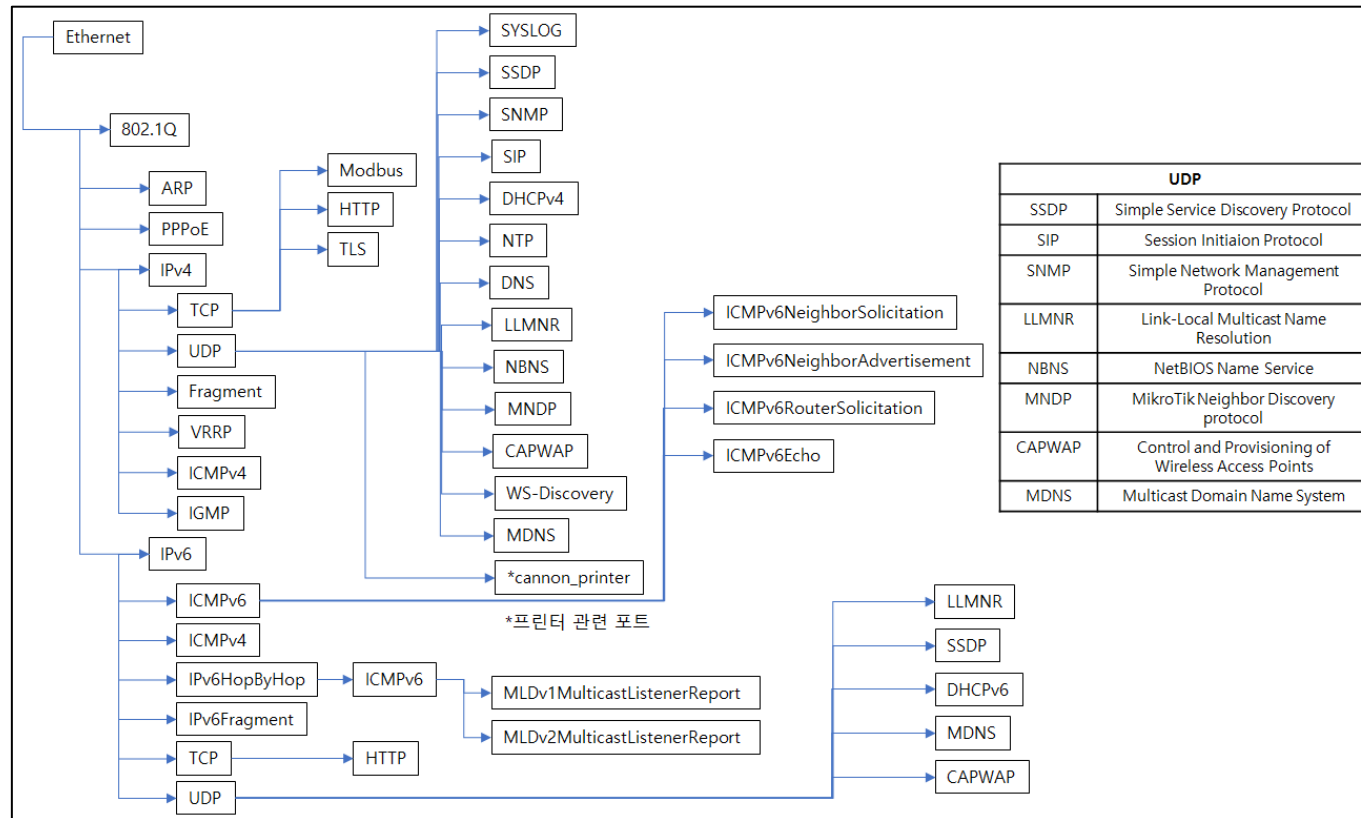
Packet Collector	packet01	packet02	packet03	packet04
Location	• Electric Equipment Room	• Electric Equipment Room	• A-Deck	• ECR
Packet Capacity	• 70GB	• 3TB	• 3.7TB	• 1.2TB
Packet count (1 pcap= about 292MB)	• 245	• 10,687	• 13,309	• 4,250



Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – Data Collection and Analysis for AI Training

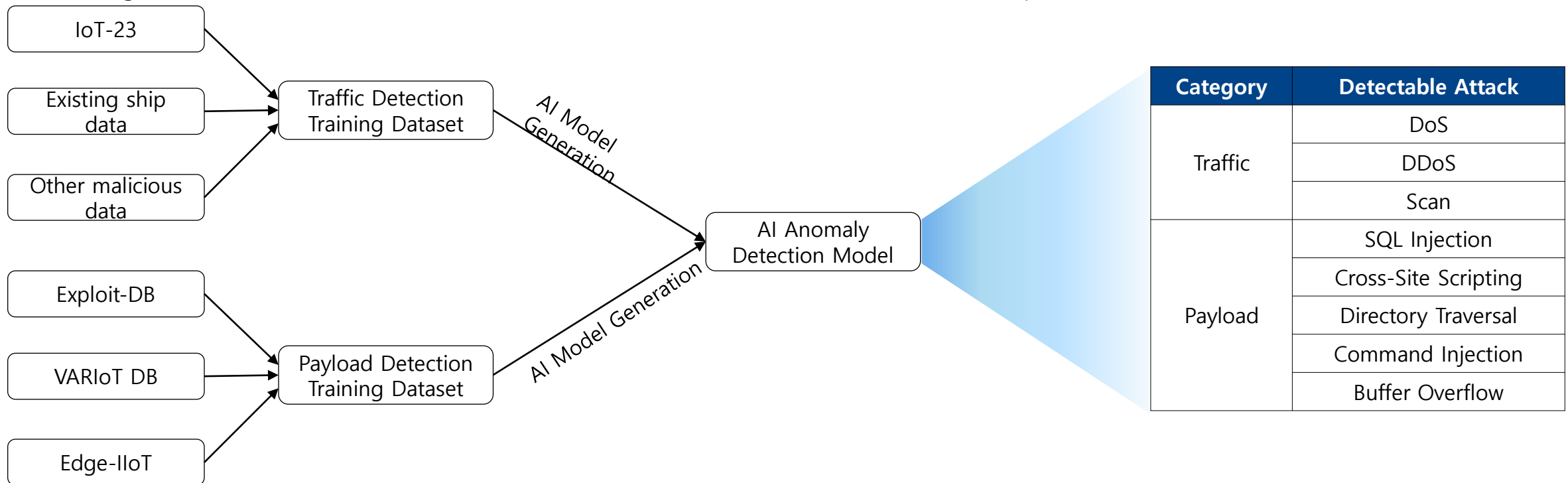
- Identification of SNMP and SSDP protocols, commonly used in DoS and DDoS attacks ⇒ **Need for DoS and DDoS detection technology**
- Identification of SMB port commonly used in ransomware attacks ⇒ **Need for network scan detection technology**
- Identification of Large number of HTTP web communication protocol packets ⇒ **Need for Web attack detection technology**



Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – Dataset Construction and Model Generation for AI Training







- Building traffic detection training datasets from IoT-23(IoT device network traffic open dataset), data from existing ship, other malicious data (Internally)
- Construction of payload detection training datasets by creating malicious web payload
 - Referencing Exploit-DB, VARIoT DB, Edge-IIoT open dataset)
 - Creating an ensemble model based on RandomForest, XGBoost, and LGBM models to enhance the performance of the AI detection model

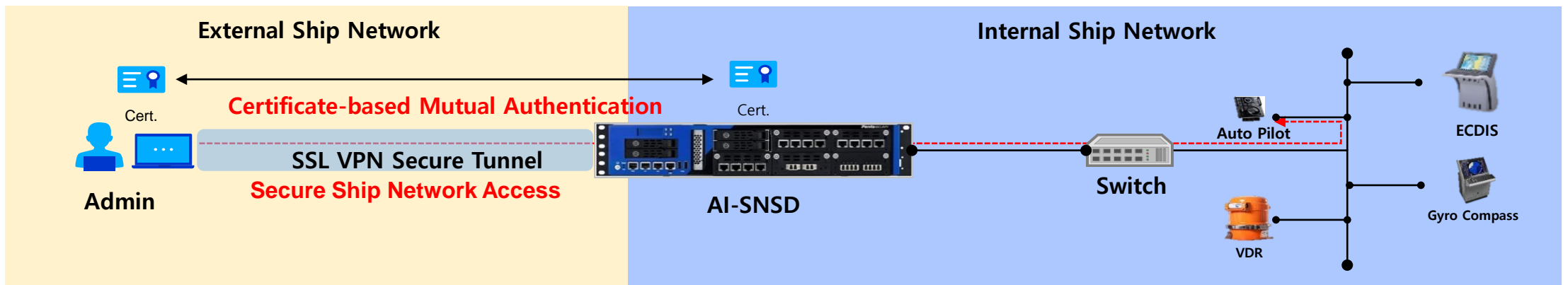


Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – SSL VPN

- Enables secure access to internal ship equipment from external sources
- Access is restricted to users possessing certificates issued by AI-SNSD
- Ensures data confidentiality and integrity through SSL VPN technology

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
AV_CA	✓	self-signed	0	CN=AV_CA Valid From: Tue, 19 Mar 2024 09:39:00 +0900 Valid Until: Fri, 17 Mar 2034 09:39:00 +0900	Squid (1)	  
snsd_vpn_CA	✓	self-signed	2	CN=snsd-vpn-cn Valid From: Tue, 19 Mar 2024 10:32:09 +0900 Valid Until: Fri, 17 Mar 2034 10:32:09 +0900		  



Development of AI-Based Network Security Systems for Autonomous Ships

Features of AI-SNSD – Antivirus using clamAV

- Detects and blocks malicious file downloads by users and devices within the ship
- Displays warning screens upon accessing malicious websites and redirects to safe sites
- Supports the latest engine through regular antivirus updates

SquidClamav 7.2 : Virus detected!

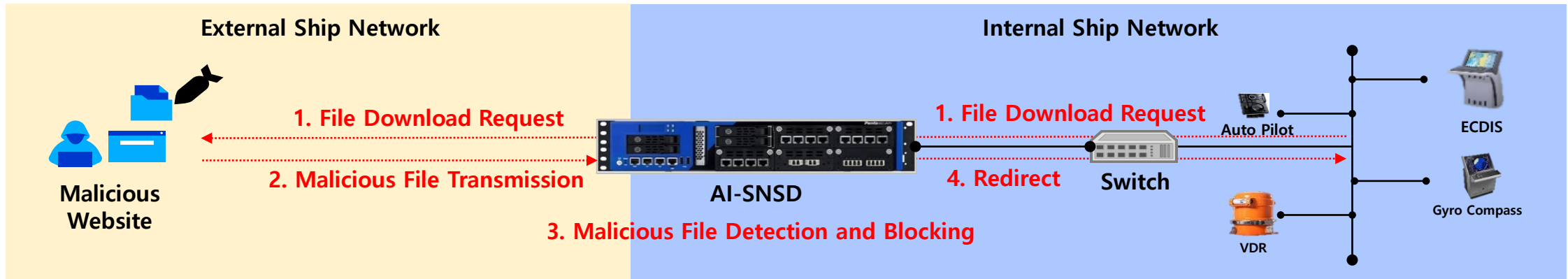
The requested URL contains a virus

Virus name:

This file cannot be downloaded.

Origin: /

Powered by [SquidClamav 7.2](#)



Development of AI-Based Network Security Systems for Autonomous Ships

Integrated Security Management System

- Monitors the current network status based on the overall network
- Monitors security information and AI-SNSD status through integration with AI-SNSD



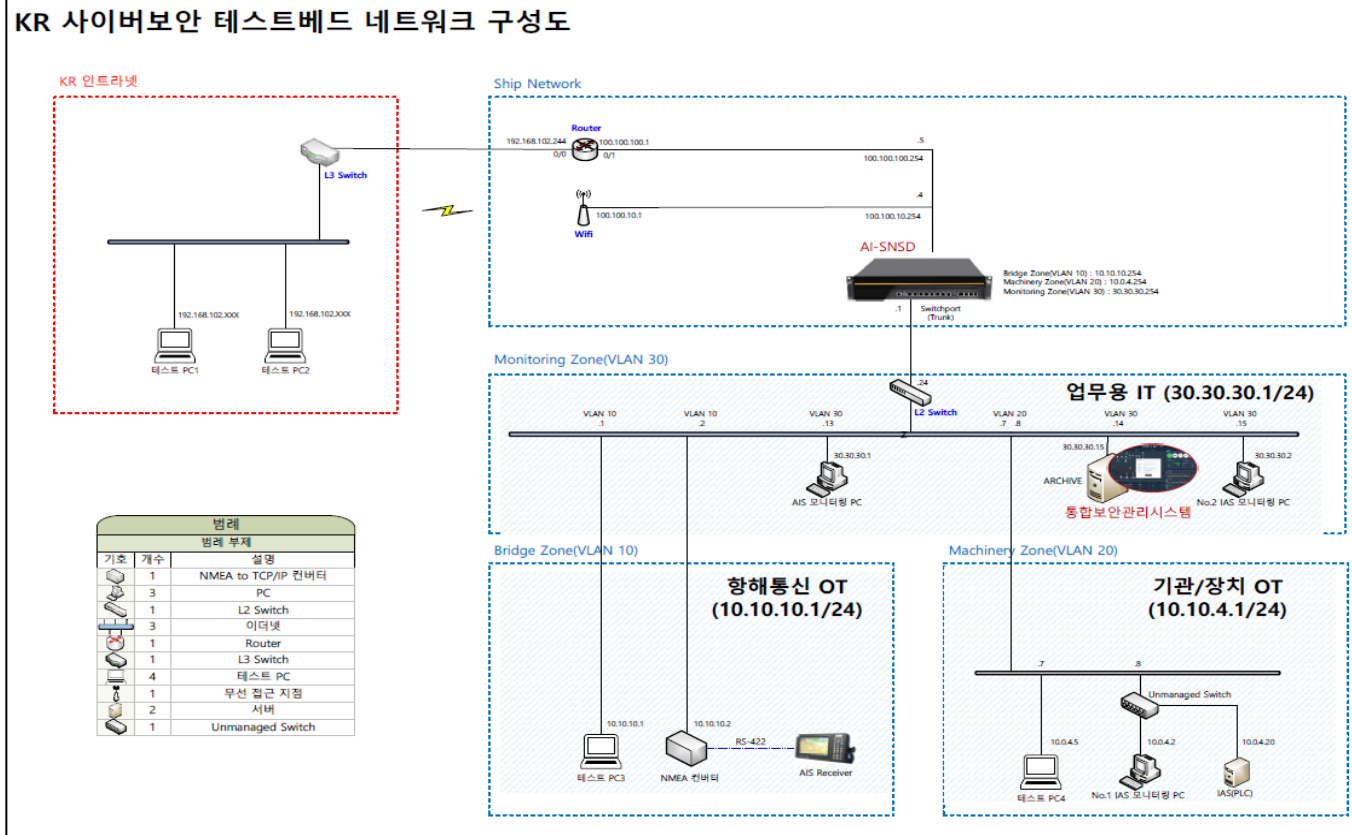
III. Demonstration of AI-Based Network Security Systems for Autonomous Ships

1. Demonstration on the Korea Register Ship Mockup Tool Testbed
2. Demonstration on the at KMOU Training Ship
3. Demonstration on the PAN Ocean Container Ship
4. Issuance of IACS UR E27 Certification

Demonstration of AI-Based Network Security Systems for Autonomous Ships

Demonstration on Korea Register Ship Mockup Tool Testbed

- Completed testing of AI-SNSD Firewall, IDS/IPS, and L3 Switch
- Completed testing of AI-SNSD and Integration with the Integrated Security Management System



Demonstration of AI-Based Network Security Systems for Autonomous Ships

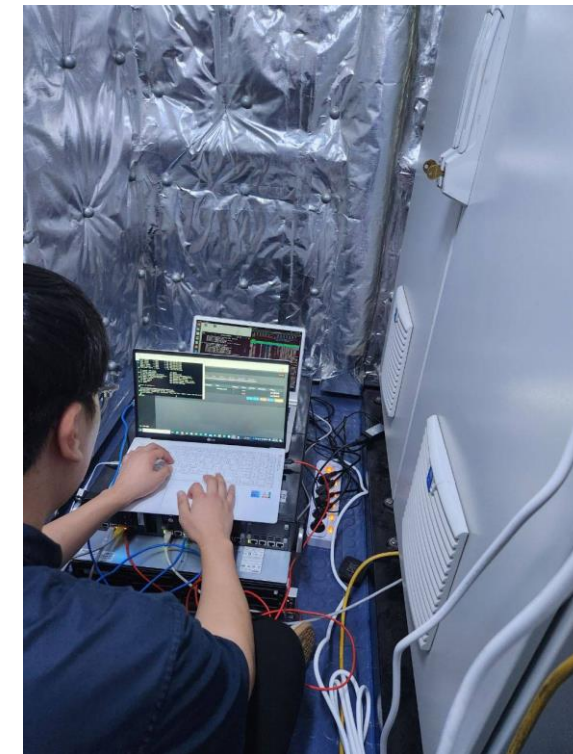
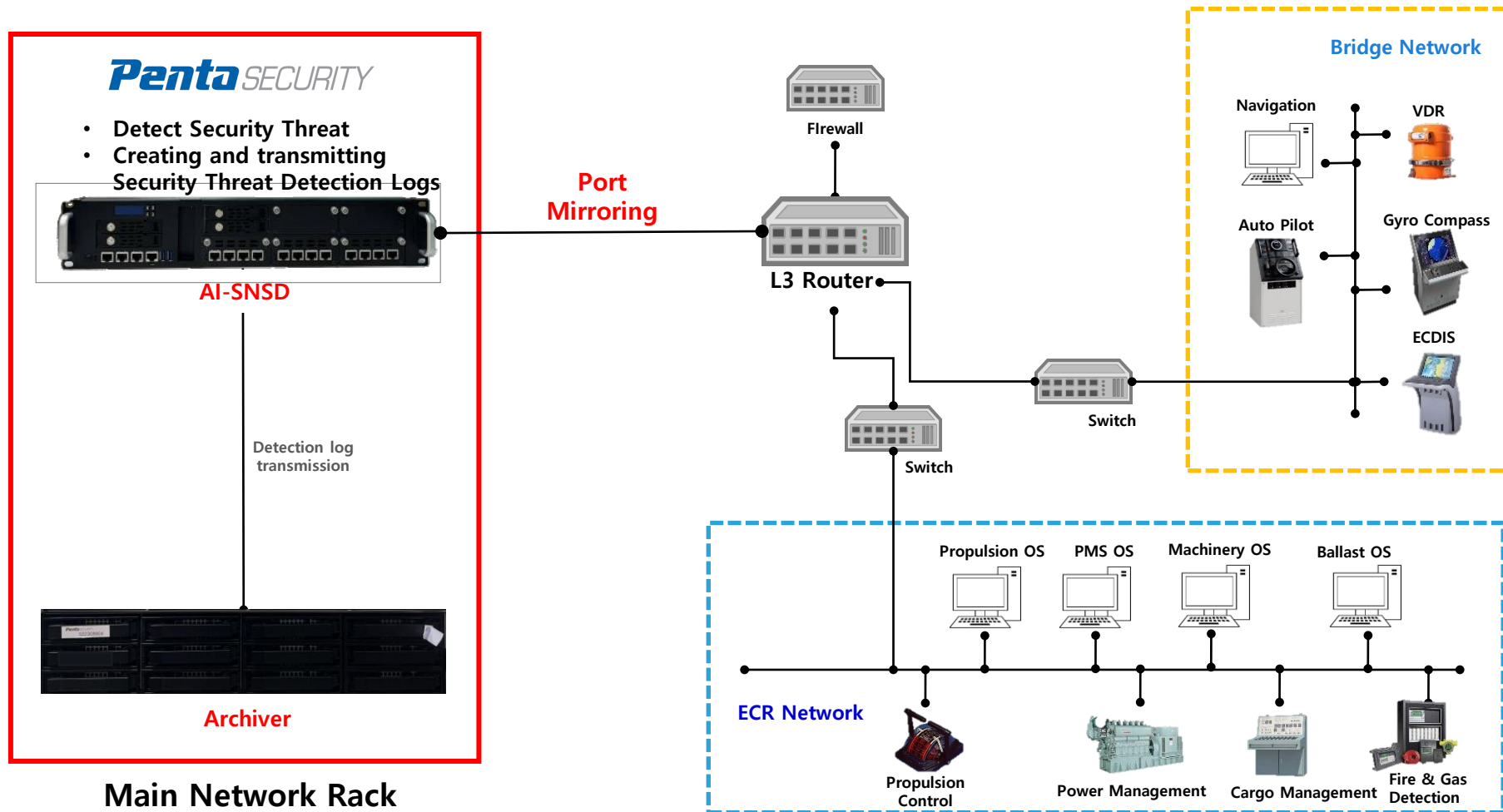
Demonstration on Korea Register Ship Mockup Tool Testbed

TC	Test Item	Objectives	Result
TC 1	(Function) Firewall – Blocking attempts to access restricted external websites	100% blocking rate	Satisfied
TC 2	(Function) Firewall – Blocking attempts to malicious external Ips	100% blocking rate	Satisfied
TC 3	(Function) Firewall - Blocking attempts to access ship's critical facilities	100% blocking rate	Satisfied
TC 4	(Function) Firewall - Blocking attempts to access ship's critical facilities	100% blocking rate	Satisfied
TC 5	(Function) IDS -Detecting attempts to access restricted external websites	100% detection rate	Satisfied
TC 6	(Function) IDS - Detecting attempts to transmit data to malicious external Ips	100% detection rate	Satisfied
TC 7	(Function) IDS - Detecting attempts to access ship's critical facilities	100% detection rate	Satisfied
TC 8	(Function) IDS - Detecting attempts to access ship's critical facilities	100% detection rate	Satisfied
TC 9	(Function) IDS - Blocking attempts to access restricted external websites	100% blocking rate	Satisfied
TC 10	(Function) IPS - Blocking attempts to transmit data to malicious external Ips	100% blocking rate	Satisfied
TC 11	(Function) IPS - Blocking attempts to access ship's critical facilities	100% blocking rate	Satisfied
TC 12	(Function) IPS - Blocking attempts to access ship's critical facilities	100% blocking rate	Satisfied
TC 13	(Non-Function) Installation - Testing AI-SNSD and Integrated Security Management System installation	Feasibility of Installation	Satisfied
TC 14	(Non-Function) Interoperability - Testing integration of AI-SNSD and Integrated Security Management System	100% integration rate	Satisfied

Demonstration of AI-Based Network Security Systems for Autonomous Ships

Demonstration of AI-SNSD on the KMOU (Korea Maritime & Ocean University) Training Ship

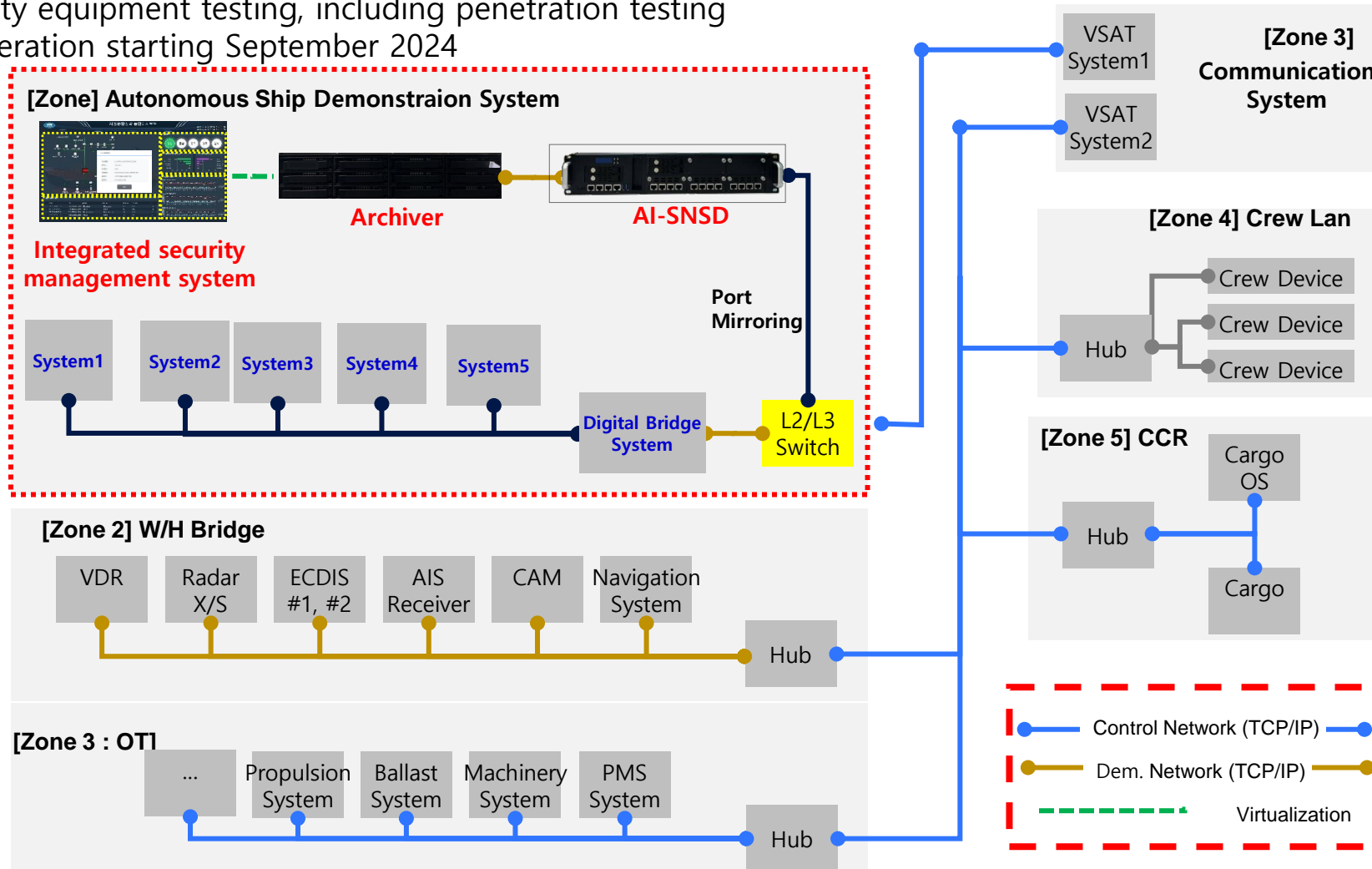
- Conducted AI-SNSD installation tests on training ships navigating in the waters of the Philippines, Taiwan, and Japan
- Successfully tested AI-SNSD's firewall, IDS/IPS, L3 switch, antivirus, VPN, and AI anomaly detection functionalities



Demonstration of AI-Based Network Security Systems for Autonomous Ships

Demonstration on the PAN Ocean Container Ship

- Completion of AI-SNSD equipment installation on PAN Ocean container vessel
- Scheduled security equipment testing, including penetration testing during vessel operation starting September 2024



Demonstration of AI-Based Network Security Systems for Autonomous Ships

Issuance of IACS UR E27 Certification

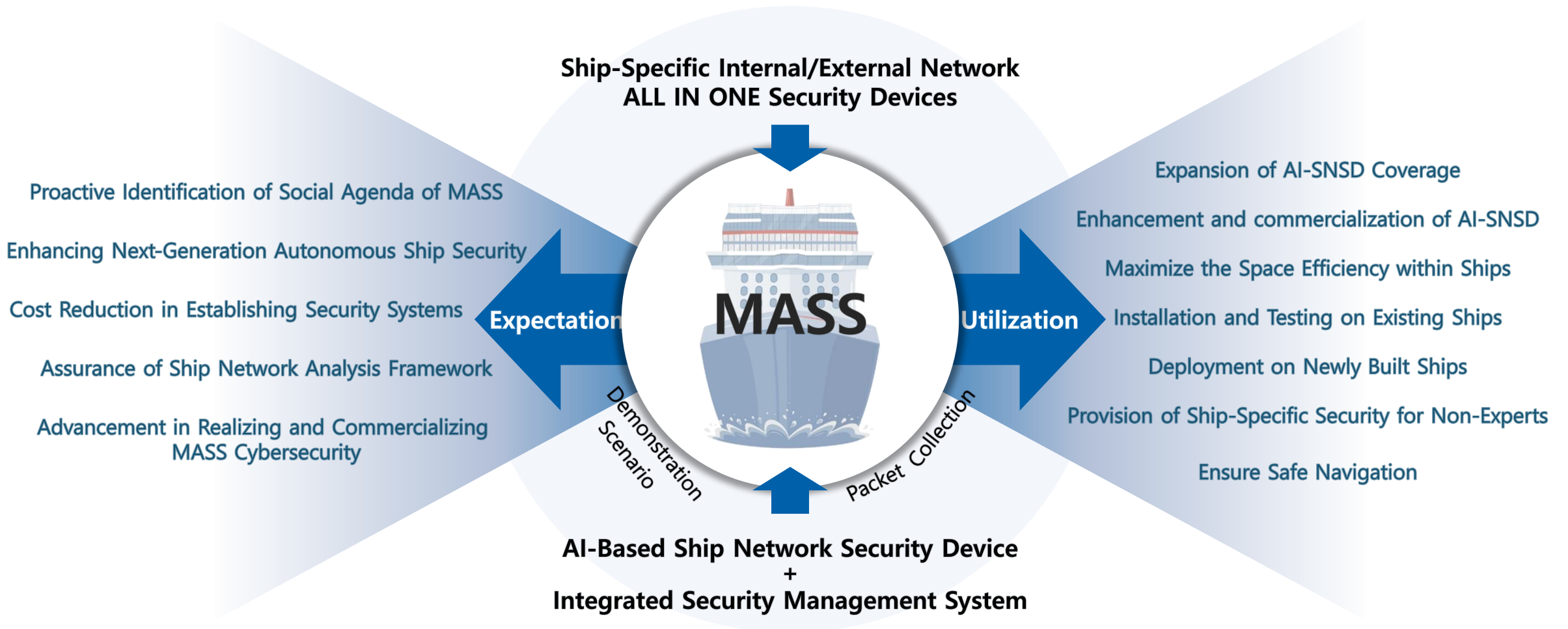
- CBS(Computer Based System) based onboard OT(Operation Technology) systems in vessels contracted after January 1, 2024, must obtain UR E27(Cyber Resilience of on-board system and equipment) certification.
- Additional feature development is currently underway to meet the requirements for UR E27 testing, with certification expected to be obtained by 2024.

Item No	Objective
1	Human user identification and authentication
2	Account management
3	Identifier management
4	Authenticator management
5	Wireless access management
6	Strength of password-based authentication
7	Authenticator feedback
8	Authorization enforcement
9	Wireless use control
10	Use control for portable and mobile devices
11	Mobile code
12	Session lock
13	Auditable events
14	Audit storage capacity
15	Response to audit processing failures

Item No	Objective
16	Timestamps
17	Communication integrity
18	Malicious code protection
19	Security functionality verification
20	Deterministic output
21	Information confidentiality
22	Use of cryptography
23	Audit log accessibility
24	Denial of service protection
25	Resource management
26	System backup
27	System recovery and reconstitution
28	Alternative power source
29	Network and security configuration settings
30	Least Functionality

IV. Expected Effects and Utilization Strategies of AI-Based Network Security Systems for Autonomous Ships

Expected Effects and Utilization Strategies of AI-Based Network Security Systems for Autonomous Ships



PentaSECURITY
cloud · iot · blockchain

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp



Overall Web Security
Solution Provider of
the Year 2021



Web Application
Security



Cyber Security Awards
Application Security
2020



IoT-based Smart
Security
Innovation Award 2020



TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2019



Cybersecurity
Excellence Awards
Winner 2018



Hot Company in
Web Application
Security for 2016



SC Magazine Europe
Best SME Solution

Gartner

Recognized on the
Gartner WAF
Magic Quadrant



ICSA Labs
Certified WAF



The First and Only
CCEAL4 Certified
WAF



PCI-DSS
Compliance