CRATE Exercise Control – A cyber defense exercise management and support tool

1st Jonas Almroth
Department of C4ISR
Swedish Defence Research Agency
Linköping, Sweden
jonas.almroth@foi.se

2nd Tommy Gustafsson
Department of C4ISR
Swedish Defence Research Agency
Linköping, Sweden
tommy.gustafsson@foi.se

***Abstract*—The growing dependency on computerized systems in society causes an increased need for a high level of cyber security competence among the professionals tasked with operating and protecting such systems. Cyber defense exercises are important for experience-based learning to train professionals working with critical computer systems. However, arranging realistic exercises require skilled instructors and technicians with the right set of tools. In this paper, we describe an exercise management and support tool called CRATE Exercise Control (CEC). The tool was developed by the Swedish Defence Research Agency (FOI), based on empirical experiences from arranging cyber defense exercises in the cyber range CRATE (Cyber Range And Training Environment), and best practices published by other organizations. We also share experiences made while using CEC during cyber defense exercises, as well as recommendations to consider when designing exercise management and support tools.**

1. Introduction

Society has become increasingly dependent on different types of computerized systems to provide fast and easy access to information and to manage industrial processes. Thus, not only everyday business operation, but critical infrastructure such as energy production, health care, banking, telecom and transportation are all depending on the robustness and security of these systems. As the value that can be gained by compromising critical systems increase, so does the number and complexity of the threats against them.

To counter these threats, it is important to continuously train the people working with computerized systems so that they can ensure that the systems are resilient against cyber threats [1, 2]. Training methods include lectures, lab sessions and more interactive activities such as exercises [3]. The main advantage of using exercises for training is the possibility to achieve an enhanced learning by creating a story-living experience as described by Perla and McGrady [4].

However, arranging cyber security exercises can be challenging even for experienced organizations. To facilitate the process, several organizations have published handbooks on the topic, including the European Union Agency for Cybersecurity (ENISA) [2], the Swedish Defence University (FHS) [1] and the MITRE Corporation [5].

Joonsoo, Youngjae, and Moonsu [6] describe how the exercise management team, referred to as the white team, operates during the exercise Cyber Conflict Exercise. Their description can be used to get an understanding of the management and support tools needed during the exercise execution phase. The paper describes a set of tools that check system availability and deduct score for system downtime. These tools also enable the white team to adjust the training environments by running exploits and providing the training teams with situational awareness [6]. A set of tools for achieving situational awareness is also described by Melón, Väisänen, and Pihelgas [7]. The tools are called EVE and ADAM, and are publicly available.

Kokkonen and Puuska [8] describe a study of inter-team communication during a cyber security exercise and experiences made using a specially developed tool to support reporting during the exercise. The tool was evaluated during an exercise and one of the conclusions was that a reporting system of some kind is required to monitor the progress of the training teams during an exercise. A similar reporting functionality as described by [8] is included in CEC. Marshall [9] presents the tool CyberSMART that can be used for scenario modelling and reporting [9] and Pihelgas [10] describes a tool based on Nagios Core that is used to score system availability.

Abbott et al. [11] describe the importance of automated performance assessment and their paper includes a brief description of a tool used during the Tracer FIRE exercise [11]. Yamin, Katt, and Gkioulos [12] present the results of a literature review of tools used in different cyber ranges and security test beds, listing a plethora of publicly available tools mainly used during the execution phase [12]. NATO has developed the Joint Exercise Management Module (JEMM) that is used for computer aided exercises (CAXs) and is described by Cayirci [13]. Even though the basic concept of CAX differs from the cyber defense exercise (CDX), there are similarities in the planning and evaluation phases.

In this paper, we present the exercise management and support tool CEC, designed to facilitate planning, execution and evaluation of cyber defense exercises. We also describe experiences made by operational use of this tool and how it may be improved in the future. CEC is one of the tools available in CRATE, a cyber range

DOI 10.1109/EuroS&PW51379.2020.00013

operated by FOI. CEC has been used in a majority of the cyber defense exercises hosted by FOI since 2015, such as the larger exercises iPilot [14] and SAFE Cyber [15], comprising 4-6 blue teams with 6-8 members each. The tool has also been used during approximately ten smaller exercises, run as an incident handling course, comprising two blue teams with 8 members each. The source code of CEC has not been made public, but this may change in the future as the tool matures.

This paper is organized into seven sections. Section 2 provides an overview of different types of cyber security exercises. Section 3 contains descriptions of the activities involved in running a cyber defense exercise and the different roles of the participants. Section 4 describes the life cycle of the cyber defense exercise, the information flow during the execution phase and the challenges that the arranging organization face. Section 5 describes the CEC tool. Section 6 describes experiences made using CEC during cyber defense exercises and includes an evaluation of how the tool addresses the challenges presented in section 4. Section 7 presents future work.

2. Cyber security exercises

The concept of cyber security exercises includes several different exercise formats. The table-top exercise (TTX) [1] and computer aided exercise (CAX) [16] are mainly used to train decision-making, while the capture the flag (CTF) and cyber defense exercise (CDX) [3] are mainly used to train technical skills.

The TTX is a discussion-based exercise where the dialogue between the participants is used as a mechanism to facilitate understanding, identify strengths and improvements as well as validate plans and procedures [17]. As such, a TTX may be run without any computerized support. A CAX meanwhile, utilize computer support to simulate a scenario where the participants are able to generate, move and manage physical entities in a simulated environment [16].

The CTF is an exercise format where the participants score points by solving different problems (referred to as flags) [18]. The size and complexity of the problems vary, from extracting information hidden in a downloaded file to penetrating entire IT environments and compromising protected systems. The problems to be solved during a CTF tend to be focused on utilizing weaknesses in different system or technologies. Because of this, Vykopal et al. [3] describe CTFs as a way to learn adversarial thinking, which is relevant to foresee future offensive actions. CTFs are also often arranged as competitions between the participants, making them a suitable exercise format to measure individual or team capabilities.

In a CDX, one or more teams are trying to protect a training environment against attacks. Scheduled attacks and other scenario objectives are often referred to as injects. In exercises arranged by FOI, the training environment is a virtualized representation of typical real world systems. Common objectives of a CDX includes training the participants, evaluating team performance, enhancing co-operation and testing tools or methods [1]. Scoring is sometimes used to measure team performance, but the competitive elements are generally more toned down during CDX events than during a CTF event. Vykopal et al. [3] describe CDXs as a way to achieve an experience-based knowledge focused at countering threats.

As the CEC tool is designed to support CDXs, this paper will henceforth focus on this exercise type.

3. Cyber defense exercise organization

The participants in a cyber defense exercise are often assigned to teams with specific functions. The roles of the different teams can be identified by specific colors [1]. This practice facilitates describing the role of each team during an exercise, since the meaning of each color has become common knowledge within the cyber training community. During larger events, such as Locked shields, the team members will even wear shirts in their team color, enabling them to be quickly identified during the execution phase [19]. Seker and Ozbenli [20] describe the colors commonly used as blue for the defending team(s), red for the attacking team(s), white for the exercise management team, green for the exercise environment support team and yellow for the team providing situational awareness.

In the exercises conducted by FOI, members of blue teams are often the participants being trained, and the number of blue teams vary depending on the scope of the exercise. Their activities include, but are not limited to, monitoring system availability, detecting vulnerabilities, indicators of compromise and malicious activities, managing incident response and performing scenario tasks.

The red team may also be subject to training, but based on the sources reviewed while writing this paper, it is more often scripted and part of the arranging teams. There may be more than one red team, working with different objectives and methods based on the exercise scope and scenario. Since the red and blue teams are the most predominant during the execution of a CDX, the exercise format is sometimes called *Red team/Blue team exercise* [21].

The white team is responsible for organizing the exercise, for planning and directing the event, executing injects, manual scoring and exercise evaluation. The green team manages the physical and logical infrastructure of the exercise and solves the technical issues that may arise during the event. The yellow team provides situational awareness for the other teams. Their main input to accomplish this is reports from the blue and red teams as well as monitoring of the training environment.

In the smaller exercises hosted by FOI, a single exercise management team exists beside the blue teams. Its individual members have one or more roles corresponding to white, yellow, green and red team functions.

4. Cyber defense exercise life cycle

This section describes the life cycle of a CDX, divided into three phases. In the end of each subsection, challenges specific to each phase are described. These challenges can be translated into basic requirements to be addressed by an exercise management and support tool.

The activities performed when arranging a CDX have been the topic of several handbooks and papers in the recent decade. Patriciu and Furtuna [22] focus on the

design of the exercise and describe the activities involved as the steps *objectives*, *approach*, *topology*, *scenario*, *rules*, *metrics* and *lessons learned* [22]. ENISA presents a CDX life cycle with several of the activities grouped into the segments *identifying*, *planning*, *conducting* and *evaluating* [2]. FHS describes the activities as a process involving the phases *planning*, *practical preparations*, *implementation* and *evaluation* [1]. The MITRE Corporation divides activities into the phases *exercise planning*, *exercise execution* and *post exercise* [5] and Vykopal et al. [3] present a cyber exercise life cycle including the phases *preparation*, *dry run*, *execution*, *evaluation* and *repetition*. Seker and Ozbenli [20] describe three stages including *planning*, *execution* and *evaluation*, where the planning phase includes the dry run described by Vykopal et al. [3]. In this paper, we will henceforth use planning, execution and evaluation as a base for further describing the activities and challenges involved in arranging a CDX.

4.1. Planning Phase

At FOI, the planning phase begins with a dialogue with the organization subject to training to establish the scope of the exercise, including identifying participants subject to training, learning objectives and duration of the event. Based on this, an exercise scenario, a training environment and injects are developed. Elements from previous CDX events are reused when possible, as described by both ENISA [2] and Vykopal et al. [3]. The planning phase ends with a test run of the exercise, which is an important activity to verify that everything works as planned [3, 20].

When FOI arranges a CDX, the planning phase normally involves intense work by the white, green and red teams. The planning phase usually stretches 2-6 months, depending on the size of the exercise with regards to number of teams, number of injects, complexity of the training environment and exercise length. The white team ensures that the exercise scenario and set-up match the prior knowledge of the participants and that the learning objectives can be achieved. The green team is responsible for building a training environment that supports the requirements of the exercise specification. If the red team is not one of the teams being trained, it is assigned to prepare the injects containing attacks.

The challenges in the planning phase that a cyber defense exercise management and support tool must address include the ability to support multiple users and teams, that a shared library of injects is included and that there is a scheduler for the injects. To provide a shared view, the data should be immediately available for everyone involved in the planning. Exercise components such as injects and training environments should be defined in a reusable manner to ensure that components used in previous exercises are easy to locate. The tool should compile a visual, shared timeline of the exercise activities.

4.2. Execution Phase

Execution is the first phase that involves the participants from the teams being subject to training, normally the blue teams. The execution phase often begins with some kind of familiarization activity as described by ENISA [2] and Vykopal et al. [3] to allow the participants to better understand the scope of the exercise, the tools and training environment used. This approach has also been taken during exercises arranged by FOI, where ample time is spent teaching the participants the tools, the training environment and running a simple pre-exercise scenario.

Once the actual exercise begins, it is important for the white team to pace the injects in relation to the scenario and the progress of the blue teams to achieve the desired learning objectives. Therefore, it is imperative that the white team achieves a good situational awareness of how the exercise scenario is played out. The situational awareness is provided by the yellow team and is achieved by the observation of the blue teams' activities during the exercise. This process is described by ENISA [2] and the MITRE Corporation [5] in their exercise handbooks, as well as by Vykopal et al. [3] and Seker and Ozbenli [20] in their papers. Seker and Ozbenli [20] also point out that it is important that each inject is performed in the same manner against all the participating teams. Otherwise, it won't be possible to compare the performance of the participating teams.

During the execution phase, the green team shifts focus from building the training environments to maintaining system availability and giving user support to the participating teams. If a system in the training environment or a system supporting the exercise execution becomes unavailable, the green team may need to work together with the white team to adjust the exercise so that the participants are affected as little as possible.

The primary challenge posed during the execution phase that needs to be addressed by a tool is to present information to allow for a good situational awareness. This especially aids the white team when assessing how each of the training teams is performing in accordance with the established learning objectives, enabling the white team to guide struggling teams. A tool should also collect reports from the blue teams and store the data in a way that enables it to be easily presented by the instructors during the evaluation phase. This includes the documentation of technical issues handled by the green team, the timeline of the events and details about the attacks carried out by the red team.

4.2.1. Information flow during the execution phase.

To achieve the sought-after situational awareness needed during the exercise execution, it is important to analyse the information flow during this phase prior to designing a tool. This analysis was performed by FOI prior to the initial design of CEC version 1 back in 2015. A similar activity is also described by Kokkonen and Puuska [8]. In addition to the information flow analysis, it is also necessary to ensure that adequate data is collected during the execution phase of the exercise to enable the after-action debriefing during the evaluation phase. FOI normally executes CDX events where the white, green and red teams collaborate, which affect the information flow. Figure 1 provides an overview of the information flow during a typical CDX arranged by FOI.

The outer gray box indicates the scope to be supported by the tool. The inner gray box indicates the training environment in the cyber range. The white team exchanges information about technical issues with the green and blue

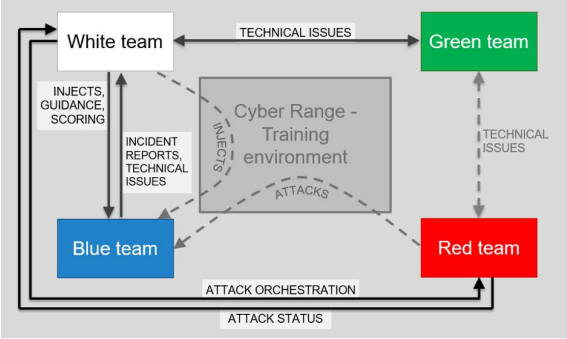

Figure 1. Information flow

teams. The latter flow may include additional instructions to the blue teams if needed. Information about technical issues can also be exchanged between the green and the red teams. The white team communicates injects to the blue teams, either as direct instructions or via in-game channels such as news sites in the training environment. The red team performs attacks against the blue team environments via the training environment in the cyber range. The blue teams will supply incident reports to the white team, enabling the white team to follow how each team progress during the exercise. When needed, the white team should be able to offer guidance to the blue teams. The white team should also be able to orchestrate the attacks that are carried out against each blue team. The guidance and the attack orchestration are important to ensure that the learning objectives can be fulfilled by each blue team. When a blue team finishes an incident report, the white team should be able to score the incident based on the report.

4.3. Evaluation Phase

After finishing the execution phase, it is important to conduct a proper evaluation of the exercise. The importance of exercise evaluations is emphasized in the handbooks published by ENISA [2], FHS [1] and the MITRE Corporation [5], as well as in the papers published by Vykopal et al. [3] and Seker and Ozbenli [20]. Based on these descriptions, the evaluation phase can be divided into two main activities. First, there is the *after-action debriefing* that involves all the participating teams and takes place immediately after the execution phase ends. The second activity is the *follow-up analysis* which is performed by the arranging teams after the exercise.

During the after-action debriefing, the exercise execution phase is revisited and the most important events are analysed. The after-action debriefing should reconnect to the learning objectives identified in the planning phase and is central for the blue teams' learning process [1, 2]. Vykopal et al. [3] describe how the debriefing is particularly important for the participants that have struggled to keep up with the events during the exercise. The debriefing involves the blue teams being trained, the white team describing the events and the red team describing the injects containing attacks. The green team may also contribute by providing technical details about the training environment.

The follow-up analysis covers the planning phase, the execution phase and the after-action debriefing and should address lessons to be learnt from arranging the exercise. One purpose of the follow-up analysis is to evaluate the exercise event and to ensure re-usability of the components, such as scenario, training environment and injects [2, 3]. Another purpose may be to secure data that may be used to conduct future research based on the exercise, a process that requires high quality data to be collected [1, 23].

At FOI, the follow-up analysis is normally carried out as a workshop involving the white, green and red teams shortly after the exercise event. The blue teams may indirectly participate by having given feedback or filled out questionnaires during and after the execution phase. Depending on the objective of the follow-up analysis, the amount of information analysed varies. FHS [1] describes data that may be analysed during the follow-up analysis.

To ensure that the experiences made by arranging the exercise will not get forgotten, it is important that the analysis is performed in close proximity to the execution. This is especially emphasized by the MITRE Corporation that stipulates that the after-action report should be finished within 21 days after the execution [5].

The primary challenge in the evaluation phase that a exercise management and support tool must address is that collected data regarding all exercise events must be compiled in a visually well-presentable way suitable for the debriefing. The tool should also save data from previous exercises, to make evaluations of different exercise runs and concepts possible. Experiences from such evaluations can be used to create better injects and training environments in the future.

5. CRATE Exercise Control

The first version of CEC was released in 2015. Since then, CEC has been used in several cyber defense exercises each year, and the functionality of CEC has been evaluated during the follow-up analysis after each exercise. The analyses were based on data collected from the training participants via evaluation forms as well as verbal feedback and observation notes provided by the personnel arranging the exercise. After having collected these experiences from using the tool, CEC was redesigned into a second version in 2018. This section begins by presenting the main functionalities of the tool and then give a brief description of how the tool is used during each phase.

Basically, CEC is a web-based, multi-user system where all data is collected and presented in shared views. During planning, each exercise is set up as a separate entity in CEC, including users, teams and scenario. Injects are then scheduled by adding them from an inject library. When running the exercise, the participants of the blue teams use CEC to report events that occur in the training environment. Once created, the reports are assigned to corresponding injects by the white team and are automatically plotted on a exercise timeline. Information may be amended to the reports, supporting an inter-team dialogue and simultaneously documenting how each event is handled. When finished, the reports are scored by the white team. The scoreboard is displayed on a separate monitor, often placed for public viewing.

5.1. Injects

Injects include administrative injects, such as social engineering and added objectives as well as technical injects such as DDOS-attacks, malware outbreaks, targeted hacker attacks, system abuse and mis-configured resources. CEC includes a library with injects that are played by the white and the red teams during the exercise. The injects are documented using a template that includes fields for administrative information, prerequisites, execution and evaluation, as described in Table 1.

TABLE 1. DATA FIELDS OF THE INJECT TEMPLATE

Category	Name	Description
Administrative	Inject name	Indicates the status of the inject as *to be implemented*, *work in progress* or *ready*
	Status	Short, descriptive name of the inject
	Description	Description of the inject
	Issues	Known issues that may arise when running the inject
	Learning goals	What are the participants expected to learn from the inject
Prerequisite	Preparation	Recommended lectures, cheat sheets needed by the participants
	Dependencies	Software, tools and other injects that may be needed
	Additional information	Resource field
Execution	Green/Red team	Detailed description of the actions required by the respective teams
	Blue team	How can the blue team detect the inject, hints to be used by the white team if needed.
Evaluation	Scoring requirements	Description of how the white team should score the inject

The inject library is a resource that is shared between different exercises. This makes it possible to build a repository of injects over time. When an inject is scheduled for an exercise, a copy of the inject is retrieved from the database to the exercise instance. Where necessary, the inject details may be edited to include adaptation to different training environments, for instance how it is run against a certain system. Figure 2 displays a view of the inject library in CEC, from where the user can see the status of different injects available as well as access details about an inject.

5.2. Users and roles

CEC includes a role-based access control system, making it possible to limit or customize user access. For each exercise, teams are created and assigned the role *participant* or *management*. Users are assigned to teams and are given access rights in accordance to their role during the exercise. The blue teams are given the participant role, which restricts their access to the corresponding team area, while the management role allows users to access

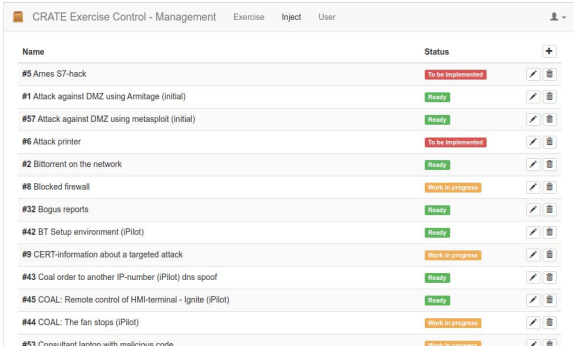

Figure 2. Inject library view

all teams' areas. Based on the access control system, the participants are only presented with the views relevant to their role in the exercise. Views that should not be accessed or are simply not relevant will be completely removed, keeping the interface clean and easy to navigate.

5.3. Event reports

During an exercise, the injects performed by the white and red teams will result in events occurring in the training environment. These will be handled in the systems as they would normally be handled in the real world, for instance by patching a certain system, editing system settings or by taking a system offline. Beside these actions, the participants will also use CEC to report the event by filling out an incident report or change request form. Figure 3 displays an example of the event view using the incident report form.

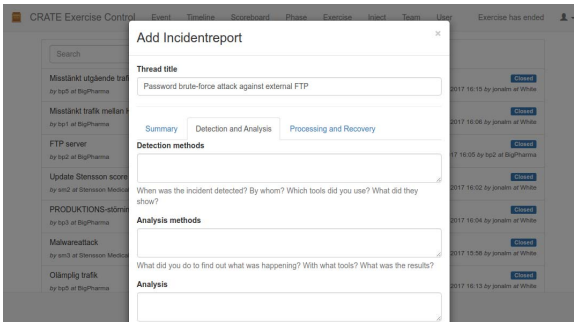

Figure 3. Event view

Forms in CEC are designed using the Angular Schema Form specification [24]. Different forms and form types are used in different exercise scenarios, and can easily be substituted with forms matching those used by the participants' organizations. This makes it possible to evaluate the actual forms during realistic incident management. In this paper, we will present the forms that are used in an incident handling course as examples.

When the CEC user submits the form, a new event thread will be created in CEC, which then can be accessed by the white and green teams. The participants in this course have three different form templates available, *Incident report*, *Change request* and *Message*. The *Thread title* field can only be set when starting a new thread.

The incident report form is used to report events detected by a participating team and the countermeasures they choose to utilize. The form is divided into three main categories of information as described in Table 2.

TABLE 2. DATA FIELDS INCLUDED IN THE INCIDENT REPORT FORM

Category	Name	Description
Overview	Thread title	A descriptive name of the incident.
	Summary	A short summary of the incident reported. What happened, who did what and what was the result.
Detection and analysis	Detection method	When was the incident detected and by which tools.
	Analysis method	What did you find out about what was happening and which tools did you use.
	Analysis	How and which parts of the system were affected. What caused the incident? How serious was it and what consequences did it have?
Processing and recovery	Mitigation	How was the incident mitigated, by whom? How did you gather evidence? Which tools were used?
	Restoration process	How did you restore the systems? What actions should be taken to prevent future incidents?
	Additional information	Can you change your routines to perform better? Did you lack any tools or training that may be included in lessons learned?

The change request form is used by the blue teams to request changes to systems where they lack privileges such as central firewalls. The form includes the fields listed in Table 3. The third event type is the Message, which includes the fields *Thread title* and *Message*.

TABLE 3. DATA COLLECTED VIA THE CHANGE REQUEST FORM

Name	Description
Thread title	A descriptive name of the request.
Type of request	Defect or Enhancement
Description	A detailed description of the change being requested.
Priority	An integer used to indicate how urgent the team regards the change.
Reason for change	A description of why the change is being requested
Impact on the system	List artefacts affected by the change
Assumptions / Other information	Resource field

The normal workflow during an exercise is that the incident reports are submitted by the blue teams and handled by the white team. The change requests submitted are handled by the green team in dialogue with the white team. Once created, it is possible to add information to the event reports created, allowing a documented dialogue between the teams. Each event report is also mapped to the relevant inject (the inject causing the report) to allow tracking. The Message form is used to pass questions to and from the blue team and management teams, which may also be done over in-game email.

5.4. Timeline

A timeline view has been integrated into CEC. In this view, planned and executed injects with related incident reports are plotted as blue dots along the timeline as depicted in Figure 4. The interface is designed using a drill-down approach, allowing each event to be further investigated by simply clicking on it. By including generic events used to report technical problems registered by the green team and unsolicited reports made by the blue teams, these unplanned events are also presented to the white team.

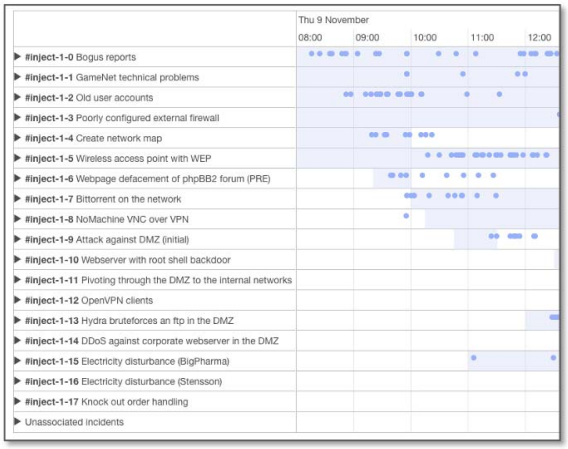

Figure 4. Timeline view

5.5. Scoring

To be able to use scoring during exercises, the functionality to collect and present the current score for each blue team have been integrated into CEC. One source of the score is availability measuring of the systems included in the training environment. Another source is scoring of the event reports reviewed by the white team. The events are scored in accordance with the information present in the inject library to ensure that each team get the correct score. CEC also includes a scoreboard view used to display the current score of all the training teams as seen in Figure 5.

6. Experiences made using CEC

This sections begins by describing how CEC is used during each phase of the CDX and how CEC addresses the challenges presented in section 4.

6.1. Planning phase

After the initial dialogue as described in subsection 4.1, planning usually starts by creating an exercise entity in CEC, where only the exercise name and execution dates need to be known. The entity is then gradually

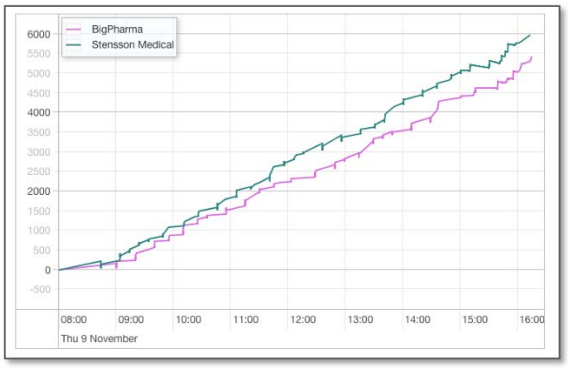

Figure 5. Scoreboard view

filled by adding more data as planning proceeds. Based on the learning objectives and the prior knowledge of the participants, the exercise timeline is populated by selecting and scheduling the injects that are to be run during the exercise. This results in a schedule that the white team will follow during the exercise.

As CEC is web-based and uses a central database, everybody involved in the planning phase can contribute to the same exercise entity and can immediately view the progress of the planning activities. To facilitate the process of matching suitable injects for each exercise, descriptions of the learning objectives are included with in the injects in the library. By updating the injects based on the follow-up analysis, the experiences made during exercise execution may be preserved. The timeline view that is integrated in CEC provide the arranging teams with a schedule for the execution phase.

6.2. Execution phase

During the execution phase, the white team will use the event reports filled by the blue teams in combination with the timeline view to get an overview of the exercise progression. The white team is also able to access the inject library to get information about different injects, for instance on how to assist struggling blue teams. The red team will use the timeline to know when to launch different attacks and will access the inject library to get instructions of how to perform certain attacks. The green team perform many of their tasks outside of the scope of CEC, but monitors and updates change requests submitted in the tool. They will also document any issues in the training environment for use during the evaluation phase.

The blue teams will mainly interact with CEC by writing incident reports and change requests. The incident reports are scored by the white team in accordance with the scenario of the exercise. Scoring is then displayed on the scoreboard, as shown in Figure 5. The blue teams do not have access to the timeline view.

One of the most important challenges to address with CEC was to enhance the situational awareness for the white team during the execution phase. FOI's experience when hosting exercises with up to six blue teams, is that the tool facilitates an overview of the exercise to a degree where a separate yellow team rarely is needed. However, it is still beneficial for the white team to observe the blue teams since it allows them to perceive details about the blue teams' progress.

In its current version, CEC does not include the monitoring tools used by the green team to monitor the availability of the training environment, but by documenting the events that occur in CEC and affiliate them to an technical issue category, this data is available during evaluation.

6.3. Evaluation phase

Evaluation of the exercise is an important part of the exercise, since it allows the participants to re-live the exercise from a different perspective. During evaluation, it is possible to explain the injects, to review the countermeasures taken by each team and compare the effect of the actions. During the after-action debriefing, the timeline view and the inject library of CEC are used. This is the first time that the teams subjected to training are able to see the timeline view. Since CEC already holds all the data, there is no need for the white team to prepare any presentation and by using a drill-down functionality in CEC, the instructors are able to present details about events where needed.

CEC is also used during the follow-up analysis of an exercise. By accessing the exercise instance in CEC, all the data collected during the exercise is available, supporting the follow-up analysis and making it more accurate. Based on the analysis of how the exercise went, the injects in the inject library in CEC are updated, improving future exercises.

7. Future work

Starting with a focus on the improvement of the tool CEC, future work includes the integration of the documentation relating to the training environments into CEC, and a new situational overview page where a granular status for each team's progression with each inject will be presented. It would also be of interest to add features that would allow documenting experiences made when arranging exercises in greater detail to allow the data to be used to perform future research. We are also looking into automating the red team by integrating the attack orchestration tool SVED (Scanning, Vulnerabilities, Exploits and Detection) [25] into CEC.

Shifting focus to cyber exercise management and support tools in general, there are still work to be done. We've found several papers that contain references to tools that exist in different cyber ranges, but these descriptions are often incomplete, leaving room for a more thorough compilation of tools and their features. There are also several exercise management methods from other training domains, such as JEMM, that could be evaluated during cyber defense exercises. It would also be of interest to include publicly available tools such as EVE and ADAM in future exercises to compare performance and impact on the situational awareness.

Finally, the scope is broadened to include general aspects concerning cyber security exercises. In this scope, it is of interest to further investigate when different types of exercises are suitable to attain stipulated learning objectives, as exemplified by research published by Lif,

Sommestad, and Granasen [26] and Karjalainen, Kokkonen, and Puuska [27]. It would be of interest to investigate how exercises can be used to conduct research experiments as described by Sommestad and Hallberg [23].

References

[1] H. Wilhelmson and T. Svensson. *Handbook for planning, running and evaluating information technology and cyber security exercises*. Handbook. Center for Asymmetric Threats Studies, Swedish Defence University, 2014.

[2] European Union Agency for Cybersecurity. *Good Practice Guide on National Exercises*. Handbook. ENISA, Dec. 2009.

[3] J. Vykopal, M. Vizváry, R. Ošlejšek, P. Celeda, and D. Tovarňák. "Lessons learned from complex hands-on defence exercises in a cyber range". In: *2017 IEEE Frontiers in Education Conference (FIE)*. Oct. 2017, pp. 1–8. DOI: 10.1109/FIE.2017.8190713.

[4] P. Perla and E. McGrady. "Why Wargaming Works". In: *Naval War College Review* 64.3 (June 2011), pp. 111–130.

[5] J. Kick. *Cyber Exercise Playbook*. Handbook. The MITRE Corporation, 2014.

[6] K. Joonsoo, M. Youngjae, and J. Moonsu. "Becoming Invisible Hands of National Live-Fire Attack-Defense Cyber Exercise". In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2019, pp. 77–84.

[7] F. Melón, T. Väisänen, and M. Pihelgas. "EVE and ADAM: Situation Awareness Tools for NATO CCDCOE Cyber Exercises". In: *Systems Concepts and Integration (SCI) Panel SCI-300 Specialists' Meeting on 'Cyber Physical Security of Defense Systems'*. 2018.

[8] T. Kokkonen and S. Puuska. "Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises". In: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer International Publishing, 2018, pp. 277–288. ISBN: 978-3-030-01168-0.

[9] J. Marshall. "The Cyber Scenario Modeling and Reporting Tool (CyberSMART)". In: *Conference For Homeland Security, Cybersecurity Applications & Technology* (Mar. 2009), pp. 305–309. DOI: 10.1109/CATCH.2009.46.

[10] M. Pihelgas. "Design and Implementation of an Availability Scoring System for Cyber Defence Exercises". In: *Proceedings of the 14th International Conference on Cyber Warfare and Security* (2019), pp. 329–337.

[11] R. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva, and J. Forsythe. *Automated Performance Assessment in Cyber Training Exercises.* Tech. rep. Sandia National Lab, Albuquerque, NM (United States), 2015.

[12] M. Yamin, B. Katt, and V. Gkioulos. "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture". In: *Computers & Security* 88 (Oct. 2019). DOI: 10.1016/j.cose.2019.101636.

[13] E. Cayirci. *NATO's joint warfare centre perspective on CAX support tools and requirements*. Tech. rep. Joint Warfare Centre Stavanger (Norway) CAX Support Branch, 2006.

[14] Strålskyddsmyndigheten. *It-attack mot kärntekniska anläggningar övas*. 2017. URL: https://www.stralsakerhetsmyndigheten.se/press/nyheter/2017/it-attack-mot-karntekniska-anlaggningar-ovas/ (visited on 05/26/2020).

[15] C. Valassi and M. Wedlin. *Övningsrapport: SAFE Cyber 2019. Planering, utveckling, genomförande och lärdomar av en storskalig CDX-övning*. Tech. rep. FOI-R–4885–SE. The Swedish Defence Research Agency, Jan. 2020.

[16] E. Cayirci and D. Marincic. "Computer assisted exercises and training". In: *New Jersey, USA: Hoboken* (2009), pp. 21–26.

[17] The Department of Homeland Security. *Homeland Security Exercise and Evaluation Program, January 2020*. The Department of Homeland Security, 2020.

[18] S. Kucek and M. Leitner. "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments". In: *Journal of Network and Computer Applications* 151 (2020). ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2019.102470.

[19] F. Absil, A. Dijk, and B. Meulendijks. "Lessons Learned from NATO's Cyber Defence exercise Locked Shields 2015". In: *Militaire Spectator, 185(2), Breda: Koninklijke Vereniging ter Beoefening van de Krijgswetenschap* (2016), pp. 65–74. ISSN: 0026-3869.

[20] E. Seker and H. H. Ozbenli. "The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation". In: *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. June 2018, pp. 1–9. DOI: 10.1109/CyberSecPODS.2018.8560673.

[21] J. Mirkovic et al. "Testing a Collaborative DDoS Defense In a Red Team/Blue Team Exercise". In: *Computers, IEEE Transactions on* 57 (Sept. 2008), pp. 1098–1112. DOI: 10.1109/TC.2008.42.

[22] V.-V. Patriciu and A. Furtuna. "Guide for designing cyber security exercises". In: *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*. World Scientific, Engineering Academy, and Society (WSEAS). Jan. 2009, pp. 172–177.

[23] T. Sommestad and J. Hallberg. "Cyber security exercises and competitions as a platform for cyber security experiments". In: *Nordic Conference on Secure IT Systems*. Springer. 2012, pp. 47–60.

[24] SchemaFormIO. *SchemaForm*. URL: http://schemaform.io (visited on 03/05/2020).

[25] H. Holm and T. Sommestad. "SVED: Scanning, Vulnerabilities, Exploits and Detection". In: *MILCOM 2016 - 2016 IEEE Military Communications Conference*. Nov. 2016, pp. 976–981. DOI: 10.1109/MILCOM.2016.7795457.

[26] P. Lif, T. Sommestad, and D. Granasen. "Development and evaluation of information elements for simplified cyber-incident reports". In: *2018 International Conference On Cyber Situational Awareness,*

Data Analytics And Assessment (Cyber SA). June 2018, pp. 1–10. DOI: 10.1109/CyberSA.2018.8551402.

[27] M. Karjalainen, T. Kokkonen, and S. Puuska. “Pedagogical Aspects of Cyber Security Exercises”. In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2019, pp. 103–108.