JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항공 우주 해상

J. Adv. Navig. Technol. 28(4): 497-506, Aug. 2024

해사 사이버 보안 대응을 위한 선박용 보안 정보와 이벤트 관리 시스템

Security Information and Event Management System for Ship Cyber Security

강 남 선[1] · 이 창 식[1] · 유 성 상[2] · 이 종 민[3]· 손 금 준[4*]
[1]이글루코퍼레이션 전략사업팀 · [2]중소조선연구원 특수선박지원센증팀 · [3]현대엘엔지해운㈜ IT팀 · [4]한국선급 사이버인증팀

Nam-seon Kang[1] · Chang-sik Lee[1] · Seong-sang Yu[2] · Jong-min Lee[3] · Gum-jun Son[4*]

[1]Strategic Business Division, IGLOO Corp., Seoul, 05836, Korea · [2]Research Institude of Medium & Small Shipbuilding, Busan, 46757, Korea · [3]Hyundai LNG shipping CO., LTD. Seoul, 04513, Korea · [4]Cyber Certification Team, Korean Register, Busan, 46762, Korea

[요 약]

본 연구에서는 해사 사이버 보안 규제와 고도화되는 사이버 위협에 대응하기 위한 기술로 선박용 보안 정보와 이벤트 관리기술을 제안하였다. 선박 사이버 보안 대응을 위한 대표기술인 네트워크 관리시스템과 보안 정보와 이벤트 관리의 주요 기술을 분석하고 이를 기반으로 선박용 보안 정보와 이벤트 관리 기술을 제안하며 선박에 최적화를 위해 국제해사기구의 해상 사이버 위협 관리 지침, IACS UR E26, 27 등 을 기반으로 선박용 보안 정보와 이벤트 관리의 주요 기능을 도출하고 선박의 이기종 장비에 대한 연동 및 정규화 방안과 선박 사이버 보안 위협의 식별을 위한 선박의 사이버 위협과 선박용 탐지 정책, 선박 운영 환경과 운영 인력을 고려한 선박 특화 기능을 정의하였다.

[Abstract]

In this study, we proposed security information and event management for ship as a technology to respond to maritime cybersecurity regulations and evolving cyber threats. We analyze the main technologies of network management system and security information and event management, which are representative technologies for responding to ship cyber security, and propose SIEM for ships based on this. Optimized for ships based on the International Maritime Organization's Maritime Cyber Threat Management Guidelines, IACS UR E26, 27, etc. Derive the main functions of the SIEM for ship, linkage and normalization plan for the ship's heterogeneous equipment, ship's cyber threat and ship detection policy to identify ship's cyber security threats, and ship's operating environment and operating personnel.

Key word : Security information and event management, Cyber resilience of ships, Cyber resilience of on board systems and equipment, Network management system, **S**hip security threats.

http://dx.doi.org/10.12673/jant.2024.28.4.497

Received 22 July 2024; **Revised** 27 August 2024
Accepted (Publication) 29 August 2024 (30 August 2024)

***Corresponding Author; Gum-jun Son**

Tel: +82-1566-1682
E-mail: gjson@krs.co.kr

Ⅰ. 서 론

해운 Shipping 4.0, 항만 Port 4.0, 조선 Smart ship 4.0, 해양 Marine 4.0 등 해양선박 분야에 4차 산업혁명 기술이 도입되면서 선박과 육상 간, 선박 내 주요 시스템 간에 다양한 네트워크와 정보 공유가 증가하고 있으며 이에 따라 해상에서의 선박 사이버 보안 위협도 높아지고 있다[1],[2].

2023년 DNV(Det norske veritas) 선급은 랜섬웨어로 인해 70개의 해운선사와 1,000척의 선박에 웹 기반 운영서비스가 중단되었고, 2019년 미국 컨테이너 선박에 멀웨어 공격을 받아 선박의 운항이 중단되었으며, 2018년 COSCO 해운의 화물 운송이 지연되는 등 수많은 사이버 사고가 발생하였다. 국내에서도 2019년 자동차운반선 내부 시스템, 2023년 액화천연가스 운반선 내부 시스템이 랜섬웨어에 감염되는 등 선박 사이버 사고가 잇따라 발생되고 있다[3],[4].

이처럼 높아지고 있는 해사 사이버 위협에 대응하기 위해 국제기구, 주요 해운국, 산업계에서는 사이버 보안 대응 지침 및 가이드라인을 개발・적용하고 있으며, 국제선급연합에서는 선박검사 항목에 사이버 보안과 관련된 항목을 추가함으로써 선박의 사이버 보안을 강화하고 있다[1],[2].

본 논문에서는 해사 사이버 보안 규제와 고도화되는 사이버 위협에 대응하기 위한 기술로 선박용 보안 정보와 이벤트 관리(SIEM; security information & event management) 기술을 제안하며, 이를 위해 2장에서 해사 사이버 보안 규제에 대한 산업계 현황을 파악하고 3장에서 선박 사이버 보안 대응을 위한 대표 기술인 네트워크 관리 시스템(NMS; network management system)과 SIEM의 주요 기술을 분석하며, 이를 바탕으로 4장에서 선박용 SIEM 솔루션을 제안한다.

Ⅱ. 선박 사이버보안 현황

국제해사기구(IMO; International Maritime Organization)는 2017년 해상 사이버 위협 관리지침(guideline on maritime cyber risk management)과 안전관리시스템에서의 사이버 위협 관리(maritime cyber risk management system)를 채택하였으며, 국제선급연합 (IACS; International Association of Classification System)은 2022년 선박의 운영기술이 중단되거나 손상될 경우 발생되는 사이버 사고를 줄이고 그 영향을 완화하기 위한 공통규칙 UR (Unified Requirements) E26 – 선박 사이버 복원력(cyber resilience of ships)과 UR E27 – 온보드 시스템 및 장비의 사이버 복원력 (cyber resilience of on-board systems and equipment)을 채택하고 2024년 1월 1일 이후 건조 계약되는 선박에 기술적 필수 요구사항으로 적용을 발표하였으나 2023년 개정판_Rev.1을 발표하고 2024년 7월 1일 이후 건조 계약되는 선박으로 적용을 연기하였다[5][6].

IACS UR E26 - 선박 사이버 복원력은 그림 1과 같이 NIST(National Institute of Standards and Technology) 사이버 보안

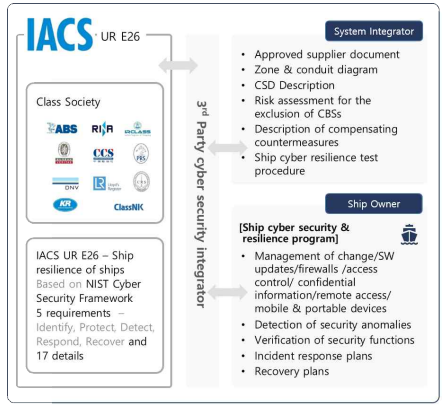

그림 1. 국제선급연합 공통 규칙 E26에 대한 산업계의 역할
Fig. 1. Industry's role in IACS UR E26

프레임워크(CSF, cyber security framework)의 식별, 보호, 탐지, 대응, 복구의 다섯 가지 핵심 기술을 기반으로 선박의 상비 복원력 확보를 위한 17가지 요구사항을 규정하고, 선박의 설계, 건조, 시운전 단계에서 조선소와 같은 시스템 통합자의 역할 뿐 아니라 사이버 보안 및 복원력 프로그램의 운영 주체로서의 선주의 역할을 선박 사이버보안 복원력 프로그램의 개발과 운항 종료 시까지 운영 관리의 주체적 역할을 규정하고 있다[7].

IACS UR E27 – 온보드 시스템 및 장비의 사이버 복원력은 CBS에 대한 위협 및 공격으로부터 보호할 수 있는 구체적인 방법을 제공하여, 최소 보안 요구사항을 충족하는 보안 기능을 CBS(computer-based systems)에 구현함으로써 선박에 대한 사이버 공격 위협 감소를 목표하고 있다[6].

IACS UR E27은 필수 보안 기능으로 그림 2와 같이 인증되지 않은 주체의 우발적 액서스로부터의 보호, 우발적 오용으로부터 보호, 우발적 조작으로부터 CBS의 무결성 보호, 정보의무단 공개 방지, CBS 운영 모니터링 및 인시던트 대응, 제어 시

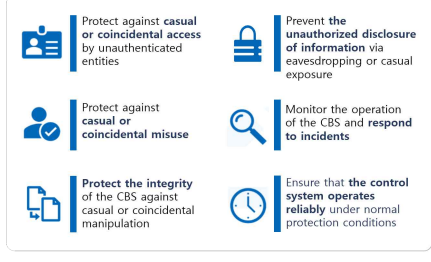

그림 2. 국제선급연합 공통 규칙 E27의 필수 보안 요구사항
Fig. 2. Required security capabilities of IACS UR E27

표 1. UR E27의 필수 요구사항
Table 1. Required security capabilities of UR E27

Item No.	Requirements
Protect against casual or coincidental access by unauthenticated entities	
1	Human user identification & authentication
2	Account management
3	Identifier management
4	Authenticator management
5	Wireless access management
6	Strength of password-based authentication
7	Authenticator feedback
Protect against casual or coincidental misuse	
8	Authorization enforcement
9	Wireless use control
10	Use control for portable & mobile devices
11	Mobile code
12	Session lock
13	Auditable events
14	Audit storage capacity
15	Response to audit processing failures
16	Timestamps
Protect the integrity of the CBS against casual or coincidental manipulation	
17	Communication integrity
18	Malicious code protection
19	Security functionality verification
20	Deterministic output
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure	
21	Information confidentiality
22	Use of cryptography
Monitor the operation of the CBS and respond to incidents	
23	Audit log accessibility
Ensure that the control system operates reliably under normal production conditions	
24	Denial of service protection
25	Resource management
26	System backup
27	System recovery & reconstitution
28	Alternative power source
29	Network & security configuration settings
30	Least functionality

스템의 안정적 동작 확인의 6가지 기본 요구사항을 정의하고 표 1과 같이 30가지 필수 보안 기능을 정의하였으며, 신뢰할 수 없는 네트워크와의 네트워크 통신이 포함될 경우를 위해 10개의 추가 보안 기능을 정의하였다[8].

그림 3과 같이 IACS UR E26은 선박을 UR E27은 선박에 탑재되는 장비를 대상으로 사이버 복원력을 정의한다. 선박에서의 UR E26/27 구현을 위해서는 UR E26의 식별, 보호, 대응, 복구, 특히 탐지 기능을 위한 네트워크 모니터링이 기술이 필수이며 UR E27 필수 보안 기능 요구사항에 따라 생성된 중요 이벤트 기록의 모니터링을 위한 기술이 필요하다.

UR E27에 따르면 선박에 탑재되는 CBS 기반의 장비 및 시스템은 엑세스 제어, 운영체제 이벤트, 백업 및 복원 이벤트, 구성 변경, 통신 두절 등과 같은 이벤트에 대한 보안 관련 감사 기록을 생성하여야 한다. 감사 기록은 보안과 관련된 중요한 이벤

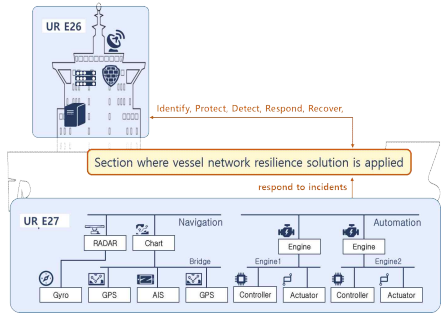

그림 3. 국제선급연학 공통 규칙 E26,27 대응을 위한 도구
Fig. 3. Tools for responding to IACS UR E26,27

트를 생성하는 것으로 필수 기록이 부족하면 감사가 제대로 이루어지지 않아 위협을 인지하기 어려울 뿐 아니라 위협 사고 발생 시 원인을 분석할 수 없기 때문에 CBS는 감사 기록을 생성하고 생성된 감사 기록은 솔루션을 통해 관리 되어야 한다.

Ⅲ. 선박 사이버보안 대응 기술 분석

UR E26의 주요 요구사항과 UR E27에서 생성된 주요 이벤트 기록을 관리하기 위한 그림 3의 관리 솔루션으로 일부 산업계에서는 네트워크 관리기술의 대표 솔루션인 네트워크 관리 시스템(NMS, network monitoring system) 도입을 검토하고 있으며 일본선급은 온보드 시스템 및 장비의 사이버 복원력에 대한 가이드라인(guidelines for cyber resilience of on-board systems and equipment)에서 SIEM을 언급하고 있다[8].

NMS는 다양한 이기종 네트워크 장치를 중앙에서 관리하고 감시할 수 있는 시스템으로 전체 네트워크를 중앙 시스템을 통해 모니터링, 진단, 분석, 가용성을 유지하기 위해 개발되었다.

NMS는 SNMP(simple network management protocol), ICMP

그림 4. 네트워크관리시스템의 대표 기능
Fig. 4. Common functions of network management system

표 2. 네트워크관리시스템 대표 기능의 세부사항
Table 2. Details of network management system representative functions

Item	Detailed features
Disability Management	- Identify/collect events such as failures, events, and warnings that occur in the network - Create alerts and notifications/notify administrators - Automatically solves or minimizes problems through predefined recovery scripts - Management of history and db statistics for errors that occurred - Rapid identification through topology map
Configuration Management	- Collection, management, and update of configuration information of network devices and services - Track and restore network changes - Visual representation through topology map - Relationship diagram between devices and services
Performance management	- Real-time monitoring/history management of network performance indicators - Bandwidth optimization, bottleneck prevention - Resource usage analysis/maintaining optimal performance

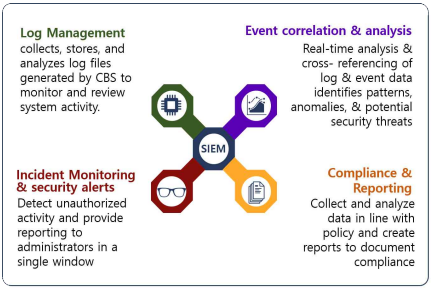

그림 5. 보안 정보와 이벤트 관리시스템의 대표 기능
Fig. 5. Common functions of network Security information and event management system

(internet control message protocol), RMON(remote network monitoring) 등 다양한 네트워크 프로토콜을 활용하여 네트워크 자산의 성능 데이터를 수집하고 모니터링하여 자산의 이상 상태나 장애가 발생할 경우 사용자에게 알림을 전달하기 위해 장애 관리, 성능 관리, 구성 관리 등 그림 4, 표 2의 주요 기능을 제공한다[9].

SIEM은 잠재적인 보안 위협과 취약성이 비즈니스 운영에 문제가 발생되기 전에 이를 인지하고 대응을 지원하는 보안 솔루션으로 그림 5와 같이 사용자, 엔드포인트, 애플리케이션, 데이터 소스, 클라우드 워크로드, 네트워크의 이벤트 로그 데이터와 방화벽 또는 안티바이러스 소프트웨어와 같은 보안 하드웨어 및 소프트웨어의 데이터를 실시간으로 수집하고 빅데이터 기반으로 분석하여 보안 위협 징후를 판단할 수 있는 통계정보를 생성

표 3. 보안 정보와 이벤트 관리시스템의 위협 탐지 범위
Table 3. Threat detection range of SIEM

Item	Detailed features
Insider threat	Security vulnerabilities or attacks originating from individuals with access to networks and digital assets
Phishing attack	Steal user data, login information, financial information, and business information through messages that appear to be from a trusted entity
Ransomware	Malware that locks the victim's data or device and threatens to unlock or damage it unless a payment is made
DDoS attack	An attack that floods networks and systems with unmanageable levels of traffic, degrading the performance of websites and servers until they become unusable.
Data Export	An act of data theft from a computer or other device, either manually or automatically using malware

하며 이를 기반으로 보안사고 분석·예방·대응을 지원한다[10].

SIEM은 특히 위협 인텔리전스와 AI(artifical intelligence) 기술을 사용하여 실시간 위협 뿐아니라 표 3과 같은 광범위한 사이버 공격과 알려진, 알려지지 않은 위협을 모두 탐지하여 빠르게 변화하는 사이버 보안 환경에 최적화되어 있으며, 모든 디지털 자산에 대한 로그 데이터를 한곳에서 수집·분석하여 보안 인시던트가 발생하면 이를 바탕으로 인시던트의 위험도, 위협 발생의 원인 등을 신속히 분석할 수 있다[10].

이처럼 NMS는 다양한 이기종 장비의 네트워크 이벤트를 수집하여 네트워크 장치를 중앙에서 관리·감시함으로써 자산의 이상 상태나 장애 발생을 예방하는 것이 목적이며, SIEM은 다양한 이기종 보안 하드웨어 및 소프트웨어 데이터를 수집하여 보안 위협의 징후를 파악하고 보안사고의 분석, 예방 및 사고 발생 시 대응을 위한 시스템이다.

NMS도 표 2와 같이 다양한 이기종의 네트워크 장비의 상태와 이벤트를 수집하며 토폴로지 맵을 이용한 장비의 직관적인 모니터링, 장비와 서비스 간의 상관관계 분석 등을 지원하기 때문에 IACS UR E27의 요구사항을 만족하는 CBS들의 관리와 UR E26에서 요구하는 기능을 일부 제공할 수 있으나 UR E26/27에서 근본적으로 요구하는 사이버 복원력 관점 즉, 보안 관점에서의 사고 예방·대응을 위한 기술로의 활용은 제한적이다.

따라서 본 논문에서는 보안 솔루션인 SIEM 고유의 기능을 바탕으로 선박 운영환경에 최적화하고 UR E27 장비의 관리 뿐아니라 운항 중 선박에서의 사이버 위협 판단과 선박검사 및 심사 대응 등 UR E26에서 요구하는 선박의 보안 및 복원력 프로그램의 도구로 활용이 가능한 선박용 SIEM에 대한 개념설계를 수행하였다.

Ⅳ. 선박 통합보안관리 시스템 개념설계

SIEM의 보안사고 탐지/분석/대응을 위한 고유 기능을 구현하기 위해서는 그림 5와 같이 로그 관리, 이벤트 상관성 분석,

인시던트 모니터링 및 보안경고, 규정 준수 관리 및 보고 기능이 구현되어야 한다[10].

또한 IMO MSC.428(98)은 NIST CSF의 식별, 보호, 탐지, 대응, 복구의 핵심 기술을 기반으로 ① 장애가 발생할 경우 선박 운항에 위협이 되는 시스템 및 기능을 식별하고, ② 선박 운항의 연속성을 보장하기 위한 위협 통제 프로세스와 비상계획을 수립하며, ③ 사이버 위협을 적시에 탐지하기 위한 절차 개발 및 이행과 함께 ④ 선박 운영 및 서비스 복원을 위한 활동과 계획 및 이행, ⑤ 사이버 사고 발생 시 선박 운영에 필요한 사이버 시스템을 백업 또는 복구하는 방법의 식별을 요구하고 있다.

IACS UR E26은 NIST CSF의 식별, 보호, 탐지, 대응, 복구의 핵심 기술을 기반으로 ① 선내 네트워크에 설치된 CBS와 네트워크 장비를 식별·목록화하며 ② 보안 구역 및 안전장치, 안티바이러스 도입, 접근통제와 무선통신 등의 보호 조치를 하며, ③ CBS 및 네트워크 상태를 모니터링하여 위협·사고 발생 시 ④ 사전에 수립된 사고 대응 계획에 따라 네트워크 격리, 수동 운전 또는 최소 위험조건으로의 fall-back, ⑤ 사이버 사고 발생 시 사전에 수립된 복구 계획에 따라 선박 운영에 필요한 사이버 시스템을 백업 또는 복구를 요구하고 있다.

SIEM 고유 기능을 바탕으로 국제 협약의 사이버 보안 프레임워크를 만족하며, IACS UR E 27 대상 장비의 감사 기록의 관리를 위한 표 1의 필수 요구사항 30 항목과 소프트웨어 프로세스 및 장비 식별 및 인증, 실패한 로그인 시도, 원격 세션 종료, 세션 무결성의 추가 요구사항을 만족할 수 있도록 그림 6과 같이 선박용 SIEM의 주요 기능을 식별하고 표 4와 같이 기능 명세를 도출하였다.

SIEM의 플랫폼은 그림 7과 같이 로그 정보 수집/변환, 보안정보 저장/적재, 보안이벤트 상관분석, 사용자 인터페이스로 구성된다.

표 4. 선박용 SIEM 주요 기능
Table 4. Main function of SIEM for ship

Item	Detailed features
Agent Management	
Agent Management	- Configuration and management - Check system communication status - Collect agent asset logs
Log collection	- Real-time collection by log source / Notification of non-collection - Check status / volume (throughput)
API connection	- Supports regular expressions, delimiters, Key/value, XML, JSON - Normalization for multiline logs - New data format integration
Log search and analysis	
Search	- Set various search conditions - TopN statistical analysis by field - Extract data from original log and all fields
analyze	- In-memory real-time log analysis and detection - Exception handling to minimize false positives
Control and monitoring	
Monitoring	- Real-time detection and monitoring by alarms
analysis	- Real-time statistics generation
Infringement incident handling process	
Response to infringement incidents	- Handling of serious incidents - Setting and processing custom infringement response steps in work- flow form
Management and Settings	
Settings	- Set up detection by combining predefined objects
user account	- Provides linked API such as creation/deletion/inquiry
User access management	- User access control (using audit logs) - Restrict user access when login fails - Secondary authentication for user access
Audit log	- Provides history management/search function for user access history and changes - Audit log data management and download
Backup & Recovery	- Backup/recovery of setting information, audit log, and alarm files

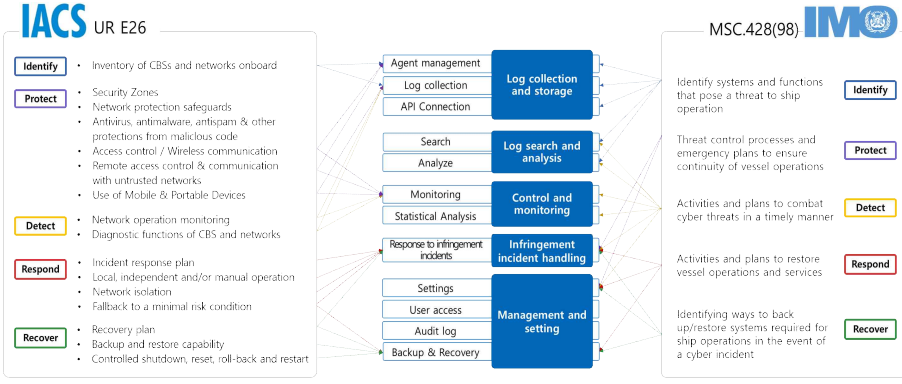

그림 6. 국제협약기반 선박용 SIEM의 주요 기능 식별
Fig. 6. Identification of key functions of international agreement-based SIEM for ship

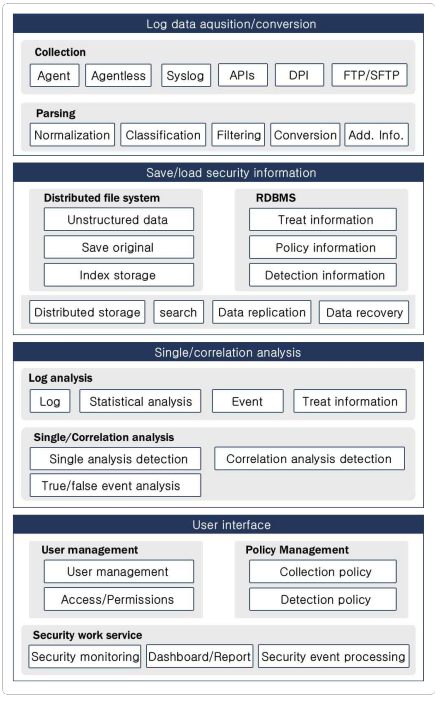

그림 7. SIEM 플랫폼 구성
Fig. 7. SIEM platform configuration

로그 정보 수집/변환 프로세스는 다양한 네트워크·장비의 로그 정보를 수집하고 데이터를 분석하여 보안 정보의 저장 프로세스 및 보안이벤트 상관분석 프로세스에서 활용할 수 있도록 중앙으로 전송하는 역할을 한다.

로그수집은 네트워크 시스템·장비에 설치하여 자동으로 로그데이터를 수집하는 로그 수집기(agent)를 활용하거나, SNMP와 같은 표준 프로토콜을 이용하는 방식, 이벤트 스트리밍, 각 기기의 DB(data base)에 직접 연결/연동하는 여러 가지 방식이 있으며 수집 대상 장비의 인터페이스 방식에 따라 수집방법을 선택한다. 하지만 SNMP와 같은 표준 프로토콜을 사용하거나 이벤트 스트리밍의 경우 또는 SYSLOG를 연동하는 경우에도 로그 정규화 작업을 하지 않는 경우는 분석, 검색, 위협 경보 생성 기능에 제한이 있어 단순 기록과 경보 발생의 기능만을 제공할 수 있다. 따라서 본 연구에서는 선박에 설치된 네트워크 장비를 분석하여 표 5와 같이 선박에 설치된 IT(information technology) · OT(operation technology) 네트워크 자산을 식별하고 식별된 선내 정보 자산의 유형별 보안 정보 수집 방식을 정의하여 수집된 정보를 정규화한다.

표 5. 선박 보안 정보 수집 방식
Table 5. Security information collection method

Method	IT information asset	Ship asset
Agent	CPU, memory, disk logs Event/security log for Linux, Unix, and Windows	· ship communication system · Security log of ship server - Internal server - Office PC - External linked server - Ship security system
Syslog	Network equipment and appliances Router, switch, backbone, NMS/SMS, firewall, VPN, IDS/IPS	· ship security system - IDS/IPS - VPN - Firewall/UTM · ship network system - L3 Router - L2 Switch · Application systems
SNMP	Network traffic	· ship network system - L3 Router - L2 Switch
ODBC/ JDBC	Information system Portal, ERP, legacy	· IT systems onboard ship

보안 정보 저장 프로세스는 수집·정규화된 데이터의 처리·분석을 위하여 파싱 데이터와 원본 로그, 실시간 압축, 암호화 저장 및 실시간 인덱싱으로 고속검색을 지원한다.

보안이벤트 상관분석 프로세스는 수집된 로그를 읽을 수 있는 형태로 제공하는 로그 시각화, 로그 분석결과를 보여주는 로그 보고와 로그 항목 간 상관관계를 분석하는 이벤트 상관분석으로 구성된다. 로그 정보와 위협정보에 대한 분석은 위협 이벤트를 단계별 위협 시나리오에 따른 위험도를 설정하여 이벤트 발생 시 설정한 가중치로 위험도를 산출되며, 수집 로그 속성에 따른 자산 기반의 이벤트 분석기능 제공과 이벤트 분석결과를 기반으로 자산별 또는 그룹별 위험도를 산출한다.

보안이벤트 상관분석 프로세스에서 선박의 사이버보안위협을 식별하고 실시간 사이버 공격 탐지 및 대응체계에 반영할 수 있도록 선박의 네트워크 환경과 통신 방법을 분석하여 선박 통신 인프라 보안 위협을 기밀성 위협, 무결성 위협, 가용성 위협, 인증 위협, 부인방지 위협, 프라이버시 유출, 투명성 및 내용 일관성 위협으로 표 6과 같이 정의하였다.

SIEM은 그림 7과 같이 사전에 정립된 위협정보와 함께 탐지 정책을 기반으로 사이버 위협을 탐지한다. 본 연구에서는 선박의 운영환경에 최적화된 선박용 SIEM 탐지 정책을 개발하기 위하여 그림 8과 같이 한국선급의 사이버 보안 규칙, BIMCO의 사이버보안 가이드라인, IMO의 안전관리시스템에서의 사이버 위협관리, IACS의 UR 26, 27과 MSC.428(98) 대응을 위한 사이버 복원력을 위한 권고서, UR E27에서 채용된 IEC 62443 3-3, 62443 4-2를 기준으로 대분류 49개 항목, 335개의 세부 항목의 기술 요구사항을 분석하여 표 7과 같이 선박용 SIEM에 적용 가능한 탐지 정책 27건을 개발하여 시스템에 적용하였다.

SIEM의 해상 환경에서의 운용을 위해서는 그림 7의 SIEM의 플랫폼과 그림 6, 표 4와 같이 국제기구의 규제 만족을 위한 기능 도출, 표 6, 7과 같이 해사 사이버 위협탐지를 위한 선박 사이버 위협과 탐지 정책의 정의, 표 5와 같이 선박에 설치된

표 6. 선박의 보안 위협 정의
Table 6. Definition of ship security threats

Threat		Definition of threat
Availability and DoS threats	DoS attacks on ship communications	System overload and data loss through sending invalid satellite communication messages /transmitting large service request data packets
Integrity and authentication threats	Manipulation of application behavior	Causes malfunctions and generates and transmits false data through normal application tampering and abnormal updates
	Data forgery /falsification	Transmitting false data by forging /altering transmitted/received data
	Access to components	Creation of false data such as forgery/falsification or deletion of satellite communication messages received through access to components
Confidentiality Threat	data breach	Leakage of confidential data through wiretapping and traffic analysis of communication sessions
Non-repudiation threat	Disclaimer regarding send /receive messages	Denial of sending/receiving satellite communication messages through spoofing attacks that manipulate location signal information
Privacy information leak	Leakage of personal and sensitive information	Malicious use of personally identifiable information such as personal signature, resident registration number, personal information, etc.
Transparency and content consistency	communication monitoring	Steal specific data through continuous monitoring of communications and use it for a different purpose than the original purpose.

표 7. 선박용 SIEM 탐지 정책 예시
Table. 7. Definition of ship security threats

Code	MR-SOC-1	Detection Device	network
Policy	[System Alert] Newly connected device detected in router/switch		
Guidelines	1) IACS Rec 166 2) BIMCO		
Item	1) Technical requirements > Network > Control, monitoring and alarming 2) Development of protective measures > Technical protective measures > Network port restrictions and controls		
Technical Requirements	1) Connect each port of network equipment 2) It is recommended to close unused ports on the router.		
Requirements Analysis	1) Detect new connections to network device ports 2) Detect unauthorized connections to unused ports		
Applicable to	L2/L3 switch	Direction	Inside->Inside
Risk level	M	Linkage method	SYSLOG
Cycle of occurrence	1 min	Occurrence conditions/ number of cases	1
Condition definition	Field : message Operator : like Value - ["%LINK -I -Up%"]		
Exclusion conditions	-		
Note	Link-up message linking of CISCO equipment considering vessel characteristics		

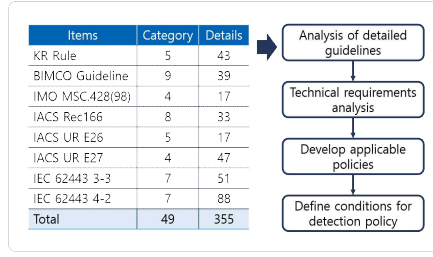

그림 8. 국제 협약 요구사항 분석을 통한 탐지 정책 개발
Fig. 8. Development of detection policy through analysis of international agreement requirements

수많은 이기종 장비에 대한 연동뿐만 아니라 운영자 및 운영환경에 대한 추가 기능이 필요하다.

일반적으로 SIEM은 보안이 필요한 장비나 시스템에 Agent를 설치하고 수집된 데이터를 중앙에서 보안전문가가 직접 관리하며 다양한 분석을 통해 사이버 위협에 대응하고 있다. 하지만 선박은 운항 특성상 선박 운항에 전문기술을 가진 소수의 인력이 근무하고 있어 네트워크 기반의 IT·OT 장비 및 시스템의 보안 관리와 사이버 위협 대응이 불가하며, 표 1과 그림 3과 같이 선박에 설치된 UR E27 대상 장비들의 통합관리에는 많은 어려움이 있다.

따라서 본 연구에서는 선박용 SIEM의 운영자와 운영환경을 지원하기 위한 사용자 지원 기능을 표 8과 같이 정의하였다.

선박용 SIEM은 선박에 근무하는 IT 비전문가도 선박에 설치된 네트워크 기반 선박 자산 상태에 대한 이상 여부와 사이버 위협 발생을 쉽게 인지할 수 있도록 사용자 인터페이스가 제공되어야 한다. 본 논문에서는 선박용 SIEM을 선박 네트워크 자산에 대한 상태 확인 기능과 더불어 사용자 재구성이 가능한 네트워크 토폴로지 맵을 기반으로 네트워크 존과 선내 운영 중인

그림 9. 토폴로지 맵 기반 네트워크 자산관리
Fig. 9. Topology map-based network asset management

표 8. 선박용 SIEM의 선박 환경 최적화 기능
Table 8. Security data log collection method of SIEM for ship

Requirements of UR E26	Ship network management system	SIEM for ship
Asset monitoring	Monitoring the status of IT and OT equipment connected to the ship network	
Asset details management	Simply displaying asset information	Collection of information liked to other systems Link to various information such as events
Traffic information	Monitoring data communication on board ship	
Network topology	Use in the form provided by the manufacturer	Customizable (scalability)
Log integration	Audit log management for UR E27 equipment connected to the ship network	
	Stores the original log data of connected network devices	After collecting various log data such as SYSLOG, DB Agnet and API, standardize the collected data so that it can be utilized
Alarm notification	Triggered every time an event occurs	Events that occur through AI-based detection policies are cumulatively processed and alarms are generated under various conditions
Risk level	Alarm information display	Calculate and visualize risk for each event though AI-based detection policy

네트워크 자산의 상태를 가시화하여 선원이 등록된 자산을 쉽게 관리할 수 있고 사이버 위협 발생 시 발생 위치와 상태를 신속하게 파악할 수 있도록 그림 9와 같이 사용자 인터페이스를 구성하였다.

선교에 설치된 수많은 IT·OT 장비 및 시스템의 개별 알람과 선박경보알람장치 등 잦은 시청각 알람으로 선교 당직자의 업무 피로도 증가와 경보에 대한 경각심 저하 등의 문제가 발생하고 있다. 이처럼 부적절하게 설계된 경보 또는 경보 과잉은 사용자의 직무 이행에 부정적인 효과를 줄 수 있다.

이에 본 연구에서는 표 5와 같이 선박의 다양한 이기종 장비 데이터를 정규화하여 특정 조건에 따라 경보를 누적·발생할 수 있으며 그림 8, 표 7과 같이 해사 분야 가이드라인의 요구사항에 따라 정의된 탐지 정책과 선박 내 설치된 네트워크 자산에서 수집되는 보안 정보를 통해 정립된 AI 탐지 모델을 기반으로 위협도를 판단하여 하이라이트 기능과 긴급알림, 보안 위협, 시스템 및 네트워크 상태 정보 등을 종합적으로 제공하도록 정의하였다.

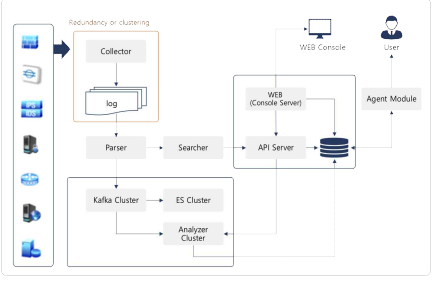

그림 10. 선박용 SIEM 시스템 구성
Fig. 10. Configuration of SIEM for ship

선박용 SIEM은 앞서 정의한 로그 소스 연결 관리, 보안이벤트 처리, 연관분석, 관리자로부터 받은 명령 처리, 요청된 관제 데이터 처리 들을 하나의 장비에서 수행하도록 그림 10과 같이 구성하였다. 시스템은 Server와 Agent로 구성되며 각 역할은 표 9와 같다.

표 9. 선박용 SIEM 구성별 역할
Table 9. Role of SIEM for ship's component

Item	Definition of threat
Server	· Verifies the integrity of important data and files when running · Performs integrated security management functions · Communication between the administrator PC's web browser and the server uses TLS V1.2. · Provides means for managing security function data and security functions, such as administrator registration management, log source group management, collection rules, and threat analysis rule management. · Provides administrators with the ability to view stored audit data through GUI · Encryption of data transmitted between agent and server · Management functions based on administrator privileges · Detect actual threats through the threat analysis function and send warning messages to general managers and administrators as a means of response. · Provides real-time search for collected security events and search for audit data through a web interface
Agent	· Verification of important data and Silpang file integrity during operation · Identification information is transmitted to the server to identify the management target system. · Encrypted communication between agent and server · Collects information and events related to magent settings received from the server · Send events that occur in the management target system to the server

Ⅳ. 결 론

본 연구에서는 IACS UR E26, 27의 세부 요구사항을 분석하여 UR E27의 필수 보안 기능 요구사항에 따라 생성된 중요 이벤트 기록의 통합관리와 UR E26의 식별, 보호, 탐지, 대응, 복구의 기능을 보안 관점에서 관리하기 위한 솔루션이 필요함을 확인하였다. 선박용 보안 솔루션으로 검토되고 있는 NMS와 SIEM의 기술을 분석하여 선박의 보안 및 복원력 프로그램의 도구로 활용이 가능한 SIEM을 제안하고 선박용 SIEM에 대한 개념설계를 수행하였다.

IMO MSC.428(98)과 IACS UR E26, 27을 기반으로 선박용 SIEM의 주요 기능을 도출하고 선박의 이기종 장비에 대한 연동 및 정규화 방안과 선박 사이버 보안 위협의 식별을 위한 선박의 사이버 위협을 정의하고 국제협약 기반 선박용 탐지 정책을 개발하였다.

또한 선박의 운영 환경과 운영 인력을 고려하여 네트워크 토폴로지 맵을 기반으로 사이버 위협 발생 위치와 상태를 신속하게 파악할 수 있는 사용자 인터페이스와 선교 환경을 고려하여 AI 탐지 모델 기반 위협도 판단 및 지능형 경보 발생 정책 등 선박에 특화된 기능을 정의하였다.

Acknowledgments

본 연구는 2023년도 산업통상자원부 조선해양산업핵심기술개발사업(20026436)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

References

[1] S. H. Park, Tasks to strengthen ship cybersecurity. [Internet]. Available: https://blog.naver.com/pttopnews/223366936958.

[2] Security News, Growing threat of ship hacking, more than 1,600 devices discovered on attack surface [Internet]. Available: https://m.boannews.com/html/detail.html?idx=126635.

[3] J. G. Im and G. J. Son, *Maritime cyber security trends and plans to build a ship cyber safety system*, Korean Register's Technology Policy Proposal Research Collection, 2020.

[4] M. J. Kang, "Ransomware struck musk, cybersecurity concerns spread," *Maritime Korea*, Vol. 2017, No. 8, pp. 36-42, 2017. Retrieved from https://kiss.kstudy.com/Detail/Ar?key=3535612

[5] International Association of Classification Societies, Unified-requirements E26 : Cyber resilience of ships – Rev.1, Nov, 2023. [Internet]. Available : https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

[6] International Association of Classification Societies, Unified-requirements E27 : Cyber resilience of on-board systems and equipment-Rev.1, Sep, 2023. [Internet]. Available :https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf.

[7] N. S. Kang, G. J. Son, R. C. Park, C. S. Lee and S. S. Yu, "IACS UR E26 – analysis of the cyber resilience of ships," *Journal of Advanced Navigation Technology,* Vol. 28, No. 1, pp. 27-36, Feb 2024. DOI : http://dx.doi.org/10.12673/jant.2024.28.1.27.

[8] ClassNK : Guidelines for cyber resilience of on-board systems and equipment, 2023.

[9] Brainz company, Components and main functions of NMS, [Internet]. Available : https://www.brainz.co.kr/tech-story/viewid/246#u

[10] IBM, SIEM concept, [Internet]. Available : https://www.ibm.com/kr-ko/topics/siem

강 남 선 (Nam-Seon Kang)

2005년 2월 : 목포해양대학교 기관시스템공학과 (공학석사),
2007년 12월 ~ 2008년 12월 : 대한조선 조선기본성능연구소,
2016년 9월 ~ 2022년10월 : 마린웍스 책임연구원,
2005년 6월 ~ 2007년 11월 : 한국해양과학기술원 연구원
2005년 3월 ~ 2016년 8월 : 중소조선연구원 선임연구원
2023년 6월 ~ 현재 : 이글루코퍼레이션 수석연구원
※관심분야 : 해사위성통신, 선박자동화, e-Navigation, 해사 사이버보안

이 창 식 (Chang-Sik Lee)

2008년 2월 ~ 현재 : 이글루코퍼레이션 부장
※관심분야 : 정보보안, 보안컨설팅, OT보안, 해사 사이버보안

유 성 상 (Seong-Sang Yu)
2017년 2월 : 인하대학교 조선해양공학과 (공학석사)
2017년 2월 ~ 2021년 1월 : 한국선급 사이버인증팀
2021년 10월 ~ 현재 : 중소조선연구원 특수선박지원센터
※관심분야 : 선박항해통신, e-Navigation, 해사 사이버보안, 스마트·자율운항선박

이 종 민 (Jong-Min Lee)
2007년 2월 : 광운대학교 컴퓨터공학과 (공학사)
2007년 1월 ~ 2016.12월 : 현대무벡스 현대상선 IT 지원팀
2017년 1월 ~ 2021년 7월 : HMM 정보전략팀 및 남중국본부 IT총괄
2022년 5월 ~ 현재 : 현대엘엔지해운 IT팀 팀장
※관심분야 : IT기획, 해운 IT시스템 설계/구축, 선박자동화, 해사 사이버보안

손 금 준 (Gum-Jun SON)
2006년 2월 : 목포해양대학교 기관시스템공학과 (공학사)
2006년 3월 ~ 2013년 2월 : STX 팬오션 1등기관사
2011년 3월 ~ 2013년 2월 : 인하대학교 조선해양공학과(공학석사)
2013년 2월 ~ 2013년 9월 : 한국해양과학기술원 연구원
2013년 9월 ~ 현재 : 한국선급 책임연구원
※관심분야 : 해사위성통신, 선박자동화, e-Navigation, 선박 사이버보안