JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–9
https://doi.org/10.1093/cybsec/tyac001
Research paper

Research paper

Overcoming information-sharing challenges in cyber defence exercises

Agnė Brilingaitė [1,*,†], **Linas Bukauskas** [1,‡], **Aušrius Juozapavičius** [2,#] **and Eduardas Kutka** [1,$]

[1]Institute of Computer Science, Vilnius University, Didlaukio str. 47, LT-08303 Vilnius, Lithuania and [2]General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A., LT-10322 Vilnius, Lithuania

*Correspondence address. Didlaukio str. 47, LT-08303 Vilnius, Lithuania, Tel. no. +370 52195021, E-mail: agne.brilingaite@mif.vu.lt

†**Agnė Brilingaitė** holds a PhD in computer science from Aalborg University, Denmark. She is an associate professor at Vilnius University in the Institute of Computer Science. Her research interests focus on spatial data modelling, location-based services, cybersecurity training and education in computer science. She is involved in the process of quality assurance in studies at the university. She has been taking part in EU-funded projects related to the development of student-centred learning, teaching, assessment and internationalization. Currently, she leads EEA-funded project *Advancing human performance in cybersecurity*, ADVANCES.

‡**Linas Bukauskas** holds a PhD in computer science from Aalborg University, Denmark. He is an associate professor and head of Cybersecurity Laboratory in the Institute of Computer Science at Vilnius University. He is involved in teaching of cybersecurity-related courses, organizing hackathon, national cyber defence and tabletop exercises. His research interests include cybersecurity, data mining and natural language processing.

#**Aušrius Juozapavičius** holds a PhD in physics from KTH Royal Institute of Technology, Sweden. Currently, he is a professor responsible for the cybersecurity specialization of study programs at General Jonas Žemaitis Military Academy of Lithuania. His research interests are cybersecurity, computer modelling of semiconductor systems, flat semiconductor GaAs/AlGaAs structures, THz radiation antennas, and automobile traffic safety and optimization.

$**Eduardas Kutka** holds a Master's degree in computer science. He is also a network administrator who is involved in cyber defence exercises and development of virtual infrastructures for network security. He has been participating in EU-funded projects on HPC and cloud computing infrastructures. His research interests include network security and analytics, virtual infrastructures and vulnerability simulation.

Received 1 July 2021; revised 9 December 2021; accepted 7 January 2022

Abstract

Active usage of threat intelligence information supports effective prevention, mitigation and defence against cyberattacks by threat actors ranging from individual amateurs to state organizations. However, threat intelligence highly depends on security specialists' ability to share incident data on threat information-sharing platforms. Unfortunately, business managers and educational institutions undervalue the information-sharing aspect when planning the professional development of cybersecurity-related specialists. Consequently, cybersecurity specialists are insufficiently motivated to correctly communicate and propagate relevant information with team members, superiors, relevant institutions and the global community about the impact of the incident. Literature review reveals many technological, legal and psychological obstacles hindering successful information exchange. This research aims to improve threat information sharing by focusing on the educational aspect of the problem and analysing the attitude of cybersecurity specialists during cyber defence exercises (CDX). Our case study disclosed nine factors obstructing both proper reporting to relevant authorities and adequate communication among teams. By addressing these factors, CDX organizers could substantially improve the development of highly beneficial soft skills of the technical specialists.

Key words: cyber defence exercises, collaborative learning, informal information exchange, incident information sharing

Introduction

Cybersecurity (CS) incidents are costly and their numbers are constantly on the rise [1]. All sectors experience direct harmful consequences. Threat intelligence is a significant defence component [2], as it contains context, indicators of compromise (IoCs), implications and advised actions regarding identified and emerging possible threats. However, application of threat intelligence requires good quality data shared by other organizations and states. This aspect of information management is critical to ensure a timely and effective prevention, mitigation and defence against cyberattacks.

Governmental institutions and businesses can benefit from improved information sharing [3, 4]. Unfortunately, this exchange meets with many technical and psychological obstacles leading to a general lack of interest [5]. First, different classification schemes of the accidents exist, e.g. ATT&CK [6] or the famous Kill Chain by Lockheed Martin [7]. Second, each threat information-sharing platform is unique, and a user has to understand loosely defined parameters to process the data correctly. Moreover, both the sender and the recipient should have the same definitions to make use of the information at all [8]. Finally, the information should be trusted and preserve privacy. CS specialists need to learn how to overcome the challenges.

Complex nature of cyberattacks requires complex training methods, and cyber defence exercises (CDX) are commonly used to educate CS specialists in near real-life systems. Typical CDX are oriented towards IT specialists with technological skills who form Blue teams (BTs) to defend against the attacks executed by other experts (the Red Team, RT). Both the resilience against cyber threats and teamwork competence can be strengthened during CDX in fully controlled environments. CDX can be organized at the (inter)national level, within some sector of the critical infrastructure or as a part of an educational process at a higher education institution. Even though reporting and information-sharing (RIS) tasks are always an integral part of CDX, they have a low priority. The defence of systems and their service availability is the main component of CDX game rules. As a result, quality of shared or reported data is given insufficient attention, and the participants do not recognize the importance of sharing outside the game.

CS specialists should be encouraged and be responsible for active collaboration with their peers in their own or other organizations. Therefore, we investigate possible ways to foster the development of information-sharing skills during a CDX event. As the primary training audience are CS specialists with technical skills, the main research questions of our work are

(1) What is the attitude of the CDX training audience towards information sharing?
(2) What factors influence the quality of executed RIS tasks?

We performed a case study during two annual international live CDX events putting our focus on the development of soft skills in general, and information sharing in particular. Based on the findings, nine factors negatively impacting the attitude towards RIS tasks were defined and analysed.

The paper is structured as follows. 'Related work' highlights the importance and challenges of information sharing in the area of threat intelligence. The 'Methods' section covers the case study performed during two CDX events. The 'Results and discussion' section presents the findings of the case study. The paper ends up with 'Conclusions and future work'.

Related Work

Timely and relevant threat intelligence data could be helpful in a proactive defence of an organization by guiding it towards the identification of weak spots in the security of its infrastructure. It is very important to use tools in cooperation with human analysis to identify threats in data lakes generated by various internal and external sources [9]. Information exchange is a critical point [10] because the analysis would fail without aggregated good quality data shared by other organizations.

Common weaknesses enumeration [11] and National Vulnerability Database [12] are widely used by CS specialists. Vulnerability databases provide threat risk assessment and describe technical properties of exploits [9]. MITRE Corporation developed its ATT&CK Framework [6] to classify all known methods using vulnerabilities for exploitation. Exchange of collected intelligence information among organizations can use several existing standards, e.g. present information in the STIX format [13] or share it using the TAXII protocol [14]. Differences between the standards may be overcome, but many other obstacles affecting the information exchange between the organizations exist.

Rajamäki [15] covers challenges related to what to share, with whom to share, why to share, how to share, as well as architectures, methods and mechanisms of sharing. Schneider, Sedenberg and Mulligan [16] indicate that rational sharing should be used to promote CS. They agree that sharing information about vulnerabilities, best practices, threats, risks and ways to manage vulnerabilities and respond to threats is advantageous for every defender. It should be yet decided what public information-sharing activities could suit best at the international level.

Similarly, Koepke [17] defines various barriers of information sharing, and technological ones are only increasing, e.g. the lack of common language, the complexity of the information, difficult validation of data and vast amounts of data. She concludes that barriers are greater than incentives, and sharing of data increases with company size.

Information sharing is acknowledged as a big problem in the CS community by several researchers, practitioners and organizations. To foster information sharing, an open-source malware information-sharing platform (MISP) [18] was co-financed by the European Union. Wagner *et al.* [19] discuss cases of MISP usage and implementation. They emphasize that there is a possibility to record only the vital data in MISP, but it can be easily extended if additional information arises. Another important feature is information-sharing levels and the possibility to fine-tune taxonomies to fulfil the needs of differently organized communities. The MISP event synchronization protocol allows usage of pull, push and cherry-picking methods. Another initiative is described by Haass, Ahn and Grimmelmann [20] who provide a case study for information sharing within Arizona Cyber Threat Response Alliance, Inc. (ACTRA). The main goal of ACTRA is to improve response to CS events by empowering information sharing. Chantzios *et al.* [21] evaluate six different vulnerability reporting frameworks that could be used to share information among organizations. The frameworks were mainly evaluated based on expressiveness, flexibility, extensibility, automation and structuring.

Several threat intelligence sharing standards currently exist. An efficient exchange of threat information would benefit from a single data sharing format, and Menges, Sperl and Pernul [22] try to create a unified metamodel. This model is based upon the characteristics of the most popular existing threat information-sharing formats STIX, IODEF, VERIS and X-ARF. The exchange of information is not the

only problem. Even more significant challenges occur when specialists try to get actionable knowledge from their collected stockpile of data. Brown, Gommers, and Serrano [23] emphasize challenges when working with multiple intelligence sources such as normalization and consolidation of gathered information.

Threats should be addressed in different countries simultaneously, and this cannot be done without well-timed information sharing. ENISA [5, 24] emphasizes that local detection and information exchange of cyberattacks is not enough. Johnson *et al.* [25] indicate that shared information awareness, improved security posture and greater defence agility would result from consolidated cyber threat information resources. They notice that organizations do not always want to participate in information sharing because of various limitations. However, intercountry information sharing has obstacles related to legal issues, technical and procedural differences and problems, lack of trust and interest from engaged parties.

Ring [26] notices that sharing of information is problematic even within a big organization and not just among different organizations or countries. One of the big drawbacks of sharing is that everyone wants to get some positive feedback on their input. If there are no compliments then in most cases this voluntary sharing stops. Analysing the information is tedious but necessary work, especially when more individualized attacks are being prepared for each organization. Therefore, having more information is better for any organization as it provides additional possibilities to prevent attacks [25].

Privacy and anonymity is an important aspect of threat information sharing [27] because there might be a lot of negative aftereffects, e.g. disclosure of private infrastructure details, damage to reputation or problems with the law. Therefore, van de Kamp *et al.* [28] propose an implementation of cryptographic techniques for information sharing. Albakri, Boiten and De Lemos [29] identify a method to share cyber threat intelligence (CTI) under privacy laws like General Data Protection Regulation, GDPR. They suggest the traffic light protocol (TLP) to mark how sensitive data in CTI are. Multisite sharing with different access levels is already implemented in MISP [19], but Murdoch and Leaver [30] identified that many organizations have legal, trust and other issues when sharing data in various communities, both locally or externally.

The issue of trust is significant in cyber threat information exchange because CTI often contains private and sensitive data. Wagner *et al.* [31] analyse various threat intelligence platforms/providers and suggest a trust taxonomy of sharing sensitive data in the cyber community. Similarly, Burger *et al.* [32] present a layered taxonomy model based on the OSI ISO model. Using the model, they could decompose CTI ontologies to get more relevant information from data.

From a technical point of view, user experience in the threat information-sharing platform (TISP) was found to be very important for it to be used. Sander and Hailpern [33] noticed that automatically acquired and aggregated data usually is not as important as enriched data shared by other users. Additionally, they performed user profiling and deduced typical CS personas. Most users working in CS teams are young, and they are accustomed to user-friendly technologies and require working interfaces that are modern and intuitive to use. This information is very important to future TISP developers. The importance of IT tools in promoting knowledge exchange within an organization was also noticed by Qureshi *et al.* [34] who found that IT-mediated social interactions benefit to individuals with different IT backgrounds.

There is a consensus among the researchers about the importance of cyber threat information sharing. Unfortunately, it is hindered by many legal, technological and even psychological obstacles. Practitioners are addressing the technological part with various levels of success, and many state-level organizations are supporting the development of collaboration tools. Meanwhile, the human part of the human–machine equation can be addressed by using education, and the most intense learning events of CS specialists where theory is being implemented in practice are CS exercises.

Methods

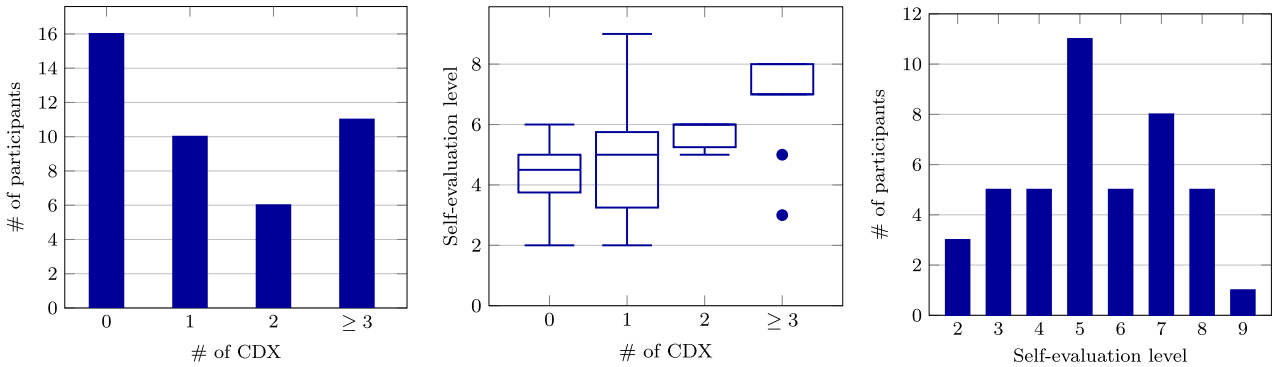
We carried out a case study of two live international CS exercises of 2018 and 2019 to determine the attitude of CS specialists regarding information sharing. The exercises were hybrid by their design: real-time technical defence of live systems had to be supplemented by proper reports to simulated legal authorities. One of the goals of the CDX was to foster interteam collaboration and communication skills. The primary training targets were junior CS specialists from the military and several critical infrastructure companies. They were grouped into several independent BTs to defend their simulated enterprise infrastructure against attacks of the RT. Identical cyber ranges were provided to all teams. The teams were not isolated, and they were encouraged to communicate with other teams and learn from one another. According to the game rules, each BT member chose one of several roles, including a reporting officer (reporter) and a threat hunter. The event was geared towards training, and scoring was provided for the teams for better estimation of their performance. The scoring was based on the availability of services, but it did not consider reporting activities.

Every BT was assigned an observer from the Evaluation team. The observers had to note how the internal team communication flows, how the reports about attacks are managed, and how their team interacts with others. The observers knew the exercise scenario, the cyber range layout and all planned attacks in advance. Additionally, the attacking RT recorded the time when their attacks started, when the BT reacted, and how well the BT performed. According to the scenario, the job of a defending team was not just to protect the organization. Additionally, they had to report to the management of the organization about the impact of attacks to the business. We received access to all the data including the BT reports.

Individual questionnaires before and after events were issued to participants to determine their level, strengths and attitudes as proposed by [35]. In 2019, expanded questionnaires were used to understand the distribution of skills in various areas relative to the overall self-evaluated competence level of a CS specialist. In particular, the research was focused on information-sharing and threat hunting skills.

Four and eight BTs participated in 2018 and 2019, respectively, and the average team size exceeded eight persons. According to the self-reported data in 2018, most of the BT members had little prior experience of similar exercises with 83% of the 24 BT respondents participating in CDX for the first or second time, and 58% of them rated their experience level as low. The next year CDX attracted more experienced participants, and 60% of the 43 respondents participated for the first (16 persons) or second (10 persons) time only (see Fig. 1a).

The self-reported level of competence on a scale from zero to 10 uniformly increases with the number of participated exercises (Fig. 1b). In 2019, the CDX gathered a group of specialists with their self-evaluated competence level distribution closely resembling the normal distribution curve with a slight weight on the lower end



(a) CDX experience (b) Competence level (c) Distribution based on the level

Figure 1: BT participants in 2019.

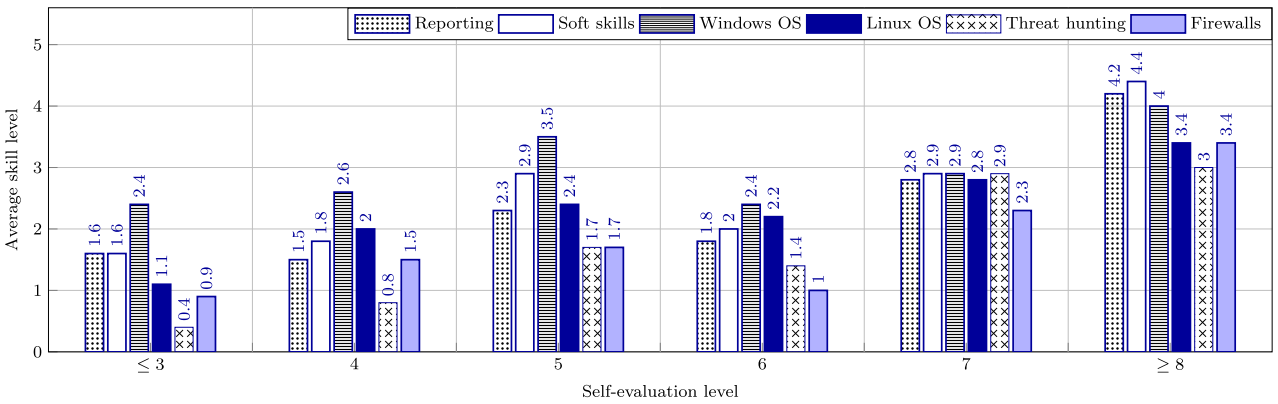
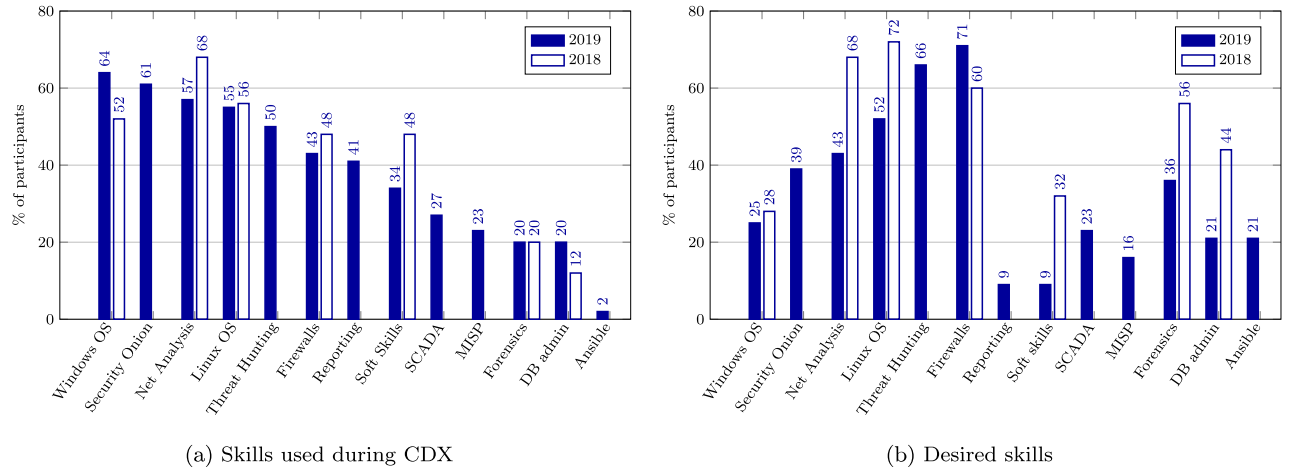


Figure 2: Average skills versus the self-evaluated competence level.

(Fig. 1c). However, the level of individual skills grows differently compared to the overall competence level (Fig. 2). Each skill was graded on an integer scale from 1 to 5. Windows OS skills dominate among the technical skills, while threat hunting and firewall skills start lowest and remain among the worst developed skills regardless of the overall skill level. The reporting and soft skills exhibited a unique skill development path. Up to level 7, the respondents reported average reporting skills without much change as their overall competence grew, and these skills were always higher than the other ones. Only specialists at or above level 8 demonstrated a sharp increase in reporting skills. The observers evaluated incident reports submitted by the participants during the exercises. They emphasized a low quality of RIS activities. Consequently, CDX participants overestimate their self-reported soft skills; only the most experienced professionals start understanding the importance and challenges of proper reporting.

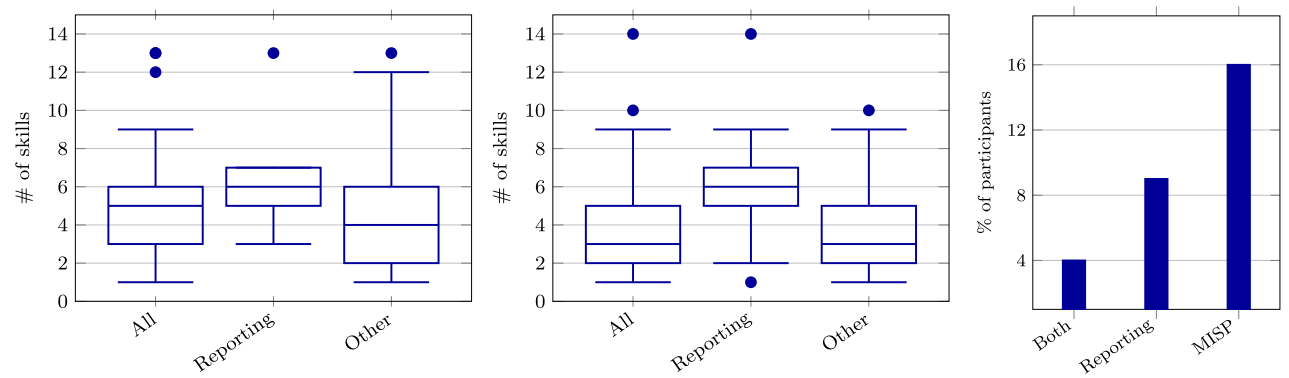
After the exercises in 2018 and 2019, the participants were asked to give feedback about the CDX. They had to specify the skills they used during the exercises (Fig. 3a) as well as point out the skills they desired to improve afterwards (Fig. 3b). In 2019, to support the objectives of the CDX, reporting and threat hunting skills were added to the questionnaire. The extended competence development framework [35] was partially implemented in 2019. A pre-training phase was introduced, and two specific tools were given significant attention via introductory lectures and hands-on tutorials before the live stage of the CDX—the threat hunting platform Security Onion and the information exchange platform MISP. Even though the exercises had a significantly different cyber range and scenario, the distribution of used skills depicted in Fig. 3a is almost identical in 2018 and 2019, except for the tools that were introduced in 2019. Most of the participants (close to 60%) needed to deal with Windows and Linux operating systems, perform network analysis and hunt for threats. About 40% of the participants claimed they were involved in reporting activities despite having a dedicated team member for reporting. This means many persons consider they are involved in reporting whenever they supply any piece of information to their colleague who is responsible for the reports. On the lower end, about 20% of the Blue team members used their forensics, database administration, and the newly acquired MISP skills. Despite the specially prepared hands-on classes about automation tools (Ansible), almost nobody used them during the exercises.

A question about the skills the participants desire to improve illustrates quite well the difficulties they encountered during the exercises (see Fig. 3b). Four main skills take the top position: firewall management, threat hunting, Linux OS and network analysis are the most in demand. On the other hand, just a few persons stated their desire to learn more about reporting and MISP in particular. The minority of the BT members who expressed their interest in learning more about reporting in general or MISP in particular (9 persons) also showed a distinctive attitude during the exercises. During the CDX, they claim to have used 6.2 different skills on average out of 13 choices in the questionnaire (see the Reporting box in Fig. 4a where the median



(a) Skills used during CDX (b) Desired skills

Figure 3: Used and desired skills of BT participants.



(a) Skills used during CDX (b) Desired skills (c) Number of participants

Figure 4: BT participants wishing to learn reporting and/or MISP.

value is 6). Their colleagues (Other) used only 4.5 skills, and the total average (All) was 4.8, while the median values were 4 and 5, respectively. The difference between the means is significant for 0.1 significance level according to the two-sample *t*-test. Similarly, these BT members also wanted to learn more than the others (Fig. 4b). Those who wanted to advance their reporting skills desired to study 6.2 skills on average, while others wanted to upgrade only 3.6 skills, and the total average was 4.1. In this case, the difference between the means is statistically significant for the 0.05 level. We can conclude that information sharers are more open-minded and knowledge hungry than their fellow CS specialists. The reporting officers should indeed be open-minded and flexible. Observation of their activities during the exercise showed a large number of systems they had to use simultaneously for a successful communication process (see Fig. 5).

First, they had to react to the requests sent by company users via a ticketing system (RTIR) whenever the users observed an attack or some system failure. The users were simulated by the Purple team (PT) members. RTIR was also used to communicate with the IT department (White team, WT) to receive approvals for any system changes the team wanted to make. Second, if the team confirmed an incident, the reporting officer had to compile an initial report and send it to the company IT management using a web-based form in a special collaboration-support system (Collab). If the management decided the incident was critical enough, the reporting officer would submit a long-version (final) report via the same Collab platform after the incident was resolved. Additionally, the reporting officer had to read and respond to CERT and IT department emails, interact with other teams using an instant messaging platform and support other team members who tried to use the MISP sharing platform. They could also visit fellow teams physically like any other team member.

Some of the teams had reporting officers who performed risk assessment and used MISP themselves to submit relevant IoCs. Regardless of the involvement level of the reporting officers, all reporting activities required sufficiently advanced technical knowledge. Unfortunately, the teams allocated the least knowledgeable or least technical persons to this role, as noted by the observers. This might be related to a rather small team size (around eight persons on average). The role of the reporter was assigned either to a person with a managerial background or to a novice, as it required more soft skills than hard ones. On the positive side, this created a possibility for persons with various educational backgrounds to enter the CS area. Even though the organizers encouraged the use of the MISP system, the teams focused most of their attention on the technical aspects of the defence and gave the lowest priority to the reporting activities. This, in turn, led to poor quality of most of the incident reports as evaluated by the organizers.

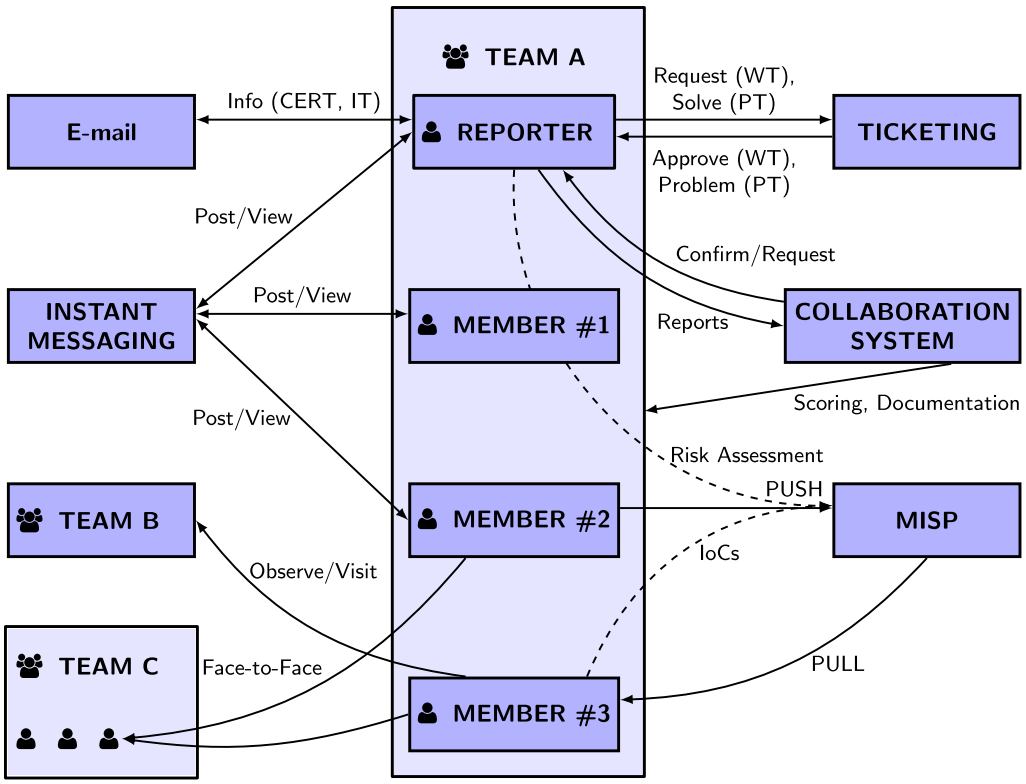


Figure 5: Communication flow from Team A perspective: actors, components, directions and operations.

Results and Discussion

Information-sharing activities constitute an integral part of the complex attack-defend-report picture during the hybrid CDX exercises. Based on our observations, nine factors can be distinguished as central pillars impeding the development of RIS-related skills and leading to poor results of a team in RIS tasks. The set of factors was derived from the qualitative assessment of observers assigned to each team. The observers consisted of experts from academia, industry and the national CERT.

Factors affecting information-sharing activities

Factor 1: a narrow focus on technical tasks

Teams assign a low priority to RIS tasks when hybrid CDX has an emphasis on technical defence and tactics. In this case, teams concentrate on active defence and allocate highly skilled participants to monitor the activities within the infrastructure of the cyber range. The role of the reporting officer is the least technical one and tech-savvy team members rarely desire it.

Due to the stress on the defence, the status on the scoring board depends on timely actions. The teams concentrate on technical mitigation tasks: changing firewall settings, searching for rogue devices on their network, updating group policies or recovering services. These competitive activities are more attractive and impressive to the participants than dealing with reporting documents and forms. As provided in the feedback, the participants liked technical tasks and challenges, and none mentioned reporting as an exciting activity. Overall, an availability-based scoring system does not support learning goals related to information sharing. In this case, technical people attribute reporting procedures to the category of soft skills and mistakenly consider them irrelevant.

Factor 2: required diverse technical skills

Even if reporting is treated as a nontechnical part of the CDX, very diverse technical skills are required to finish RIS tasks successfully. The reporter has to communicate with all members to gather required information components. For example, in the case of a SQL injection, a database administrator, a Linux administrator and firewall specialists can provide different pieces of the puzzle. To build a comprehensive picture of the attack and explain it professionally, the reporter has to understand the low-level details of its artefacts and the high-level impact on the infrastructure. Therefore, the reporter should have the necessary skills to manipulate technical terms and communicate with colleagues efficiently and independently. At the same time, the team members are focused on the system recovery or active defence and cannot supervise the reporter through the RIS tasks.

Factor 3: no common vocabulary and taxonomy

During the CDX event, it is assumed in advance that all participants use the same vocabulary and are aware of the taxonomy related to the attack description and evaluation. Usually, the introduction into the terminology is skipped and not stated explicitly, although some documentation and procedures are provided as a part of game rules.

Still, if the reporter or other members of the team do not perform reporting in their everyday activities, the vocabulary and taxonomy might be ambiguous due to the lack of time to analyse provided documentation and recommendations in more detail. For example, a message *cannot access the server* in the report might be interpreted in several ways, e.g. the web service is down, a DDoS attack is in progress, an incorrect URL was used or incorrect credentials were provided.

Factor 4: fragmented knowledge of legal documents

CDX rules may require to know many legal documents related to reporting procedures [36]. At the national level, CERT provides procedures on timely reporting and risk evaluation of cyber incidents, e.g. EU countries integrate ENISA recommendations based on the national CS strategy. However, different countries can have distinct CERT templates. Therefore, the organizers of the international CDX adapt or compile existing forms into the CDX form based on the event goals. Also, an organizational workflow is simulated during the event, and specific internal procedures are defined. Therefore, CDX participants need additional training on report form structure and filling requirements. Otherwise, they apply pre-event knowledge and assumptions based on their experience while interpreting the provided material. The problem is recognized in the recent proposal for changes in the Network and information systems directive by the European Commission [37], where a particular emphasis is placed on the harmonization of incident reporting requirements. Common reporting standards and their real-world applicability would encourage the CDX participants to learn and use them.

Factor 5: missing knowledge of data exchange standards

There exist data exchange standards and protocols related to threat hunting. They can be used during the CDX by integrating threat information-sharing platforms into the game play. As a rule, participants lack knowledge about any of the existing standards and their specific features. Acquaintance with the information-sharing standards would help them to structure pieces of data and eliminate common reporting errors, e.g. avoid an intermix of numeric and text data in the same form field.

Knowledge of data exchange standards covers abilities to share threat intelligence and/or integrate exported data into the threat hunting systems, intrusion detection or prevention systems, or security information and event management systems. A lack of these skills may lead to a delayed or missed utilization of threat intelligence data, as observed during the CDX events.

Factor 6: unfamiliarity with information-sharing platforms

During the CDX event, information sharing is implemented using information-sharing platforms and communication tools. Information-sharing platforms are information systems that support a set of customizable functionalities, and these platforms could be individualized, adapted or installed as-is from open repositories or provided by a vendor. Also, platforms can be specifically developed for a particular CDX type or event. At least some of the participants would use the system for the first time, and they would be unfamiliar with the functionality of the provided information-sharing system. The inability to use the system correctly leads to skipped/unfinished tasks and insufficient information about the attacks in the event descriptions. The participants are inclined to use instant messaging platforms or any chat-like system instead of trying to master the specific platform.

Any information system has its usability issues and friendliness level from the perspective of human-computer interaction. It is not enough to provide the system without any training. In the feedback, participants suggested providing specialized MISP training. For example, the MISP system requires several steps and states to publish an attack with its metadata [38]. However, its graphical user interface options and the usual workflow are not self-explanatory. Research shows that the platform is technical oriented, the learning curve is steep and beginners might face challenges using it [39]. However, human aspects and behaviour in MISP have not been sufficiently explored [40].

Factor 7: a variety/excess of communication channels

During the on-site CDX event, organizers establish many communication channels to simulate information flows of an enterprise. As a rule, an email would be used to send the scenario information for the team, such as information about a supposed accident within the critical infrastructure, or the ticketing system is used to simulate IT support within an organization. In a business environment, many different persons are responsible for different communication channels, while only one or two persons per team are responsible for managing all of them during the CDX.

During the CDX, the primary responsibility of the reporter is to ensure the communication, and each communication channel and platform provides a piece of the puzzle. However, the reporter is overloaded with multitasking, e.g. checking for updates and informing the team. Each channel has a different response time, e.g. information-sharing platforms require manual browsing unless organizers support automatic notification about registered events. Excess of communication channels prevents teams from receiving timely, structured, relevant, correct and high-quality information needed to accelerate learning and resolve attacks faster.

Factor 8: team size

Team size influences the effectiveness of RIS tasks. When the team is too small (up to 6–8 members) participants have overlapping roles, i.e. one team member covers responsibilities of several roles. For example, a team leader mostly organizes the work and distributes tasks, but she might also be involved in the analysis of audit logs. Participants have to concentrate on several infrastructure systems and monitoring tools. Shifting from one system or task to another one makes work more stressful. If the reporter has another role, reporting is postponed for a later time. If the reporter has only one role, she has to interrupt the work of colleagues to gather all the extensive details needed for the reports.

Large teams (above 15 members) have roles and responsibilities more separated. However, larger teams make data gathering more complicated for the reporter as more team members have to be contacted for the artefacts of the attack to construct a set of IoCs. Further research might reveal the optimal team size for different setups of CDX.

Factor 9: blurred benefits of skills outside the exercises

Participants of the CDX event consider RIS activities and corresponding skills as having only local importance with little value outside the event, especially when reporting forms and procedures are unique for the game. In that case, it takes time to adapt to the new RIS requirements while disregarding prior real-life experience, and reporting literacy does not look like a transferable skill easily applied in everyday position and future career.

Indeed, the information-sharing and reporting skills attained during CDX are never considered to be the primary goal of the participants. It is the responsibility of the organizers to elucidate the real value of these skills both on a personal and a global level. In fact, our observations show that it is beneficial for each specialist to have a report-oriented mindset. Then instead of just alerting their teammates about a nonresponsive service they would be inclined to get a better look first and send a more informative message with timestamps and IoCs. This minimal effort makes the alerts actionable to other team members, puts the specialist on the right track, and reduces both the clutter in the information exchange channel and the attack mitigation time. On a higher level, even though national legal documents and international recommendations are not fully covered during the CDX, nevertheless the RIS activities involve common at-

tributes and steps used in real-life situations, e.g. IoCs, attribution, various Kill Chain phases and risk assessment. The assessment scale and organizational procedures might be different, but the exercises provide a possibility to develop the competence of adapting to a new situation, applying new requirements and reviewing existing legal documents.

Information sharing in CS curricula

According to our data, CDX participants prioritize their technical skills over their soft skills. We made a brief analysis of the most famous ACM CS curriculum [41] and NIST NICE workforce requirements [42] to see whether the attitude is reflected there as well. The NICE framework does not define a reporting officer role explicitly. The NICE workforce framework assigns the responsibility to establish and coordinate reporting to the managerial level roles (All Source-Collection Requirements Manager and Communications Security Manager in particular). It is understandable because they have to aggregate reports coming from many different sources—threat hunters, analysts and system administrators, and act as intermediaries between higher management, all the reporting IT specialists, and external organisztions. On the other hand, the ability to gather, collect, analyse and share the information is included in the description of many other roles—most notably analysts, but also various other specialists, e.g. All-Source Analyst or Defence Forensics Analyst. In total, 23 out of 52 roles defined in the NICE framework have an explicit requirement to have either knowledge or skills to perform information reporting or information dissemination tasks. Additionally, NICE is reintroducing a concept of CS competencies [43]. One of the four proposed categories of competencies covers soft skills and effective communication in particular. According to the proposal, they are called professional skills needed for each person's employability.

Similarly, the ACM cybersecurity curriculum, prepared by a multinational team [41], describes the essential knowledge each CS professional should have. It lists eight broad areas of knowledge in total. The Organizational Security area includes the requirement to understand the principles of collection, analysis and dissemination of security information. The topics dealing with information sharing combine the requirements for technical as well as soft skills. The soft skills part is emphasized in the curriculum stating that 'delivering information to executives and external decision-makers is a critical skill for information security leaders', and the ability to make presentations or give meaningful feedback is essential in the career of a CS specialist.

Overall, information-sharing and reporting skills are an integral part of all skills and abilities a CS specialist should have. In many ways, they stand as a bridge between the technical and nontechnical world. Proper reporting skills may help the specialists to resolve the incidents faster by providing relevant information to their colleagues and by attracting sufficient attention and resources from often nontechnical managers.

Stimulation of attitude towards information sharing

It is essential to stimulate a positive attitude towards RIS activities and demonstrate the strategic value of related skills. The gained practice and competences would benefit the global community and the personal portfolio of a CS specialist. We noticed that the assignment of an experienced technical person to RIS tasks is treated as a sacrifice from the team's perspective. Moreover, the nine listed factors are the reason for the situation.

Conclusions and Future Work

The CS community raises initiatives to foster information sharing and overcome existing technical obstacles by creating common sharing standards and open platforms. We focus on the educational aspect and address the attitude of CS specialists towards reporting and information-sharing tasks during live CS defence exercises. The results of the case study revealed nine significant factors negatively impacting prioritization and execution of RIS tasks due to overly focused attention on technical tasks, insufficient knowledge of information-sharing importance, standards and tools, and unclear benefits of these skills. Organizers of CDX should consider these factors during all exercise phases if RIS-related objectives are defined among the CDX goals. The findings show the need to pay special attention to explicit integration of RIS tasks in the scenario and assessment in CDX-based training.

Future research could be devoted to the development of automatic analysis of RIS artefacts to evaluate the quality of the shared information. Also, future studies could investigate aspects of environments that combine communication channels and other CDX platforms in a specialized dashboard to simplify communication and ease the work of information-sharing specialists.

Acknowledgements

The authors of the paper would like to express their gratitude to the organizers, participants and the evaluation team of the international cybersecurity exercises Amber Mist 2018–2020 for the opportunity to gather the data.

Supplementary Data

Supplementary data is available at *Cybersecurity Journal* online.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author contributions statement

A.B.: conceptualization, related work, data analysis, investigation, methodology, results and discussion, and writing. L.B.: conceptualization, investigation, methodology, results and discussion, and writing. A.J.: conceptualization, data analysis, investigation and writing. E.K.: related work, software, investigation and writing.

References

1. Check Point. Cyber Security Report. 2020.
2. Shin B, Lowry PB. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Comput Secur* 2020;**92**:101761.
3. Cui R, Allon G, Bassamboo A. *et al.*. Information sharing in supply chains: an empirical and theoretical valuation. *Manag Sci* 2015;**61**:2803–24.
4. Scott ED. *Police Information Sharing: All-Crimes Approach to Homeland Security*. LFB Scholarly Pub. 2009.
5. European Union Agency for Network and Information Security (ENISA). Detect, share, protect: solutions for improving threat data exchange among CERTs. 2013.
6. MITRE Corporation. MITRE ATT&CK®. 2020.

7. Hutchins EM, Cloppert MJ, Amin RM. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. 2011. Lockheed Martin Corporation. White paper.
8. Beynon-Davies P, Wang Y. Deconstructing information sharing. *J Assoc Inf Syst* 2019;**20**:476–98.
9. Pokorny Z (ed). *The Threat Intelligence Handbook: Moving Toward a Security Intelligence Program*. 2nd edn. CyberEdge Group, 2019.
10. Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. *Comput Secur* 2016;**60**:154–76.
11. MITRE Corporation. CWE: common weaknesses enumeration. 2020.
12. National Institute of Standards and Technology. National vulnerability database. 2020.
13. Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (STIX™). Technical report, The MITRE Corporation, 2014.
14. Connolly J, Davidson M, Schmidt C. The trusted automated eXchange of indicator information (TAXII™). Technical report, The MITRE Corporation, 2014.
15. Rajamäki J. ECHO information sharing models. European network of cybersecurity centres and competence Hub for innovation and operations, research and innovation action, European Commission. 2019.
16. Schneider FB, Sedenberg EM, Mulligan DK. Public cybersecurity and rationalizing information sharing. In: *Opinion Piece for the International Risk Governance Center (IRGC)*. Lausanne: IRGC, 2016.
17. Koepke P. Cybersecurity Information sharing incentives and barriers. Working paper cisl# 2017-13, Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, MIT, 2017.
18. MISP Project. MISP: open source threat intelligence platform & open standards for threat information sharing. 2019. (1 July 2021, date last accessed). https://www.misp-project.org
19. Wagner C, Dulaunoy A, Wagener G. *et al.*. MISP: the design and implementation of a collaborative threat intelligence sharing platform. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS*, 2016. p. 49–56.
20. Haass JC, Ahn G, Grimmelmann F. ACTRA: a case study for threat information sharing. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, WISCS, 2015. p. 23–6.
21. Chantzios T, Koloveas P, Skiadopoulos S. *et al.*. The quest for the appropriate cyber-threat intelligence sharing platform. In: *Proceedings of the 8th International Conference on Data Science, Technology and Applications, DATA*, 2019. p. 369–76.
22. Menges F, Sperl C, Pernul G. Unifying cyber threat intelligence. In: Gritzalis S, Weippl ER, Katsikas SK, Anderst-Kotsis G, Tjoa AM, Khalil I (eds). *Trust, Privacy and Security in Digital Business - 16th International Conference, TrustBus, Proceedings, volume 11711 of Lecture Notes in Computer Science Springer*; 2019. p. 161–75.
23. Brown S, Gommers J, Serrano O. From cyber security information sharing to threat management. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, WISCS, 2015. p. 43–9.
24. European Union Agency for Network and Information Security (ENISA). Report on cyber security information sharing in the energy sector. 2016. (1 July 2021, date last accessed). https://www.enisa.europa.eu/publications/information-sharing-in-the-energy-sector
25. Johnson C, Badger L, Waltermire D. *et al.* NIST special publication 800-150: guide to cyber threat information sharing. Technical report, NIST, 2016.
26. Ring T. Threat intelligence: why people don't share. *Comput Fraud Secur* 2014;**2014**:5–9.
27. Nweke LO, Wolthusen SD. Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In: *12th International Conference on Cyber Conflict, CyCon IEEE*, 2020. p. 63–78.
28. van de Kamp T, Peter A, Everts MH. *et al.*. Private sharing of IOCs and sightings. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS*, 2016. p. 35–38.
29. Albakri A, Boiten EA, Lemos RD. Sharing cyber threat intelligence under the general data protection regulation. In: *Privacy Technologies and Policy - 7th Annual Privacy Forum, APF*, 2019. p. 28–41.
30. Murdoch S, Leaver N. Anonymity vs. trust in cyber-security collaboration. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, WISCS, 2015. p. 27–9.
31. Wagner TD, Palomar E, Mahbub K. *et al.*. A novel trust taxonomy for shared cyber threat intelligence. *Secur Commun Netw* 2018;**2018**:9634507:1–11.
32. Burger EW, Goodman MD, Kampanakis P. *et al.*. Taxonomy model for cyber threat intelligence information exchange technologies. In: *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, WISCS, 2014. p. 51–60.
33. Sander T, Hailpern JM. UX aspects of threat information sharing platforms: an examination & lessons learned using personas. In: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, WISCS, 2015. p. 51–9.
34. Qureshi I, Fang Y, Haggerty N. *et al.*. IT-mediated social interactions and knowledge sharing: role of competence-based trust and background heterogeneity. *Inf Syst J* 2018;**28**:929–55.
35. Brilingaitė A, Bukauskas L, Juozapavičius A. A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput Secur* 2020;**88**:101607.
36. Harašta J. What LEGAD needs to know? Analysis of AARs from locked shields (2012–2018). In: *Proceedings of the 19th European Conference on Cyber Warfare and Security*, ECCWS Academic Conferences and Publishing International Limited, 2020. p. 136–42.
37. European Commission. Proposal for a directive of the European parliament and of the council on measures for high common level of cybersecurity across the Union. 2020.
38. MISP User Guide. Using the system: user guide of MISP malware information sharing platform, a threat sharing platform. 2020. (1 July 2021, date last accessed). https://www.circl.lu/doc/misp/using-the-system
39. Stojkovski B, Lenzini G, Koenig V. *et al.*. What's in a cyber threat intelligence sharing platform?: A mixed-methods user experience investigation of MISP. In: *Annual Computer Security Applications Conference (ACSAC'21) ACM*, 2021.
40. Stojkovski B, Lenzini G. A workflow and toolchain proposal for analyzing users' perceptions in cyber threat intelligence sharing platforms. In: *IEEE International Conference on Cyber Security and Resilience*, CSR IEEE, 2021. p. 324–30.
41. Joint Task Force on Cybersecurity Education. Cybersecurity curricula 2017: curriculum guidelines for post-secondary degree programs in cybersecurity. Technical report, ACM/IEEE/AIS-SIGSEC/IFIP WG 11.8; New York, NY, USA, 2017.
42. Newhouse W, Keith S, Scribner B. *et al.*. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Spec Publ* 2017;**800-181**:144.
43. Wetzel KA. NICE framework competencies: assessing learners for cybersecurity work. NIST Internal Report 2021,p. 18.