Training the Maritime Security Operations Centre Teams

Marco Raimondi, Giacomo Longo, Alessio Merlo, Alessandro Armando, Enrico Russo
DIBRIS - University of Genova, Italy
{marco.raimondi, giacomo.longo}@dibris.unige.it, {alessio.merlo, alessandro.armando, enrico.russo}@unige.it

2022 IEEE International Conference on Cyber Security and Resilience (CSR) | 978-1-6654-9952-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSR54599.2022.9850324

***Abstract*—A Security Operation Centre (SOC) is a powerful and versatile infrastructure for cybersecurity due to the capabilities of monitoring and improving the security posture of an organization. While they found great diffusion in companies to defend IT/OT infrastructures, their employment in the maritime domain is still narrow but required. Nevertheless, SOC analysts working in traditional SOCs may be unprepared to operate proficiently in the maritime environment due to its context-specific features. They require specific training to fully exploit these newfound requirements. In this work, we leverage the NICE framework to outline the profile definition of a SOC operator in terms of required knowledge and skills. This profile allowed us to define the requirements of a training program tailored for maritime SOC operators. Moreover, we show how this program can be fulfilled with targeted hands-on exercises. An example exercise set in a representative scenario highlights that we are able to train the specific skills with metrics for evaluating their proficiency.**

I. Introduction

Ships have become complex cyber-physical systems, with traditional Operation Technology (OT) infrastructures strictly connected to new and essential Information Technology (IT) components. This rapid digitalization of the maritime industry has brought significant advantages but at the cost of increasing the attack surface of the ship. As a matter of fact, the number of cyber-attacks targeting the maritime system is growing [1], thereby suggesting that the current threat environment is larger and more complex than in the past. Furthermore, the context-specific features and the lack of detailed and updated threat reports make it hard to build reliable countermeasures. For this reason, the first line of defense lies in preparing and engaging facilities capable of monitoring and analyzing the security posture of assets of this domain, along with the knowledge building to improve it. The state-of-the-art approach used for traditional IT/OT infrastructures is to create a Security Operations Center (SOC). This solution poses the problem of employing operators with specific domain knowledge and expertise, but the reliable training of such personnel is still an open issue in the maritime domain [2]. To this aim, this paper provides a three-fold contribution. First, we propose a description of the profile of a maritime SOC operator. Using a standard and detailed taxonomy, we distinguish and explain two different expertise, one related to the skills and knowledge for operating in traditional IT and OT infrastructures, and another including only maritime-specific one. Our second contribution consists of a virtual scenario for simulating a vessel's Integrated Navigation System (INS) and monitoring infrastructure, which helps carry out hands-on exercises in a controlled and flexible environment. Finally, we propose a training exercise that leverages our testbed and focuses on a specific subset of skills and tasks. We also show some metrics for evaluating the acquired skills of the trainees.

978-1-6654-9952-1/22/$31.00 ©2022 IEEE

The paper is structured as follows. Section II describes the profile of the maritime SOC operator. Section III depicts the testbed infrastructure and its implementation. Section IV describes the training exercise and the metrics used for the evaluation. Section V discusses some related work concerning the training of maritime SOC operators. Finally, Section VI points out some future work.

II. Maritime SOC Operators

A. Overview

Ship's infrastructures can be compared to traditional IT/OT systems. For this reason, the SOC operators already engaged in such infrastructures can have the essential capabilities to operate in the maritime context. We identify the above capabilities as the *main expertise*. However, ship's infrastructures also have significant differences from traditional systems. These differences require SOC operators to adapt and enhance their expertise in such scenario. We identify the capabilities that qualify maritime SOC operators as the *qualifying expertise*.

To define the main expertise, we use the taxonomy and common lexicon described in the National Initiative for Cybersecurity Education [3] (NICE) framework provided by the National Institute of Standards and Technology (NIST). NICE represents a common and fundamental reference for describing and sharing information about cybersecurity work. In particular, we refer to three building blocks of the framework, i.e., *Knowledge* (K), *Skill* (S), and *Task* (T). Briefly, K includes topics that an operator should know. S represents the technical capabilities learned through training. T comprises activities to achieve a specific objective.

For each of them, NICE provides a rich catalog of statements (named with unique numeric identifiers) to detail a cybersecurity work, i.e., a *Work Role* (WR), in terms of KST.

Referring to NICE, the qualifying expertise requires growing K of WRs related to SOC operators. As a consequence of such an extension, a maritime SOC operator has to leverage their S to perform the associated T.

For example, the knowledge of computer networking concepts and protocols (see K0001) is suitable for the infrastructure connecting the equipment of an INS. Nevertheless, the INS equipment communicate with the ship's sensors using a context-specific protocol, namely NMEA [4]. For this reason, maritime SOC operators require extending their knowledge to the internals of the above protocol. Thus, operators can enhance their skill in developing and deploying signatures (see S0020) to address NMEA packets and successfully apply the task of using cyber defense tools for monitoring the system activity (see T0259) of an INS.

In Section II-B, we detail the WRs that correspond to SOC operators and hold KSTs defining the main expertise.

In Section II-C, we describe the context-specific features that extend the above KSTs with the qualifying expertise.

B. Main expertise

SOC teams usually follow a tiered structure that organizes operators according to their experience. Starting from the level that comprises operators with the lowest experience, in this paper, we consider the first two, namely *Tier 1* and *Tier 2*.

As detailed in [5], Tier 1 refers to a group devoted to real-time triage of alerts, i.e., the process of sorting, categorizing, and prioritizing incoming events and other requests for SOC resources. Tier 2 accepts cases from Tier 1 and performs in-depth analysis. This group acts to determine what happened and whether further action is necessary.

We map the expertise required by the duties of the above levels with the *Cyber Defense Analyst* [6] and *Cyber Defense Incident Responder* [7] WRs from NICE.

To arrange S and T from such WRs in accordance with the goals of a hands-on training program, we used the Stenmap framework [8]. In particular, a Stenmap maps the skills that a serious game can measure along with the corresponding actions to determine their achievement and levels of proficiency.

Briefly, a Stenmap follows a layered structure where, starting from the top, $L1$ groups skills into areas, $L2$ specifies skills that each area requires, $L3$ indicates tasks for each skills, $L4$ identifies measurement points for each task, and $L5$ associates a proficiency scale to each measurement point.

Figure 1 depicts the first three layers of the Stenmap of the main expertise. It covers S and T from the two WRs that we identified above. NICE provides an extensive list of such statements to outline the WRs. For the sake of presentation, we identify groups of S (SG) and groups of T (TG) that gather statements related to the same activity or objective [1]. In particular, we associate the Areas of skills layer (L1) with the two tiers that can be assigned to SOC operators. The Skills layer (L2) holds SGs connected to each tier. The Tasks layer (L3) collects TGs and connects them to SGs.

Below, we provide details about SGs and their related TGs.

SG1 Configuring: This group gathers skills related to the security monitoring tools that a SOC typically uses, e.g., the Security Information and Event Management (SIEM) or the Intrusion Detection System (IDS). In particular, related tasks (TG1) allows operators to tailor the signatures and configurations of the above tools.

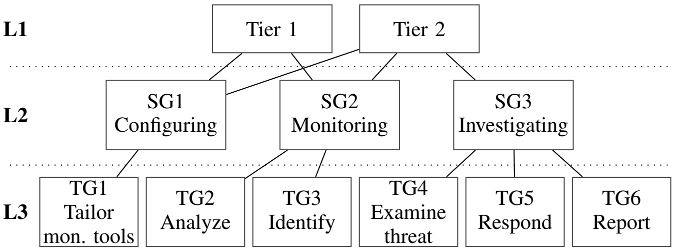

Fig. 1. Stenmap (partial) of the main expertise.

SG2 Monitoring: This group collects capabilities that allow operators to analyze and interpret data and events collected from the system under monitoring. The first set of connected tasks (TG2) allows the operators to maintain situational awareness by analyzing received data. When an anomaly arises, operators must be able to distinguish between false positives and real threats by correlating multiple events (TG3).

SG3 Investigation: This group identifies skills that allow tier 2 operators to conduct a deep investigation of an incident after receiving evidence from tier 1. An investigation starts with tasks for examining all the necessary information regarding the incident, like objectives and possible consequences on the system (TG4). Then, operators must perform tasks for responding to the incident by helping affected users, assisting the team in charge of recovering from its consequences, and suggesting possible actions for improving cybersecurity (TG5). Finally, they require reporting all the findings and details about the incident to keep and share the acquired knowledge (TG6).

C. Qualifying expertise

As previously mentioned, knowledge of distinctive features of vessels creates the qualifying expertise allowing SOC operators to carry out their activities in a maritime scenario. Below, we present such distinctive features and the SG and TG of the main expertise that they affect.

Sensors: All vessels are equipped with a common set of sensors needed to operate, e.g., GPS, gyroscope, speed log, and Automatic Identification System [9] transponder. Many documented attacks [10] aim at deceiving seafarers by spoofing sensors and injecting false data. Maritime SOC operators require knowing the functions, the output data, the admissible values, the tolerable measurement error, and the level of trustworthiness of onboard sensors. Such knowledge helps create context-specific skills related to SG1, SG2, and SG3 and performs tasks to collect (TG1), validate, and correlate sensors data (TG2, TG3) to identify and examine anomalies (TG4, TG6).

Integrated Navigation System: Whenever modern vessels depend on many IT and OT assets, the core of all the onboard systems is the INS. It collects data coming from sensors and peripheral systems integrating them to provide

[1] Exercises built on our Stenmap can make explicit the individual statements involved as a reference for instructors and trainees (see Section IV-A).

a comprehensive view of the ship. INS integrity ensures the ship's operativity and safety during navigation. For this reason, a maritime SOC must carefully monitor and assess its integrity. This duty requires operators to know the components it hosts, e.g., the Electronic Chart Display and Information System (ECDIS) or the Radar and Conning display, and hone skills related to SG1, SG2, and SG3. In particular, knowledge of principles of their use, the data they produce and exchange, and their interaction allows operators to perform tasks to configure the tools (TG1), monitor for anomalies (TG2, TG3), and investigate and report incidents appropriately (TG4, TG6).

NMEA: The electronic exchange of navigational data is standardized through NMEA 0183 and transmitted using IP networks and UDP datagrams. NMEA uses simple ASCII messages, namely *sentences*, that hold the talker and sentence identifier, the payload, and a checksum. The skills and tasks we have introduced for sensors and INS strictly depend on the knowledge of the internals of this protocol and the data sources it supports.

Satellite connection: Ships access the Internet through a satellite connection. The satellite also provides a way to connect ships to remote SOCs for sending data to be monitored and enabling access to operators. Nevertheless, such connections are limited in bandwidth and subjected to downtimes [11]. This condition affects SG1. In particular, operators require configuring the monitoring tools within these limitations and appropriately selecting the data sources and the rules for aggregating them (TG1).

Regulations: Shipping is subjected to different international regulations that cover both the procedures that crews must comply with and the performance standards of the equipment. In particular, the International Maritime Organisation (IMO) has recognized that a cyber attack could significantly impact ships' safety. For this reason, they update Safety of Life at Sea (SOLAS) treaty with the resolution MSC.428(98) [12], requiring all ship owners and operators to manage cyber security risks within their safety management systems. The knowledge of such regulations allows SOC operators to improve SG3 and perform the incident responding tasks (TG5) accordingly. Furthermore, knowledge of the performance standards impacts SG1, SG2, and SG3. SOC operators must configure tools (TG1) and conduct monitoring and incident analyses (TG2, TG3, TG4) by ensuring that their activities do not affect certifications and expected performances.

Soft skills: In most cases, a ship's crew does not include IT specialists, and often deck officers carry out the related procedures [13]. In general, officers have a shortage of cybersecurity awareness and they lack the knowledge of procedures to measure the impact and evaluate the spread of a cyber attack onboard [14]. Maritime SOC operators must be aware of this condition and must be trained with the soft skills to relate to crews. These soft skills mainly impact SG3 and tasks to examine (TG4) and respond to an incident (TG5).

III. Training Scenario

Cybersecurity training requires practical learning opportunities to gain real-world skills. To this aim, we propose a scenario where maritime SOC operators can practice with hands-on experiences.

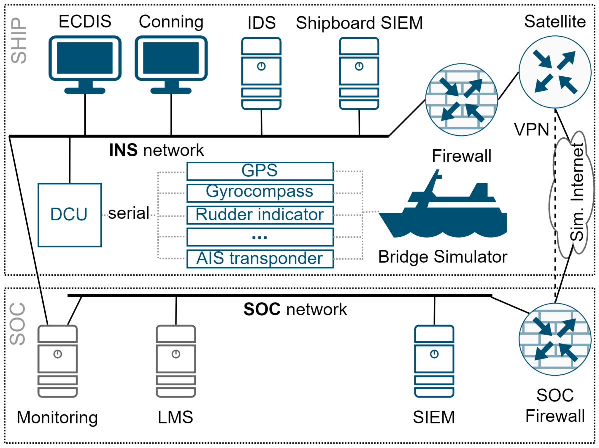

Fig. 2. Training scenario

Figure 2 shows its general layout and components. It is inspired by the architecture proposed by Jacq et al. [11] and includes a shore-side center hosting the maritime SOC and a ship representing the remote site to monitor.

We implemented the above scenario using LiDiTE [15], a digital twin framework that leverages Linux containerization.

Below we detail the remote site and the shore-side center.

A. Remote site

As previously mentioned, the remote site is the ship under monitoring. In particular, it replicates the INS network and a set of components and configurations related to the distinctive features that we presented in Section II-C.

Briefly, we use the *Bridge Command* [16] ship simulator to simulate a ship at sea and onboard sensors, e.g., GPS, speed log, rudder indicator, and AIS transponder. A python script works as a Data Collection Unit (DCU) by collecting data generated by the simulator and transmitting them on the INS network using IP multicast and NMEA over UDP. A Microsoft Windows workstation runs the *OpenCPN* Chart Plotter Navigation [17] that serves as the onboard ECDIS. Instead, we replicate the conning display using a Linux container running the instrument panel of the *Signal K* [18] server.

The INS network also hosts two tools managed by the maritime SOC, i.e., the IDS and the shipboard SIEM. We use *Suricata* [19] Lua [20] scripting to parse NMEA traffic for implementing the IDS functionalities. Regarding INS, IDS functionalities are twofold: (i) capturing NMEA traffic from the INS network and forwarding parsed data to the shipboard SIEM, (ii) performing the real-time detection of anomalous patterns [21] on such traffic, e.g., nonexistent/unexpected values or conformity issues.

The shipboard SIEM is implemented with the Splunk [22] platform and provides the *cyber situational awareness console* by collecting and correlating data from different sources, i.e., IDS alerts, NMEA data, and logs from the workstation and the ECDIS software. Moreover, the shipboard SIEM forwards data to the shore-side center and can select and aggregate them to overcome bandwidth and connectivity issues related to the satellite connection.

A host running the *OPNsense* [23] platform provides the firewall capabilities to the INS network and interacts with a satellite router for connecting the ship to a network working as the simulated Internet. It also creates a Virtual Private Network (VPN) with the shore-side center leveraging the simulated Internet. Such a VPN allows SOC to receive data from the shipboard SIEM and operators to access the ship remotely.

Finally, a node running the *OpenWrt Project* [24] works as the satellite router. It can also be configured to simulate the ship's bandwidth limitation and potential disconnections from the shore-side center during the training.

B. Shore-side center

The shore-side center replicates the SOC facilities. In particular, it comprises a network hosting a OPNsense firewall and a Splunk node working as the main SIEM.

The firewall provides the endpoint for the VPN with the ship under monitoring. The main SIEM receives and collects (possibly aggregated) data from the shipboard SIEM. Tier 1 operators use it to configure rules (TG1), monitor the remote side (TG2), and perform alerts triage (TG3). Tier 2 operators can leverage the VPN to connect to the ship and access the shipboard SIEM to perform tasks related to examining threats (TG4), responding (TG5), and reporting (TG6).

Moreover, the SOC network hosts two nodes that work as facilities for the training execution: the Learning Management System (LMS) and the Monitoring host.

The LMS keeps learning material and information about the scenario, e.g., network scheme, addresses, and credentials. During exercises, it can also receive reports from trainees about their activities. Such reports contribute to the final evaluation after the instructors review them. *Moodle* [25] implements the functionalities of the LMS.

The Monitoring host interacts with nodes of the SOC and INS networks for retrieving the measurement points and artifacts, and associates them with a proficiency scale. For example, it queries the SIEM to check a measurement point based on whether an alert was triggered after an attack. Then, the timestamp in the alert can be used to calculate the time elapsed to detect the attack and associate the proficiency scale. Prometheus [26] and Grafana [27] implement the functionalities of the Monitoring host.

IV. Training Example

A. Overview

Although all exercises can share the same scenario, we denote them by means of the qualifying expertise they require, the skills and tasks they train, and how they measure the trainees' performances. As an example, we consider an exercise for Tier 1 operators that requires the qualifying expertise related to sensors and INS. In particular, trainees need to work on the SIEM to prove their skills to (i) configure rules (SG1) for detecting attacks against INS and sensors and triggering an alarm (TG1), and (ii) correlate data (SG2) to distinguish between benign and anomalous activities (TG3).

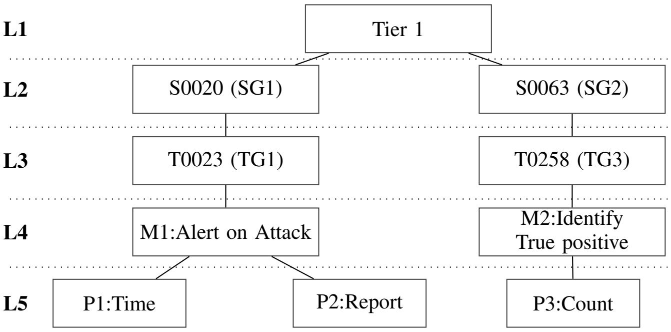

Fig. 3. Stenmap of the example exercise.

In Figure 3, we depict the Stenmap associated with the example exercise. Briefly, it is about skills related to Tier 1 operators (L1). The specific statements it is focused on (L2) are "*skill in developing and deploying signatures*" (S0020), and "*skill in collecting data from a variety of cyber defense resources*" (S0063). The above skills require training tasks (L3) related to "*characterize and analyze network traffic to identify anomalous activity and potential threats to network resources*" (T0023) and "*provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities*" (T0258), respectively. The measurement points (L4) are when an alert is successfully triggered after an attack (M1) and when an artifact is correctly identified as anomalous or benign (M2). We associate with M1 a proficiency scale computed on (i) the time elapsed from the attack to the alarm trigger (P1), and (ii) a report from trainees describing the query they used to trigger the alarm (P2). Finally, we associate with M2 a scale based on the count of anomalies (true positive) properly classified (P3).

Below, we detail the implementation of the exercise.

B. Settings

In the example exercise, the ship under monitoring is at sea. Before leaving the port, the crew reported gyrocompass problems due to fluctuating values during previous trips. Since the sensor does not seem faulty, SOC has been alerted to monitor the navigation network for possible attacks.

The SIEM at the shore-side receives all data collected by the shipboard one, and it does not have any presets.

The objectives of the exercise are (1) configure the SIEM at the shore-side by adding a query that triggers an alarm when an attacker tries to tamper with data from the compass, (2) document the above query in the form of a report, (3) use the SIEM to identify anomalous values during an attack. To prove the achievement of the objectives, the trainees have to (1) write an alert query that adds an event in the *score* repository, or index, of Splunk when triggered, (2) submit a report to the LMS explaining the alert query, and (3) move anomalous events to the *anomalous* index of Splunk.

C. Execution

Executing the exercise requires to start an attack that injects NMEA packets with false values for `HDT` sentences (true heading) on the INS network. To this aim, we implemented a python script that injects such malicious packets.

In detail, it connects the INS network and overhears NMEA traffic from multicast. When it receives an `HDT` sentence with h as the heading value, it injects a number of n_{pkts} new packets having a heading value $h_{new} = (h + x) \mod 360$, where k is an offset, and x $\sim \mathcal{N}(k, \sigma^2)$. The values of n_{pkts}, k, and σ are customisable parameters of the script.

Moreover (see [10]), the script spoofs the address of the DCU to make packets appear legitimate and can superimpose actual values of the gyrocompass by injecting them with a high frequency, i.e., $n_{pkts} > 10$.

The exercise allows a timeframe for the trainees to familiarize themselves with the scenario and configure the SIEM before running the script. When it starts, it logs the timestamp related to the start of the attack, the value of n_{pkts}, and the details of each sent malicious packet. The trainees' evaluation requires these data to calculate the proficiency scale.

Seen from the standpoint of trainees, detecting such an attack requires monitoring for an *Over Reporting* anomaly [21], i.e., the rate of receiving `HDT` sentences is more than usual.

To detect the anomaly, they first need to establish the baseline rate of NMEA packets emitted by the gyrocompass before the attack. Below, we show the query `q1` written in Splunk *Search Processing Language 2* (SPL2) [28] that calculates a statistical upper bound `UCL` of the `HDT` packets rate based on the mean and standard deviation. We use data belonging to a sliding window of ten seconds across a time span of two minutes.

```
/* q1 */ index="main" earliest=-2m latest=-10s
| timechart aligntime=earliest
  count(eval(type="HDT")) as npkts span=10s
| eventstats avg(npkts) as Avg,
  stdev(npkts) as Std | eval UCL=Avg+3*Std
```

Then, trainees can use the second query `q2` to trigger an alarm when the `HDT` packets rate exceeds the calculated `UCL`, e.g., 8.99534.

```
/* q2 */ index="main" earliest=-20s latest=-10s
| timechart aligntime=earliest count(eval(type="HDT"))
  as npkts span=10s | where npkts > 8.99534
```

Finally, achieving the third objective requires trainees to envision a query that separates legitimate and malicious sentences. Below, we show the query `q3` that realizes such a goal by mapping the heading values to the unit circle (a domain in which euclidean distance well approximates the closeness of values) and performing k nearest neighbor to split the data into two classes.

```
/* q3 */ index=main type=HDT earliest=-10s
| eval x=cos(hdt*pi()/180), y=sin(hdt*pi()/180)
| table x y hdt | kmeans k=2 x y
| stats avg(hdt),count(hdt) as ct_hdt,values(hdt)
  by CLUSTERNUM | eventstats max(ct_hdt)
  as max_ct_hdt | where ct_heading=max_ct_hdt
```

Recognizing the malicious sentences implies selecting the class with the highest population, a consequence of the high-frequency nature of the attack.

We omit the SIEM configurations that fulfill the requests of adding events to score and anomalous indexes for brevity.

D. Trainees' evaluation

At the end of the exercise, the Monitoring Host (MH) retrieves the event from the score index stating if trainees detected the attack. MH calculates Δt that represents the detection delay w.r.t. the start time of the attack. MH also checks if the events of the anomalous index match with the logged malicious packets. It returns the total number of (i) packets (T_{num_pkts}), (ii) malicious packets (A_{num_pkts}), (iii) packets correctly classified as anomalous (TP), (iv) packets incorrectly classified (FP).

Moreover, R_{eval} represent the score $\in [0 - 10]$ the instructors assigned to the report.

We propose the following weighted sum to evaluate the overall trainee performance.

$$\alpha\frac{R_{eval}}{10} + \beta\frac{TP}{A_{num\_pkts}} - \gamma\frac{FP}{T_{num\_pkts}} - \eta R\left(\frac{\Delta t - k_t}{T}\right)$$

The first term covers the evaluation of the report. The second term weights the malicious packets that trainees correctly classified. The third term introduces a penalization related to the number of incorrectly classified packets. Finally, we add a penalization for Δt, normalized by the exercise length T, with a grace period of k_t implemented via the *ramp* function $R(x) := \max(0, x)$. Chosen a maximum score M, and weights s.t. $\alpha+\beta = M$, $\gamma+\eta = \lambda M$ with $\lambda \in [0, 1]$, the ratio between α and β controls the relative weight of the report w.r.t. the actions in the SIEM, while λ allows to customise how much penalties can influence the final score. By balancing α, β, γ, η, and λ, the exercise score composition can be tailored to the desired S and T, e.g., an exercise aimed only at evaluating S0063 and T0258 (see Figure 3) might only include β and γ as non-zero coefficients.

V. Related Work

Jacq et al. [11] design complete infrastructure for a maritime SOC emphasizing that traditional one are not ready to be directly applied to this context. Unlike us, they do not focus on the operators, their specific knowledge, and training.

Vielberth et al. [29] highlight challenges in training SOC operators and a general lack of specialized programs. As we developed for INS, they presented in [30] a digital twin of an IT/OT scenario to train SOC analysts. However, their scenario does not fit the unique features required to train maritime SOC operators.

Canepa et al. [31] argue that it is necessary to create a training framework for increasing cyber security awareness of personnel working in the maritime sector. Similar to our scenario, in the Cyber-MAR project [32], they propose to reproduce vessel navigation and automation systems to simulate and validate cyber attacks. Tam et al. [33] also propose the use of a cyber range with maritime scenarios to raise awareness and prepare defensive strategies. Nevertheless, they do not detail exercises for SOC operators and the assessment metrics.

VI. Conclusions and future works

In this paper, we outline the profile of a maritime SOC operator by identifying the qualifying expertise needed for operating in this specific context. A scenario replicating the main components of a SOC facility and ship's INS and a hands-on exercise showed the feasibility of a training program tailored for maritime SOC operators. As future work, we plan to include other ship components in our scenario and execute additional exercises covering the different skills and tasks of such operators. In this way, we can further improve the training program and level of involvement.

VII. Acknowledgments

This work was partially supported by research funding from Fincantieri S.p.A. The research activities are carried out thank to the ShIL (Ship-In-the-Loop) research infrastructure, co-funded by Regione Liguria, University of Genova and DLTM under the program POR FESR LIGURIA 2014-2020 ASSE 1 "Research and Innovation (OT1)" Action 1.5.1 Notice "Support for research infrastructures considered critical / crucial for regional systems".

References

[1] P. Meland, K. Bernsmed, E. Wille, Ø. Rødseth, and D. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, 2021.

[2] M. Vielberth, M. Glas, M. Dietz, S. Karagiannis, E. Magkos, and G. Pernul, "A digital twin-based cyber range for SOC analysts," in *Data and Applications Security and Privacy XXXV*. Springer International Publishing, 2021, pp. 293–311. [Online]. Available: https://doi.org/10.1007/978-3-030-81242-3_17

[3] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (nice) cybersecurity workforce framework," *NIST special publication*, vol. 800, no. 2017, p. 181, 2017.

[4] *61162-1 Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces—Part 1: Single Talker and Multiple Listeners*, International Electrotechnical Commission Std., Rev. 2016.

[5] C. Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*. MITRE Corporation, 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[6] "Cyber Defense Analyst Work Role," NIST, accessed on 09/04/2022. [Online]. Available: https://https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Analyst&id=All

[7] "Cyber Defense Incident Response Work Role," NIST, accessed on 09/04/2022. [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Incident+Responder&id=All

[8] S. Mäses, L. Randmann, O. Maennel, and B. Lorenz, "Stenmap: Framework for Evaluating Cybersecurity-Related Skills Based on Computer Simulations, booktitle = Learning and Collaboration Technologies. Learning and Teaching." Springer International Publishing, 2018, pp. 492–504. [Online]. Available: https://doi.org/10.1007/978-3-319-91152-6_38

[9] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of ais automated identification system," in *Proceedings of the 30th annual computer security applications conference*, 2014, pp. 436–445.

[10] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge attack tool for cyber security assessments of maritime systems," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, no. 1, pp. 35–44, 2021. [Online]. Available: https://doi.org/10.12716/1001.15.01.02

[11] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin, "Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre," in *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, Oct. 2018. [Online]. Available: https://doi.org/10.1109/csnet.2018.8602669

[12] "Maritime cyber risk management in safety management systems," International Maritime Organization, MSC.428(98). [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[13] Z. Škrlec, Z. Bićanić, and J. Tadić, "Maritime cyber defense," in *6th International Maritime Science Conference (IMSC 2014)*, vol. 1, 2014, p. 19.

[14] O. Jacq, P. M. Laso, D. Brosset, J. Simonin, Y. Kermarrec, and M.-A. Giraud, "Maritime cyber situational awareness elaboration for unmanned vehicles," in *Maritime Situational Awareness Workshop*, 2019.

[15] E. Russo, G. Costa, G. Longo, A. Armando, and A. Merlo, "Lidite: a full-fledged and featherweight digital twin framework," 2022. [Online]. Available: https://arxiv.org/abs/2202.06954

[16] J. Packer, "Bridge command," accessed on 16/04/2022. [Online]. Available: https://www.bridgecommand.co.uk/

[17] "Opencpn chart plotter navigation," accessed on 17/04/2022. [Online]. Available: https://opencpn.org

[18] "Signal k," accessed on 17/04/2022. [Online]. Available: http://signalk.or

[19] "Suricata," Open Information Security Foundation (OISF), accessed on 17/04/2022. [Online]. Available: https://suricata.io/

[20] R. Ierusalimschy, L. H. de Figueiredo, and W. C. Filho, "Lua—an extensible extension language," *Software: Practice and Experience*, vol. 26, no. 6, pp. 635–652, Jun. 1996. [Online]. Available: https://doi.org/10.1002/(sici)1097-024x(199606)26:6⟨635::aid-spe26⟩3.0.co;2-p

[21] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation data anomaly analysis and detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022. [Online]. Available: https://doi.org/10.3390/info13030104

[22] "Splunk," Splunk Inc., accessed on 20/04/2022. [Online]. Available: https://www.splunk.com/

[23] "Opnsense," Deciso B.V., accessed on 20/04/2022. [Online]. Available: https://opnsense.org

[24] "Openwrt," accessed on 20/04/2022. [Online]. Available: https://openwrt.org/

[25] "Moodle," accessed on 20/04/2022. [Online]. Available: https://moodle.org/

[26] "Prometheus," accessed on 20/04/2022. [Online]. Available: https://prometheus.io/

[27] "Grafana," Grafana Labs, accessed on 20/04/2022. [Online]. Available: https://grafana.com/

[28] "Search reference," Splunk Inc., accessed on 20/04/2022. [Online]. Available: https://docs.splunk.com/Documentation/Splunk/latest/SearchReference

[29] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. PP, 12 2020.

[30] M. Vielberth, M. Glas, M. Dietz, S. Karagiannis, E. Magkos, and G. Pernul, "A digital twin-based cyber range for SOC analysts," in *Data and Applications Security and Privacy XXXV*. Springer International Publishing, 2021, pp. 293–311. [Online]. Available: https://doi.org/10.1007/978-3-030-81242-3_17

[31] M. Canepa, F. Ballini, D. Dalaklis, and S. Vakili, "Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain," *INTED2021 Proceedings*, 2021.

[32] Cyber-mar. [Online]. Available: https://www.cyber-mar.eu

[33] K. Tam, K. Moara-Nkwe, and K. D. Jones, "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training," vol. 3, p. 16–30, Jul. 2020. [Online]. Available: https://so04.tci-thaijo.org/index.php/MTR/article/view/241410