대한조선학회논문집 Research Paper
Journal of the Society of Naval Architects of Korea
eISSN:2287-7355, Vol. 61, No. 4, pp. 278-288, August 2024
https://doi.org/10.3744/SNAK.2024.61.4.278

선박용 Security Information Event Management (SIEM) 개발을 위한 보안 정책 모델에 관한 연구

손금준[1,†] · 안종우[1] · 이창식[2] · 강남선[2] · 김성록[3]
(사)한국선급[1]
이글루코퍼레이션[2]
현대LNG해운[3]

Research on Security Detection Policy Model in the SIEM for Ship

Gumjun Son[1,†] · Jongwoo Ahn[1] · Changsik Lee[2] · Namseon Kang[2] · Sungrok Kim[3]
Korean Register[1]
IGLOO Coporation[2]
Hyundai LNG Shipping[3]

According to International Association of Classification Societies (IACS) Unified Requirement (UR) E26, ships contracted for construction after July 1, 2024 should be designed, constructed, commissioned and operated taking into account of cyber security. In particular, ship network monitoring tools should be installed in accordance with requirement 4.3.1 in IACS UR E26. In this paper, we propose a Security Information and Event Management (SIEM) security policy model for ships as an effective threat detection method by analyzing the cyber security regulations and ship network status in the maritime domain. For this purpose, we derived the items managed in the SIEM from the maritime cyber security regulations such as those of International Maritime Organization (IMO) and IACS, and defined 14 detection policies considering the status of the ship network. We also presents the detection policy for non-expert crews to understand it, and occurrence conditions depending on the ship's network environment to minimize indiscriminate alarms. We expect that the results of this study will help improve the efficiency of ship SIEM to be installed in the future.

Keywords : SIEM(Security Information Event Management, 보안 정보 및 이벤트 관리), Security(보안), Policy(정책), Traffic(트래픽), Event log(이벤트 로그)

1. 서 론

1.1 연구 배경 및 목적

초고속 인터넷, 모바일 4, 5세대 등 통신 기술의 발전과 인터넷 연결이 가능한 통신 단말(컴퓨터, 스마트폰, 태블릿PC, 자율주행 자동차 등)의 유형 증가에 따라 대량의 사이버 위협이 시도되고 있으며, 사이버 공격 기술 또한 나날이 진화, 고도화되고 있다 (Ko and Jo 2021).

해사분야 또한 스마트 선박의 출현과 디지털 기술의 확대로 인한 해상에서의 사이버 사고가 증가됨에 따라 국제해사기구(IMO, International Maritime Organization)는 국제 선박 및 항구등을 국제 안전 관리(ISM, International Safety Management) 코드와 같은 다양한 규범과 조치를 통해 해양 보안 및 안전을 주요 목표중 하나로 삼았다 (Park, 2020). 이에 국제해사기구(IMO)는 MSC (Maritime Safety Committee).428(98)을 발행/채택하여 (KMI, 2023) 안전관리체계(ISM, International Safety Management Code) 내 사이버안전을 포함하도록 권고하고 (IMO, 2017), 2021년 1월 이후 도래하는 첫 번째 Document of Compliance(DOC) 심사 시 확인하도록 주관청에 권고하고 있다 (Lee et al., 2020).

뿐만 아니라, Baltic and International Maritime Council (BIMCO, 2016)은 2016년 선박 사이버보안 가이드라인을 발간하고, The Oil Companies International Marine Forum (OCIMF, 2017)은 2017년 Tanker Management and Self Assessment

Received : 5 June 2024 | Revised : 19 June 2024 | Accepted : 9 July 2024
† Corresponding author : Gumjun Son, gjson@krs.co.kr

(TMSA) 3에 사이버보안 위험 식별에 관한 절차 및 요건을 포함하였으며, (2018) 2018년 Ship Inspection Report (SIRE) Vessel Inspection Questionnaire(VIQ) 7에 사이버보안 요건을 추가하는 등 민간기구 주도로 선박 사이버보안에 대한 활발한 활동이 이루어지고 있다 (Gang, 2018).

이러한 시대적 흐름에 발맞추어 '국제선급연합회(IACS, International Association of Classification Societies)는 2022년 4월 선박 건조 및 선박 기자재 개발에 관한 요구사항으로 UR(Unified Requirement) E26 (2022), UR E27 (2022)을 발행하고, 2024년 7월 1일 건조 계약되는 선박에 적용할 예정이다.

UR E26은 4.1 식별(선내 사이버 자산관리), 4.2 보호(무선통신을 포함한 선내 네트워크 토폴로지 구성), 4.3 탐지(선내 네트워크 모니터링), 4.4 대응(사이버 사고 대응 절차) 및 4.5 복구(백업 등 복구 절차) 등의 요구사항을 포함하고 있으며, 특히, 4.3 탐지 요구사항 대응을 위해 현대중공업그룹은 Paessler AG 그룹의 Network Monitoring System(NMS)을 기반으로 개발된 Hi-Secure를 발표하였으며(THE KOREA ECONOMIC DAILY, 2024.), 일본 NYK선사는 사이버보안 핵심 활동으로서 관리 선박 내 Security Information Event Management(SIEM) 솔루션 도입을 추진 중임을 소개하였다 (Shibata, 2023).

선박용 NMS, SIEM 등 사이버보안 모니터링 도구는 선박 사이버보안을 위한 핵심 기술로서, 단순히 선박의 보안 위협 모니터링 외 사이버 사고 분석, 선박 검사/심사 등 사이버보안 관련 활동을 위한 필수 시스템으로 활용될 수 있다. 다만, NMS는 Simple network management protocol(SNMP)을 활용하여 네트워크 장치로부터 장비의 상태 정보를 수집·모니터링하는 솔루션으로 네트워크 장치에서 일상적으로 발생되는 다양한 이벤트 정보가 무분별하게 알람으로 표출될 수 있으며, 사이버 위협 발생 시 선원이 해당 네트워크 장치에 접근하여 로그 원본 파일을 분석하여, 사이버 위협에 대한 대응 방안을 직접 제시할 수 있어야 한다.

Table 1 SIEM and NMS difference

Function	SIEM	NMS
Asset health monitoring	O	O
Asset data management	O	X
Traffic information	O	O
Log linkage	O (Data normalization after collecting various syslogs (Log, API, DB, Agent))	△ (Manage original logs after collecting designated logs)
Alarm notification	O (Create alarms with various criterias)	△ (Unable to manage (alarm when occurs))
Risk	O (Application by event, visualization display)	X (No risk management Functions)

IACS UR E26 4.3 탐지 요구사항에 대한 대응 기술로서 NMS는 Table 1과 같이 부족하지 않으나 선박-육상 간 통신 환경, 네트워크에 미친숙화된 선원의 역량 등 선박이라는 특수한 환경속에서 NMS가 얼마나 효율적인지는 숙고해 보아야 한다.

본 논문에서는 NMS가 SIEM 대비 비용적으로 큰 강점을 가지고 있음에도 불구하고, 사이버 위협 대응을 위한 선원의 의사결정 지원, 무분별한 알람 자제를 통한 항해 업무 효율 향상, 원활하지 못한 원격 지원 환경 등을 감안하여 직관적으로 비전문가인 선원이 사이버 위협에 용이하게 대응하는 기술로서 SIEM이 보다 효율적이라고 판단하였다. 이에 선박에 최적화된 SIEM 개발을 위하여 본 논문에서는 선박에서 발생 가능한 이벤트(로그)별 위협 여부 및 위협의 종류 등을 판단하기 위한 보안 정책 모델을 제안한다. 2장에서는 IMO 등 해사분야의 사이버보안 요구사항을 분석하였고, 3장에서는 선박 내 설치된 보안 장치, 네트워크 장치 등을 포함한 선박의 네트워크 토폴로지 및 트래픽/이벤트 현황을 분석하였다. 4장에서는 2장, 3장의 분석 결과를 토대로 효율적인 SIEM 운영을 위한 탐지 정책을 제시하고 이에 대한 실선 적용 결과를 기술하고 5장에서는 결론을 제시하였다.

2. 선박 사이버 복원력 규정 분석

2.1 IMO Resolution MSC.428(98)

IMO MSC.428(98)은 제조업체, 서비스 제공업체, 항만 및 항만시설, 기타 모든 해양 산업 이해관계자를 대상으로 현재 또는 미래의 사이버 위협과 취약점으로부터 선박을 보호하기 위한 지침으로 동 지침의 세부 요건은 IMO MSC-FAL(Facilitation Committee). 1/Circ.3 (2022) 참조를 권고하고 있다. IMO MSC- FAL.1 /Circ.3는 BIMCO 등 선주 주도로 개발된 회람문서로서 취약한 비밀번호 사용과 같은 직접적, 네트워크 미분리와 같은 간접적으로 발생되는 선내 사이버 시스템의 취약점에 대한 효율적인 사이버 리스크 관리 방안에 대하여 소개하고 있다. 동 지침은 네트워크 장치 등 기술적 고려사항 보다는 리스크 관리 기반 접근법을 활용하여 사이버 위험 관리 계획 수립 등을 통해 효과적으로 사이버 위협에 대응하는 것을 제안하고 있다. 동 회람문서(MSC-FAL.1/Circ.3)에서 제공하는 사이버 리스크 관리체계는 ①장애가 발생할 경우 선박 운항에 위협이 되는 시스템 및 기능을 식별하고, ②선박 운항의 연속성을 보장하기 위한 위험 통제 프로세스 및 조치 그리고 비상계획을 수립하도록 권고하고 있다. 또한, ③사이버 위협을 적시에 탐지하기 위한 절차 개발 및 이행과 함께 ④선박 운영 및 서비스 복원을 위한 활동과 계획 개발/이행을 요구하고 있다. 그리고 ⑤사이버 사고 발생 시 선박 운영에 필요한 사이버 시스템을 백업·복구하는 방법을 식별하는 것 등 총 5가지 관리적 측면의 프레임워크로 구성되어있다.

2.2 BIMCO Guidelines on Cyber Security Onboard Ships

BIMCO는 관리적/기술적 관점에서 선박의 사이버 안전 확보를 목적으로 '16년 2월 발행된 Ver.1.1을 시작으로 Ver.4 까지 선박

Table 2 7.2. Technical protection measures requirements

Requirements	Details
Limitation to and control of network ports, protocols and service	· Allow only appropriate ports/protocols/services according to corporate network or sub-net control policy
Configuration of network devices such as firewalls, routers and switches	· Block access of unidentified devices to controlled/uncontrolled networks · Control of remote access for OT(Operational Technology) & IT(Informational Technology) systems · Considering any wireless network as uncontrolled network · Configuring ship's network zone using firewalls, etc. and continuous monitoring of firewall logs
Satellite and radio communication	· Physical access control to LAN ports such as satellite modems or switches · Using Virtual Private Network(VPN) and encrypted protocols for ship-shore communications · Disable “remote administration page” and “port forward” functions · Communicate and monitoring of ship to shore communication through firewall · Encrypt data traffic during remote access
Wireless access control	· Wireless network access control through appropriate devices and change encryption keys regularly · Control of wireless network access through appropriate devices and change of encryption keys regularly · Monitoring of wireless access using NAC, etc. · Installation of security devices in wireless network-related devices

사이버보안 가이드라인을 발행하고 있다. 동 가이드라인은 NIST (National Institute of Standards and Technology) Framework (NIST, 2018)를 준용하여, 위협 및 취약점 식별, 리스크 평가, 보호 및 탐지 대책, 사고 대응 및 복구 등으로 구성되어 있으며 (Cha et al., 2017), 지침 내 선박 운영단계의 기술적 사이버보안 요구사항으로 7항 보호 대책 개발의 7.2 기술적 보호 대책, 7.3 절차적 보호 대책, 8항 탐지 대책 개발의 8.1 탐지, 차단 그리고 알람, 8.2 멀웨어 탐지 등을 포함하고 있다. 동 지침서(The Guidelines on Cyber Security Onboard Ships V4) 내 네트워크 설계 및 구성과 관련된 사이버 위협에 대한 대응 기술 요건은 Table 2와 같이 제시되어 있다.

또한, 동 지침서에서는 상기 언급된 기술적 사이버 보호 대책 요건의 적용 방안으로서, Table 3과 같은 절차적 요구사항이 포함되어 있다.

뿐만 아니라, 동 지침서는 선내 네트워크에 대한 보안 위협 및 멀웨어 감염 등을 탐지하기 위한 기술을 사이버 위험 관리의 핵심이라 언급하며, 사이버 사고 경보를 위한 임계값 설정의 필요성을 강조하고 있다.

Table 3 7.3 Procedural protection measures requirements

Requirements	Details
Computer access for visitors	· Establishing procedures to restrict access to onboard computers by port and terminal staff, etc.
Crew's personal devices	· Establishing procedures related to the use of IT devices by crew, including utilization of the ship's communication network, etc.
Upgrades and software maintenance	· Establishing procedures for updating firmware of OT & IT systems for ship operation/control and ship's network devices(router, firewall)
Remote access	· Establishing procedures for remote access to ship's IT & OT systems and monitoring remote access
Use of administrator privileges	· Restricting access to information except to authorized personnel
Multi/factor authentication and passwords	· Applying multi-authentication system and strong password policy for access to important systems/data

2.3 IACS Recommendation on Cyber Resilience

IACS Rec.166 – 사이버 복원력을 위한 권고서 (2020)는 IMO MSC.428(98) 및 FAL.1/Circ.3 대응을 목적으로 ‘20년 4월 발행되어 7월 개정된 문서로서, 기술적 요건에 중점을 둔 사이버 복원력 권고서이다. IACS Rec.166은 IMO 결의서와 마찬가지로 NIST 프레임워크를 준용하여 식별, 보호, 탐지, 대응, 복구 등 5가지 핵심 목표를 중심으로 기능 요구사항을 제시하고 있다. 이 중 네트워크 구성과 관련된 기술 요구사항은 Table 4와 같다.

2.4 IACS Cyber Resilience of Ship(UR E26)

IACS는 선박 사이버 복원력을 위한 기술 문서인 IACS Rec.166 발행 후 전 수명주기 관점에서 선박 사이버 복원력 강화를 위해 선박 건조/운영을 위한 최소 요구사항인 UR을 발행하였다. IACS Rec.166은 선급의 문제가 아닌, 산업계에 권고로 제공되는 기술 문서로서 선박 건조 및 운항에 직접적 영향을 끼치지는 않지만, IACS UR은 IACS 내 모든 선급의 실행 지침/규칙에 직접적으로 연관된 사항을 결의한 문서로서, IACS를 구성하는 모든 선급은 IACS 이사회(Council)에서 승인된 UR을 승인 시점으로부터 1년 내 각 선급의 규칙 및 실행 지침 등에 반영하여야 하고 그 시행 일자를 IACS 이사회 회원에게 통보하여야 하는 선박 건조/운영에 관한 강력한 제약사항이다.

IACS UR E26은 선박 건조 및 운영과 관련된 사이버 복원력에 대한 필수 요건으로 선내 탑재되는 자산의 관리 그리고 자산간 연계를 위한 네트워크 설계 그리고 이를 운영 관리하기 위한 기술에 관한 요구사항을 포함하고 있으며, UR E27은 UR E26 내 포함되는 대상 장치의 보안 기능 요구사항을 포함하고 있다.

Table 4 Network-related technical requirements

Requirements	Details
Equipment	· installation of network monitoring and alarm systems · Approving UR E22 and E10 for network device connected with cat 2 and 3 in UR E22
Design	· Designing network considering network data throughput, data processing speed, etc. · Network redundancy when necessary according to risk assessment · Network vulnerability analysis
Installation	· Installation of CBS(Computer Based System) in the airtight device
Control, monitoring and alarm	· Capability to identify and authenticate valid sessions and reject any usage of invalid session · Capability of network monitoring for link up and down of each port on the network device, power on or hardware reset, fan failure, etc. · Capability of monitoring for the status of cat' 2 & 3 devices · Capability for identification and authentication related to wireless communication use, wireless communication encryption, user management, etc.
Segregation and segmentation of network	· Physical network segregation, such as through a firewall, if permitting connections between different networks · Restriction of wireless access to category 2 and 3 device permanently · Disable function for use of removable devices such as USB · Configuring DeMilitarized Zone (DMZ) on the ship network if needed remote access from shore to ship's OT system
Network protection safeguards	· Functions of credentials for network access · Functions of enhanced authentication control or limited authorization for remote access · Restricting physical access to network devices · Configuring minimum privilige policy
Cyber incident detection safeguards	· Intrusion Detection System (IDS) and Intrusion Protection System (IPS) · Timely incident alert systems · Network Performance Monitoring System · Displaying of security events, e.g. Security Information Event Monitoring (SIEM)
Network and system Recovery Measures	· Network device backup and recovery function

Table 5 Network design and configuration requirements

Requirements	Details
Network Protection safeguards	· CBS-related networks separate other networks by firewall or equivalent means · Functions to prevent excessive traffic and protect resources · Ability to deactivate unnecessary functions/ports/protocols and services
Antivirus, antimalware, antispam and other protections from malicious code	· Functions to protect against malicious code such as viruses, worms, trojan horses, and spyware
Access control	· Procedures and functions of access control for cat 2 & 3 system-related networks · Ability of control(write) of access-control lists for file systems/networks/applications · Granting minimal privileges to users permitted to access the network
Wireless communication	· Configuring as a network zone separate from the wired network · Ability to access only authorized users/ devices
Remote access control and communication with untrusted networks	· Ability to disable direct networking from untrusted networks into the secure zone. · Functions related to endpoint authentication, integrity and authentication protection, VPN, etc.
Network operation monitoring	· Monitoring and protecting against excessive traffic · Monitoring or protecting against connection of unauthorized devices
Diagnostic functions of CBS and networks	· Diagnostic functions for CBS and network

특히 IACS UR E26은 선박 사이버 복원력의 핵심 기술로서 사이버 위협 탐지 기능 요구와 함께 CBS 및 네트워크 장치에 대한 기술적 요건을 포함하고 있다. 이중 네트워크 설계 및 구성/설정에 관한 요건은 Table 5와 같다.

3. 선박 네트워크 현황 분석

3.1 선박 네트워크 현황

이 절에서는 현재 건조되어 운항중인 선박의 노드와 링크를 포함하는 네트워크 토폴로지에 대하여 분석하고, 이를 통해 발생 가능한 이벤트 현황에 대하여 식별하고자 한다.

선내 네트워크 토폴로지 분석을 위해 최근 국내 조선소에서 건조·인도된 스마트 선박 3척에 대한 네트워크를 분석하였다.

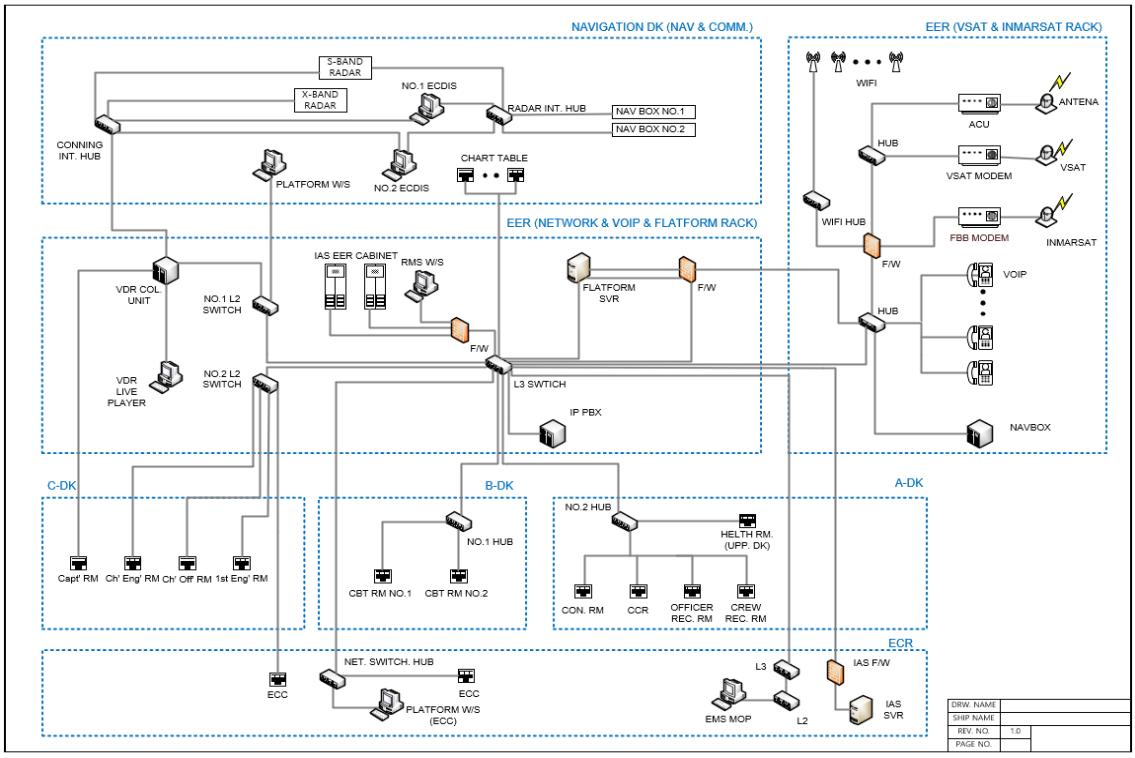

Fig. 1 Ship network topology

선박의 네트워크 구조는 Fig. 1과 같다. 다만, 선사의 내부 보안으로 인해 보안적 이슈가 될 사항은 삭제하고, 일부 내용은 보편적 형식으로 변경하였다.

선박 네트워크는 선박-육상 간 통신을 위한 Inmarsat, VSAT 등의 모뎀이 최상위에 위치해 있으며, 하위에 선박-육상 간 네트워크 보안을 위한 방화벽이 위성 통신 사업자 또는 선주에 의해 설치되어 있다. 다만, 일부 선박의 경우 방화벽이 설치되지 않는 경우도 존재하였다. 방화벽 Downlink로는 선내 네트워크와 선원용 와이파이 간의 망분리를 위해 하나의 허브가 설치되어 있으며, 동 허브에 VoIP(Voice over Internet Protocol) 모뎀 및 스마트쉽 플랫폼, 선내 네트워크를 구성하기 위한 L3 스위치 등이 연결되어 있다.

분석된 대부분의 선박은 L3 스위치에서 OT 시스템 또는 일부 IT 시스템으로 직접 연결되어 있으며, 선내 또는 사무 공간의 업무용 PC 연결을 위한 L2 스위치가 1식 또는 2식 별도로 설치되어 있다.

기관제어의 핵심 시스템인 IAS의 경우 선내 네트워크와 별도로 사설 네트워크망을 구성하고 있으며, 선내 네트워크와는 방화벽을 통해 연결되어 있고, 원격 모니터링 서버(RMS, Remote Monitoring Server)를 통해 DMZ를 구성하고 있다.

항해·통신장비는 별도의 허브를 통해 하나의 네트워크 망을 구성하고 있다. 그리고 Wifi의 경우 외부 네트워킹은 가능하지만 선내 네트워킹은 불가능하도록 설정되어 있다.

3.2 선박 네트워크 트래픽 및 로그 분석

선박 네트워크 트래픽 및 보안 로그 현황 파악을 위해 Fig. 2와 같이 현대LNG해운사에서 최근 건조되어 운항중인 선박 내 상용 SIEM을 설치하였다. 그리고 선내 네트워크 장치(L3 스위치) 및 보안 장치(방화벽)에 CPU & 메모리 상태, 포트 ON/ OFF 정보 등을 획득하기 위하여 SNMP 프로토콜 정보를 수신할 수 있도록 설정하고, Syslog 연계를 통해 보안 장치(방화벽)에서 발생된 다양한 이벤트를 수집할 수 있도록 환경을 구성하였다.

이와 함께 상용 SIEM 내 육상에서 보편적으로 적용중인 보안 정책을 적용하여 선박 네트워크 내에서 발생되는 이벤트를 수집/관리할 수 있도록 설정하였다.

이후 약 45일 동안 선내 네트워크 각 구역(zone)별 트래픽 및 사이버 위협 정보를 수집하였다.

이를 통해 CCTV 및 Wifi 등 비 업무용 네트워크 트래픽을 제외하고 선박 내 교환되는 트래픽 양은 Table 6와 같이 일평균 256MB로 높지 않는 사용률을 확인할 수 있었다.

Fig. 2 Demonstration vessel (HLS)

Table 6 Network traffic status

	Total	Daily average	Daily highest	Daily lowest
Volume	11.5GB	256MB	725MB	186MB

또한, 발생된 위협 이벤트 로그를 확인 결과 Switch로부터 ping fail, port scan 로그 등이 송신됨을 확인할 수 있었다.

4. 선박용 SIEM 탐지 정책 모델 개발

선박용 SIEM의 탐지 정책모델은 운항중인 선박의 선원이 사이버 위협 판단을 위한 효율성 및 편의성 향상과 함께 선박 검사 및 심사 대응을 지원하는 것을 목적으로 하며, SIEM과 상호 연동되는 선내 네트워크 및 보안 장치에 부합되도록 구성하는 것을 목표로 설정하였다.

본 논문에서 제시하고자 하는 선박용 SIEM 탐지 정책 모델은 육상 IT 체계의 사이버보안 탐지 정책을 그대로 적용시키는 것이 아니라 선박 장치와 환경에 최적화되어 선원이 사이버 위협을 이해하고 대응 가능토록 대응 가이드 수립을 목적으로 한다.

선박용 SIEM 탐지 정책 모델 제시를 위해 2장의 해사 분야 규정/지침, 3장의 선박의 네트워크 분석 정보를 토대로 탐지 정책 수립에 필요한 정보 유형으로 변환/분류하고 이를 검증하는 과정 등을 포함한 선박용 SIEM 탐지 정책 개발 절차를 Fig. 3과 같이 제시하였다.

4.1 선박용 SIEM 탐지 정책 항목 선정

3장에서 분석된 바와 같이 최근 건조되는 고부가가치 스마트 선박의 경우 L3 스위치, 방화벽 등은 선내 네트워크 장치로서 이미 설치/운용되어지고 있다. 뿐만 아니라, 고부가가치 선박 외 벌크선 등 선가가 높지 않은 선박 또한 IACS UR E26이 적용됨에 따라 2024년 7월 1일 건조 계약되는 선박의 경우 방화벽 등이 필수적으로 설치 되어질 것으로 판단된다.

다만, IDS(Intrusion Detection System)/IPS(Intrusion Prevention System) 등 대부분의 육상 IT 네트워크 환경에서 설치되는 행위기반 보안 도구는 현재까지 선박 내 설치 사례를 찾기가 쉽지 않을 뿐만 아니라 IACS UR E26에서도 권고 기술로 한정하고 있다.

따라서, 동 논문에서 제시하는 SIEM 탐지 정책은 보편적인 탐지 정책을 목표함에 IACS UR E26에서도 권고 장치로 포함된 IDS/IPS 등은 고려하지 않고 L3 스위치 및 방화벽을 대상으로 선박용 SIEM 탐지 정책을 개발하고자 한다.

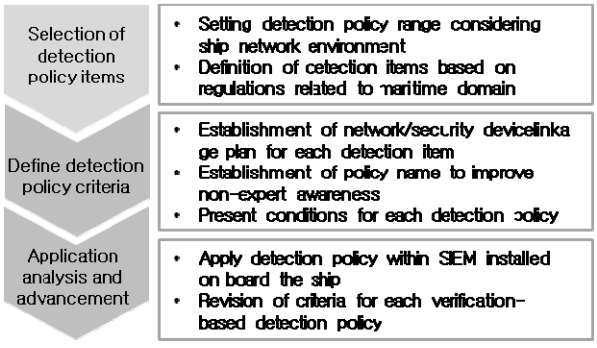

Fig. 3 SIEM detection policy development procedure

Table 7 Definition of detection items

Regulation	Category	Requirements
BIMCO guidelines on cyber security on board ships	Technical protection measures	· Allow specified ports/ protocols /services according to company policy only · Remote access control of OT & IT systems
	Procedural protection measures	· Restrict access to information except to authorized personnel
	Detect, block and alarm	· Set cyber incident alert threshold based on network status data (traffic flow, network operation)
IACS Rec.166	Control, monitoring and alarm	· Connect each port · Downlink of each port · Network(hardware) reset · Network FAN failure · Temperature abnormality
	Network protection safeguards	· Credentials functions for network access · Enhanced authentication control or limited permission control for remote access
IACS UR E26	Network Protection safeguards	· Functions to prevent excessive traffic and protect resources · Ability to deactivate unnecessary functions/ports/protocols/services
	Antivirus and other protections from malicious code	· Functions to protect against malicious code such as viruses, worms, trojan horses, spyware
IACS UR E26	Network operation monitoring	· Monitoring and protecting against excessive traffic

상기 언급된 바와 같이 L3 스위치, 방화벽으로부터 발생/공유되는 보안 로그를 토대로 선원에게 위협 경보를 제공하기 위한 탐지 정책 수립을 위해 2장의 분석된 해사 분야 사이버보안 관련 규정 및 지침을 기준으로 시스템 관점에서 관리 가능한 항목을 Table 7과 같이 식별/분류하였다.

4.2 선박용 SIEM 탐지 정책 및 조건 정의

선박용 SIEM 탐지 정책은 오탐 방지 및 무분별한 알람 방지 그리고 전문성이 결여된 선원이 현장에서도 대응 가능토록 네트워크/보안 장치로부터 이벤트 로그 정보, SIEM 정책 적용 시 필요 정보인 아래의 기준을 토대로 재구성하였다.

· (위협분류) 사이버 위협 종류 구분
· (정책명) 사이버 위협에 대한 이해도 향상을 위한 명칭 정의
· (주기) 식별된 사이버 위협의 신뢰성을 판단하기 위한 기준
· (발생 건수) 사이버 위협 여부를 판단하기 위한 근거
· (근원) 사이버 위협의 근원(Source) 정의
· (조건) 장비별 형상(configuration) 설정값

Table 8 Definition of detection policy

Requirement	Link method	Policy name	Details
Network each port connection (BIMCO, Rec.166)	L3 switch/ Link up message/ Syslog	[System alarm] Detection of a new connected router/switch	· Detect new connections to network ports · Detect unused port unauthorised connections
Network device port link down (Rec.166)	L3 switch/ Link down message/ Syslog	[System alarm] Loss of connection of device connected to router/switch	· Detect down/ failure of each port connected to the network equipment
Network equipment FAN failure (Rec.166)	L3 switch/ FAN function down message / Syslog	[System alarm] Stop rear cooler of router /switch	· Detect failures in the fan function of network equipment
Network hardware reset (Rec.166)	L3 switch/ Config initialization execution message/ Syslog	[System alarm] Router/switch configuration Information changed to default by an outsider	· Detection of unauthorized initialization of network settings
Network hardware reset (Rec.166)	L3 switch/ Factory reset execution message/ Syslog	[System alarm] Restore router /switch to initial state by outsider	· Detection of unauthorized initialization of network equipment settings
Remote access control (BIMCO, Rec.166)	Firewall/ Rule message / Syslog	[System access] Detection of unauthorized remote access service access	· Detection unauthorized remote access to ship's critical assets
Network equipment temperature anomaly (Rec.166)	L3 switch/ Thermometer malfunction message/ Syslog	[System alarm] Thermometer function failure of router/switch	· Detection abnormal temperature changes in network equipment
	L3 switch/ Maximum temperature exceeded message/ Syslog	[System alarm] Router/switch maximum allowable temperature exceeded	· Detect abnormal temperature changes in network equipment
Disabling unnecessary functions/ ports/ protocols/ services (UR E26)	Firewall/ Rule message / Syslog	[Information leak] Detection of unauthorised service use(email,messenger)	· Detect non-business (unauthorized) programs such as email
Disabling unnecessary functions/ ports/ protocols/ services (UR E26)	Firewall/ Rule message / Syslog	[Information collection] Detection of search behavior for collecting information on an operating service (port)	· Detection of unnecessary access (disabled ports, protocols, services, etc.)
	Firewall/ Rule message / Syslog	[Information collection] Detection of search behavior for collecting information on an operating service (IP)	
Monitor excessive traffic (UR E26, BIMCO)	Firewall/ Rule message / Syslog	[Denial of Service] Detection of assets using abnormally large amounts of traffic	· Detection of overused assets exceeding normal traffic volume
Restricted (administrator only) access to information (BIMCO)	Firewall/ Rule message /Syslog	[System access] Detection of unauthorized access to critical assets	· Access to ship's critical assets is granted only to authorized administrators
Protection from malware (UR E26)	Firewall/ Rule message /Syslog	[Malicious code] Detection of connections to services (ports) commonly used by viruses	· Detection of through minimal suspicious communication events if antivirus installation is not possible

이를 위해 Table 7에 정의한 탐지 항목과 선내 설치된 L3 스위치 및 방화벽에서 수집 가능한 이벤트 로그를 매칭시켜 위협 종류별로 항목을 분류(시스템 경보, 시스템 접근, 정보유출 의심, 서비스 거부, 정보 수집, 악성코드)하였다. 그리고 보안 정책의 이해도 향상을 위해 상기 분류된 6가지 위협을 포함하여 Table 8과 같이 사이버 위협 설명을 탐지 정책 명으로 정의하였다.

이와 함께, 발생 근원지(네트워크/보안 장치)로부터 제공되는 이벤트를 위협으로 인지하기 위한 발생 주기 및 건수를 조건으로 정의하였다. 이에 3장 선박 네트워크 트래픽 및 로그 분석 결과를 토대로 상기 정의된 SIEM용 탐지 정책의 발생 비율 등의 조건을 임의로 산출하여 Table 9과 같이 보안 탐지 정책을 수립하였다.

5. 선박용 SIEM 탐지 정책 검증

국제 규정 등 선박의 환경에 부합되는 선박용 SIEM 탐지 정책

Table 9 Definition of alarm criteria for detection policy

Policy name	Time	Criterias	Basis
[System alarm] Detection of a new connected router/switch	10 minutes	1case	· See section 3.2
[System alarm] Loss of connection of device connected to router/switch	10 minutes	1case	· Related cases None
[System alarm] Stop rear cooler of router /switch	1minutes	1case	· Related cases None
[System alarm] Router/switch configuration Information changed to default by an outsider	1minutes	1case	· Related cases None
[System alarm] Restore router/switch to initial state by outsider	1minutes	1case	· Related cases None
[System alarm] Thermometer function failure of router/switch	1minutes	1case	· Related cases None
[System alarm] Router/switch maximum allowable temperature exceeded	1minutes	1case	· Related cases None
[System access] Detection of unauthorized remote access service access	1minutes	1case	· Related cases None
[Information leak] Detection of unauthorised service use (email, messenger)	1minutes	20case	· Related cases None
[Information collection] Detection of search behavior for collecting information on an operating service(port)	1minutes	d_ip>=200	· See section 3.2
[Information collection] Detection of search behavior for collecting information on an operating service(IP)	1minutes	d_ip>=200	· Related cases None
[Denial of Service] Detection of assets using abnormally large amounts of traffic	1minutes	S_ip>= 5000	· Related cases None
[System access] Detection of unauthorized access to critical assets	1minutes	1case	· Related cases None
[Malicious code] Detection of connections to services (ports) commonly used by viruses	1minutes	5case	· Related cases None

을 검증 없이 선박 내 적용한다면 과도하게 탐지 알람을 발생시키거나, 주기 또는 조건이 알람 조건에 부합되지 않아 실제 위협이 선원에게 제대로 전달되지 못하는 효용성의 문제가 발생 될 수 있다. 이에 장비를 운영/사용하는 운영자 입장에서 실제 환경에 맞는지 정책의 효율성을 검증할 필요가 있다.

이에 선박의 보안 현황 분석을 위해 선박에 설치된 상용 SIEM 내 선박용 SIEM 탐지 정책을 적용하여, 가상 이벤트를 발생시켜 탐지 여부를 확인한 후 45일간의 실선 실증을 통해 유효성 검증을 수행하였다.

5.1 관제 시스템 적용

본 논문에서의 검증용으로 설치된 SIEM 솔루션은 이글루코퍼레이션사의 SpiderOT이다. 보안 정책 적용을 위해 SpiderOT의 룰 조건 정의 기능을 사용하여 동 연구를 통해 개발된 선박용 SIEM 탐지 정책을 적용하였다.

이를 위해 Fig. 4, Fig. 5와 같이 방화벽, L3 스위치 등 로그 발생 장치/시스템별로 분류된 그룹 내 동 논문을 통해 개발된 탐지 정책의 이름을 신규 오브젝트로 추가하고, 필드명, 연산자, 값 등의 기본 정의 항목에 발생주기 및 발생조건을 적용하였다.

- 필드명 : sublog, msg, method 등(수집 로그 중 탐지 경보로 설정될 필드의 이름)
- 연산자 : like, in, not 등(경보 발생의 조건 연산자)
- 값 : accept, drop, 22, 23 등(경보로 설정할 문자열)

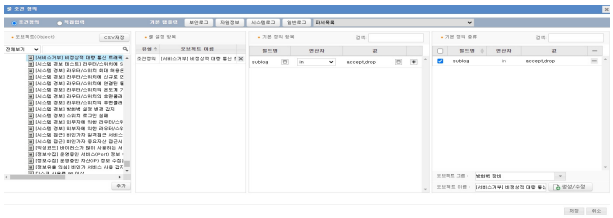

Fig. 4 Applying security detection models to SIEM

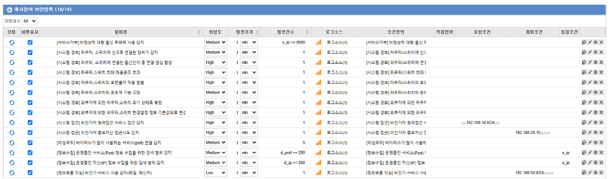

Fig. 5 Results of applying security detection model

5.2 탐지 확인

SIEM 내 보안 정책이 적합하게 적용되어 졌는지 확인하기 위해 Fig. 6과 같이 제조사에서 제공해주는 도구를 활용하여 Table 10과 같이 12종의 탐지 정책에 대한 Test event를 발생시켜 솔루션이 정책에 부합되도록 해당 위협 탐지 여부를 확인해 보았다.

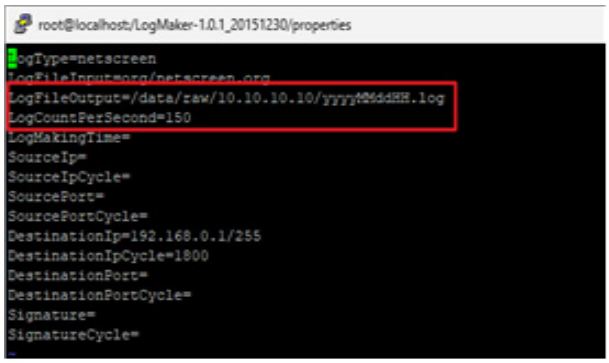

Fig. 6 Log generator

이를 위해 선내 SIEM 서버 내 로그 생성 소프트웨어인 Log Maker를 설치하였으며, 생성된 로그가 SIEM으로 송부되도록 설정하였다. 또한, 물리적 사이버 위협 행위 생성을 위하여 별도로의 노트북을 준비하여 비인가된 IP를 할당하고, NMAP(포트 스캐닝 도구) 및 Hping(대용량 트래픽 생성 도구) 사용을 위해 칼리리눅스(해킹 툴이 포함된 OS)를 설치하였다. 마지막으로 Fig. 7와 같이 선내 네트워크 라우팅 테이블이 생성된 L3 스위치의 빈 포트에 노트북의 LAN 케이블을 연결하였다.

Table 10 Perform virtual attacks and verify detection

Policy name	Test procedure	Validation
[System alarm] Detection of a new connected router/switch	· Connect the LAN cable connected to the laptop prepared to create physical cyber threats to an unused port on the L3 switch. · Check alarm occurrence when connected	○
[System alarm] Loss of connection of device connected to router/switch	· Remove the shipping company email server cable connected to the L3 switch · Check alarm occurrence when disconnected	○
[System alarm] Stop rear cooler of router/switch	· Create log(system fan failed) using Log maker(log creation program) · Check alarm occurrence when creating an event log	○
[System alarm] Router/switch configuration Information changed to default by an outsider	· Create log(reset switch image to factory default) using Log maker · Check alarm occurrence when creating an event log	○
[System alarm] Restore router /switch to initial state by outsider	· Create log(cleared switch configurations) using Log maker · Check alarm occurrence when creating an event log	○
[System alarm] Thermometer function failure of router/switch	· Create log(hardware fan error) using Log maker · Check alarm occurrence when creating an event log	○
[System alarm] Router/switch maximum allowable temperature exceeded	· Create log(temperature measurement not functioning) using Log maker · Check alarm occurrence when creating an event log	○
[System access] Detection of unauthorized remote access service access	· Access the ship's email server via TELNET with a laptop prepared to create physical cyber threat actions. · Check alarm occurrence when accessing	○
[Information leak] Detection of unauthorised service use (email, messenger)	· Remove outlook from SIEM white list · Install outlook s.w on the ship's email server · Check alarm occurrence when installing the s.w	○
[Information collection] Detection of search behavior for collecting information on an operating service (port)	· Collect onboard network port information via NMAP on laptops prepared to create physical cyber threat actions. · Check alarm occurrence when collecting information	○
[Information collection] Detection of search behavior for collecting information on an operating service (IP)	· Collect onboard network IP information via NMAP on laptops prepared to create physical cyber threat actions. · Check alarm occurrence when collecting information	○
[Denial of Service] Detection of assets using abnormally large amounts of traffic	· Generate massive traffic via Hping on laptops prepared to create physical cyber threat actions. · Check alarm occurrence when generating traffic	○
[System access] Detection of unauthorized access to critical assets	· Access to onboard mail servers with a laptop prepared to create physical cyber threat actions. · Check alarm occurrence when accessing	○
[Malicious code] Detection of connections to services (ports) commonly used by viruses	· Forced access to vulnerable ports via TELNET on prepared laptops to create physical cyber threat actions · Check alarm occurrence when accessing	○

Fig. 7 Testing environment

5.3 유효성 검증

본 논문에서 제안한 선박용 SIEM 탐지 정책 모델의 유효성 평가를 위해 Table 9의 조건이 적용된 SIEM을 Fig. 8과 같이 현존선에 탑재하여 45일간 운영 및 평가를 진행하였다.

Table 11은 본 논문에서 제안하는 선박용 SIEM 보안 정책에 따라 발생된 알람을 목록화한 표이다.

본 검증을 통해 등록된 자산의 통신 이상 발생, SSH 서비스 접근, Port 스캔 이벤트 등의 사이버 위협 이벤트 경보가 확인되었다.

발생된 통신 이상 이벤트는 다수의 자산이 동시 다발적으로 다양하게 발생되었으며, 실제 선박 내 일부 통신 구간에 단발적 문제가 있었던 것으로 확인되었다. 다만, 신조선으로 인해 시스템이 아직 안정되지 않은 상황임을 고려할 필요가 있었다. SSH 서비스 접근, Port 스캔 이벤트 등의 정보 수집형 이벤트는 오픈된 서비스 포트가 외부에 노출되어 있어 지속적인 접속 시도가 발생하는 것을 확인할 수 있었다. 상기 노출된 서비스 포트는 원격 접속을 통해 방화벽에 보안 설정(해당 IP 차단)을 진행하였다.

Fig. 8 SIEM installed on-board

6. 결 론

스마트 선박의 도입에 따라 선박의 사이버 침해사고가 급증하고 있다. 이에 국제해사기구(IMO) 등 공공/민간기구에서는 선박

Table 11 Effectiveness evaluation results

Policy name	Number of occurrences	Remark
[System alarm] Detection of a new connected router/switch	–	–
[System alarm] Loss of connection of device connected to router/switch	35,766 cases	Change occurrence cycle. 1minute → 1hour
[System alarm] Stop rear cooler of router/switch stops working	–	–
[System alarm] Router/switch configuration Information changed to default by an outsider	–	–
[System alarm] Restore router /switch to initial state by outsider	–	–
[System alarm] Thermometer function failure of router/switch	–	–
[System alarm] Router/switch maximum allowable temperature exceeded	–	–
[System access] Detection of unauthorized remote access service access	138 cases	Add firewall white list
[Information leak] Detection of unauthorised service use (email, messenger)	–	–
[Information collection] Detection of search behavior for collecting information on an operating service (port)	1 cases	Add firewall white list
[Information collection] Detection of search behavior for collecting information on an operating service (IP)	–	–
[Denial of Service] Detection of assets using abnormally large amounts of traffic	1 cases	Add firewall white list
[System access] Detection of unauthorized access to critical assets	–	–
[Malicious code] Detection of connections to services (ports) commonly used by viruses	–	–

사이버보안과 관련하여 선박 건조 및 운항에 직접적인 영향을 끼칠수 있는 다양한 규제/기준을 발행하고 있다. 특히, 국제선급협회의(IACS)의 UR E26은 선박 네트워크 설계 등 사이버보안과 관련된 강제 요구사항으로서, 선내 네트워크 모니터링 도구 도입을 필수 항목으로 제시하고 있다. 따라서 본 연구에서는 선박의 보안 관점에서 네트워크 모니터링 도구 개발의 첫 단계로서 선박용 SIEM을 위한 탐지 정책 모델을 개발하였다.

제안된 선박용 SIEM 탐지 정책 모델은 해사분야 규정의 최소 요건을 만족하도록 구성하였으며, 네트워크 관련 지식이 부족한 선원도 이해하기 용이하도록 구성하였다. 따라서 향후 선박 내 SIEM이 탑재/설치되면 손쉽게 적용하여 선박 보안 관제에 활용할 뿐만 아니라 검사/심사에 활용될 수 있도록 개발하였다. 뿐만 아니라 선박의 특수한 환경을 고려한 보안 탐지 모델로서, 향후 선박용 SIEM 구축 시 다양한 아이디어를 제공해 줄 수 있을 것이라 기대된다.

하지만, 본 정책 모델을 그대로 선박용 SIEM에 적용하기에는 다소 미흡한 부분이 남아있다. 현재 운항중인 선박 내 네트워크 모니터링 도구 설치 사례가 전무함에 동 논문에서 제시한 정책 모델은 국제 규제/기준을 기반으로 세부 항목이 도출되어졌다. 이에 방화벽으로부터 제공되는 트래픽 정보를 토대로 추론 가능한 위협 정보 유형(서비스 거부 공격 등) 등 선주의 정책에 따라 결정될 수 있는 항목들은 고려되어져 있지 않다.

향후 국내 선사와 협력하여 본 논문에서 제시한 보안 정책을 선박 내 적용하고, 1년 이상의 장기간 실증을 진행할 예정이다. 이를 통해 단기간 검증으로 만족하지 못한 정책 조건의 고도화와 함께 장기적 누적된 이력(이벤트 로그, 트래픽 정보)을 기반으로 추론 가능한 위협 정보 유형을 보완할 예정이다.

후 기

본 연구는 2024년도 산업통상자원부 조선해양산업핵심기술개발사업(20026436)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

References

Baltic International Maritime Conference(BIMCO), 2016. The Guidelines on cyber security onboard ships edition 1.

Cha, B.R., Choi, M.S, KANG, E.J., Park, S. and Kim, J.W., 2017. Trends of SOC & SIEM Technology for Cybersecurity. Smart media Journal, v.6 no.4, pp.41-49.

Gang, N.S., 2018. Analysis of onboard ship cybersecurity. *Journal of the Korean Society of Marine Engineering,* 42(6) pp.463-471.

International association of classification societies(IACS), 2020. Rec 166 - Recommendation on Cyber Resilience, URL : https://iacs.org.uk/resolutions/recommendations/161- 180/rec-166-new-corr2-cln.

International association of classification societies(IACS), 2022. unified- requirements E26 Cyber resilience of ships - Rev.1, URL : https://iacs.s3.af-south-1.amazo naws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf.

International association of classification societies(IACS), 2022. unified- requirements E27 cyber resilience of on-board systems and equipment-Rev.1, URL : Available :https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf.

International Maritime Organization(IMO), 2017. Maritime cyber risk management in safety management systems, resolution MSC.428(98), pp.1.

International Maritime Organization(IMO), 2022. Guidelines on maritime cyber risk management, MSC-FAL/Circ.3/Rev.2, pp.1-6, 2022.

Ko, K.J. and Jo, I.J., 2021. Application of integrated security control of artificial intelligence technology and improvement of cyber-threat response process. *The Journal of the Korea Contents Association*, 21, pp.59-66.

Korea Maritime Institute(KMI), 2023. IMO International Maritime Policy Trends, 126, pp.3.

Lee, E.S, Ahn, Y.J. and Park, S.H., 2020. A study on the development of a training course for ship cyber security officers. *Journal of the Korean Society of Marine Environment & Safety,* 26(7), pp.830-837.

National institute of standards and technology(NIST), 2018. Framework for improving critical infrastructure cybersecurity ver 1.1, pp.6-8 URL: https://csrc.nist.gov/pubs/cswp/6/cybersecurity-framework-v11/final.

Oil Companies International Marine Forum(OCIMF), 2017. *Tanker management and self assessment 3* - A Best Practice Guide, pp.2.

Oil Companies International Marine Forum(OCIMF), 2018. *SIRE-overview-factsheet*, pp.1-2, 2022.

Park, J.S., 2020. The components of a cyber ship model. *Bulletin of the Society of Naval Architects of Korea,* 57(4), pp.7-13.

Shibata J, 2023. Journey towards cyber-resilience of ship. Maritime cyber security and resilience symposium.

The Korea Economic Daily, 2024. HD Hyundai Marine Solution to enter ship cyber security, URL: https://www.kedglobal.com/shipping-shipbuilding/newsView/ked202401220008.


손금준


안종우


이창식


강남선


김성록