Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D6.5

Flagship 2

Document Identification	
Due date	31 January 2022
Submission date	12 April 2022
Revision	1.3

Related WP	WP6, WP7	Dissemination Level	PU
Lead Participant	JAMK	Lead Author	Jani Päijänen (JAMK)
Contributing Beneficiaries		Related Deliverables	D6.4, D7.1, D7.2, D7.3

Abstract: Flagship 2 was a umbrella event comprising events: a cross-border, online only cybersecurity exercise, targeted at CyberSec4Europe partners (participants), and an open event to simulate working as a cybersecurity analyst (analysts). The exercise participants simulated new employees of an critical infrastructure operator. They detected anomalies in a master system that controlled a railway network and investigated and responded to the issue using modern, well-integrated cybersecurity controls. The analysts were expected to perform forensics, reverse engineering, script de-obfuscation and analysis of a malicious office document to six digital samples, that were exported from the exercise environment.

Flagship 2 showcased that even in an organisation that has modern and well-integrated security controls, investigating a cyber incident requires skills and knowledge to use the available tools to understand the attack path and to perform low-level digital forensics, such as memory dump or reverse engineer a binary. If an organisation does not have such skills or knowledge in-house, it should have ready thought and exercised practicalities, i.e. standard operating procedures, in place to quickly alert external cybersecurity specialists to support the organisation. Flagship 2 exercise also showcased that even modern systems or subsystems, that have no requirements of backward compatibility, may have weaknesses that a threat actor may exploit.

Flagship 2 received 82 registrations from twelwe European countries. Registrations were distributed as 21 to the exercise and 61 to the analyst activity. Participants of both events welcomed the Flagship 2 concept and were looking forward to participate into a similar event in the future.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

The Flagship 2 cybersecurity exercise was a continuation to Flagship 1. In the Flagship 2 exercise the participants, simulating new employees of a modern critical infrastructure operator (a fictional Italian train operator, Cyber Rails s.r.l.) detected anomalies that they investigated. The investigation revealed that there was really an active threat actor in the environment. The threat actor had succeeded in penetrating networks of Cyber Rails. It had moved laterally and eventually it had modified the on-train firmware which was guarded by a Trusted Platform Module (TPM). The exercise participants followed the attack path, cleared the environment and detected the initial weakness that allowed the threat actor to penetrate the network. Due to the limited exercise time and the technical nature of the exercise, no GDPR, communications nor managerial roles were simulated in the exercise.

To raise awareness of cybersecurity analysts work, an open analysts activity was planned and offered to anyone of legal age and experience in Linux command line tools. The analyst activity was run in parallel with the actual exercise. The analysts were expected to analyse samples exported from the exercise environment and report their findings to the exercise using a dedicated self-hosted open-source capture the flag (CTFd) platform instance. The analysts woked solo without any instructutions on how to analyse the samples. They were offered and required to use a prepared virtual machine to analyse the samples, which they commissioned to their own environments. A total of six samples were offered to the analysts. From the 61 registered analysts, total 43 reported findings, 19 reported correct answers to all the six sample challenges. Two analysts reported correct answers with no errors. 18 analysts did not return any reports.

In total there were 19 exercise participants from CyberSec4Europe. They gave highly positive feedback about the exercise. After the exercise the participants answered to a short survey. All survey respondents reported that the exercise was beneficial for them, they learnt something new and would recommend the Flagship 2 exercise to a friend or a colleague.

There were 43 active analysts, providing either correct or incorrect submissions. No systematic feedback was collected from the analysts, but they gave positive feedback in the technical support chat that was offered. The conductor of the Flagship 2 estimates that the analysts activity attracted junior and high-performing specialists, and also IT professionals with no previous experience in analyst work. Based on the received feedback and from the statistics of the analysts activity, the conductor estimates the analyst activity was in demand.

The technical platform used in the exercise was a cyber arena. It included all the necessary technical cybersecurity controls and systems that supported the exercise participants learning experience and learning outcomes.

Document information

Contributors

Name	Partner
Juha Piispanen	JAMK
Jarmo Viinikanoja	JAMK

Reviewers

Name	Partner
Jozef Vyskoc	VAF
Antonie Lioy	POLITO
Liina Kamm	CYBER

History

Version	Date	Authors	Comment
1.1	2022-03-02	Jani Päijänen	Draft for internal review
1.2	2022-03-16	Jani Päijänen	Modifications based on review comments.
1.3	2022-04-08	Jani Päijänen	Modifications based on the review comments.

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AS**	Autonomous System
B	**BRNO**	Masaryk University, Czech Republic
	BBB	BigBlueButton, is an open-source virtual classroom software, initially created in Technology Innovation Management (TIM) program at Carleton University's Institute for Technology Entrepreneurship and Commercialization in Ottawa, Canada
C	**CPU**	Central Processing Unit
	CRM	Customer Relationship Management system
	CSE	Cybersecurity exercise
	CTF	Capture The Flag
D	**DFIR**	Digital Forensic Investigation and Response
G	**GDPR**	General Data Protection Regulation
I	**IT**	Information Technology
	IPR	Intellectual Property Rights
	ISP	Internet Service Provider
J	**JAMK**	JAMK University of Applied Sciences, Finland
	JYVSECTEC	Jyväskylä Security Technology (JYVSECTEC), is the cybersecurity data-analytics and artificial intelligence research, development and training center, in the Institute of Information Technology in JAMK.
O	**OT**	Operational Technology
R	**RBC**	Radio Block Centre
	RGCE	Realistic Global Cyber Environment
	RT	Red Team
S	**SD-WAN**	Software Defined Wide Area Network
	SSO	Single sign-on
	SIEM	Security Information and Event Management
T	**TMS**	Traffic management system
	TPM	Trusted Platform Module

TTPs	Tactics, Techniques and Procedures
TUDELFT	Delft University of Technical, the Netherlands

Glossary of Terms

A **Autonomous System**

An Autonomous System (AS) specifies a network, mostly an organization that can own or announce network addresses to the Internet (NIST 2022).

C **Capture the Flag**

Capture the Flag (CTF) is a cybersecurity competition or training event. The objective is to capture the predefined flags. There may be a technical solution where the participants submit their flags, and the solution gives feedback wheter the flag is correct or incorrect. Capture the flag events may be targeted to both individuals and teams.

Cyber Arena

An training environment containing many cyber ranges, or environments that can be used for domain specific, cross-domain or generic cybersecurity research, development and training.

Cyber Range

A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend on. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components, which are, in turn, desirable or required for achieving specific cyber range use cases. (European Cyber Security Organization (ECSO) 2020)

Cyber Range Technical Federation

The technical federation of cyber ranges (CRTF) enables the federated parties to utilize or consume specified functionalities, services, capabilities or resources from another party or parties of the federation. Once the technical federation is established, the usage of the resources or services may happen seamlessly, i.e. transparently from end user perspective. It may require contracts or other kinds of a trust relationship where the parties agree e.g. acceptable usage of provided functionalities or services.

O **Operational Technology**

Operational technology (OT) referes to the hardware and software systems used in industrial and critical infrastructure operations to monitor and control physical processes, devices and infrastructure.

R **Radio Block Centre**

Radio Block Centres (RBCs) are part of the European train control systems, and they are used to authorise trains to continue on their route.

Realistic Global Cyber Environment

Realistic Global Cyber Environment (RGCE) is a technical platform that contains several domain specific and generic cyber-physical and simulated systems for cybersecurity research, development and training. The platform is designed, developed and operated by JYVSECTEC.

Red Team

Red team (RT) simulates one or more threat actors in cybersecurity exercises.

S **SIEM**

Security Information and Event Management (SIEM) is a technical solution that collects the defined security and event information from various systems an organisation has.

T **Tactics, Techniques and Procedures**

Tactics, techniques and procedures (TTPs) are the behaviour of an (threat) actor.

(Rail) Traffic Management System

Rail Traffic Management Systems (TMS) are designed to support railway operations, processes and procedures.

Trusted Platform Module

A Trusted Platform Module (TPM) is a hardware based implementation (a chip) embeded in modern systems which enables to trust in computing systems in general. Specific goals may be e.g. securing cryptographic keys.

Z **ZeroTier**

A software only SD-WAN implementation, developed and opensourced by ZeroTier Inc.

1 Introduction

Flagship 2, a cross-border cybersecurity umbrella event organised by CyberSec4Europe, contained two events - a cybersecurity exercise (CSE) that was targeted at CyberSec4Europe affiliates, and a cybersecurity analyst activity that was open. Both events took place in two consecutive days on 25–26 January 2022. Whilst the exercise participants were hands-on investigating cyber incident that a fictional critical infrastructure operator had faced, the analysts were performing analysis on digital samples exported from the exercise environment. In the analyst activity narrative, the analysts were playing a role of external cybersecurity consultants, searching for evidence and relevant information from the samples and reporting their findings to the exercise, which simulated a customer. The exercise was the main event.

The exercise and analysts activity were loosely coupled, because of the uncertainty of the number of analysts, their capabilities and performance. Had there been late reports from the analysts, the exercise would have been impacted. Therefore, the conductor had prepared key information for the team coaches that could be provided to the exercise participants, had the analysts' reports not been received. Neither the the exercise participants nor the analysts were scored, because the conductor wanted to create a safe environment for learning.

The Flagship 2 was conducted by JAMK University of Applied Sciences' cybersecurity, data-analytics and artificial intelligence research development and training center JYVSECTEC (conductor), Finland. The analysts virtual machine were planned in co-operation with Masaryk University (BRNO), Czech Republic, and created by BRNO using the cyber sandbox creator (CyberSec4Europe 2020a, Masaryk University 2022a). Technical support for the analysts was offered by BRNO on an open-source web conferencing system for online learning (BigBlueButton 2021) instance hosted by Delft University of Technology (TUDelft), the Netherlands. The technical exercise platform was Realistic Global Cyber Environment (RGCE).

A concept map of Flagship 2 showing participants and analyst relationship to the event, and the technologies the participants and analysts used is is shown in Annex A: Concept Map of Flagship 2.

1.1 The Application Form

An application form was created for both exercise participants and analysts. The form had mandatory questions to indicate the respondent's relationship with a CyberSec4Europe affiliate, the kind of the relationship (employee, student or not working for the affiliation), the track to apply for (exercise, analyst activity), privacy policy related questions and terms of service related questions. The privacy policy and terms of service were links to a pdf file. The application form did not survey applicants' profiency in English, despite it was used language both in the exercise and the analyst activity.

The survey form had one question with multiple options the perform self-evaluation on skills and concepts related to the exercise and analyst activity. One question gathered information on experience in previous cybersecurity exercises and capture the flag events. These subject matter questions are shown in Annex B: Subject Matter Questions from the Application Form.

The responses provided by the exercise applicants were used when placing them into teams. The conductor target was to create balanced teams so that each team would have skilled members and members having knowledge on cybersecurity concepts, e.g. cyber kill chain and threat hunting. The reationale selecting the

team members was to ensure the teams had the technical skills and theoretical knowledge to solve the tasks they would be given and to support peer-learning within the teams.

1.2 The Path from Flagship 1 to Flagship 2 Cybersecurity Exercise

The storyline of Flagship 2 continued from Flagship 1. In Flagship 1 two organisations, the University of Kybereo and Cyber Rails s.r.l, published a R&D co-operation. The co-operation was that the Swiss University conducts research on the vast amount of railway related data that the Italian train operator (Cyber Rails) had collected. The participants of Flagship 1 were placed as employees of the Kybereo University and they faced a cybersecurity incident, which they had to mitigate and respond to (CyberSec4Europe 2021a). The activity included non-technical roles and activities, such as GDPR related, in addition to technical roles and activities. In Flagship 1 there were organisational charts and guidelines prepared for the participants. Had there been missing information or erroneous information in the guidelines, the participants were told that they could improvise as needed. Because the background of the participants was heterogeneous, an introduction level online open course was created for the technically oriented participants. The voluntary course introduced them to digital forensics (CyberSec4Europe 2021b).

The Flagship 2 exercise was technical in nature, had only technical participant roles available and focused on technical investigation of a suspected cybersecurity incident. The participants were not shown the exercise scenario nor detailed information of it, simulating a real-world scenario of a cyber incident. An organisation rarely knowns in advance when a cyber incident is about to take place, if it is intentional or unintentional, let alone who is behind the incident and with what objectives, if any. In Flagship 2 the exercise participants were simulating being new employees of Cyber Rails, and they had to detect an anomaly and technically investigate it by using the features and functionalities that the exercise environment offered.

The learning contents of the analysts activity and the exercise were created by experienced red team (RT) specialists, whom have participated to cybersecurity exercises and capture the flag competitions, and have experience in teaching cybersecurity to Bachelor’s and Master’s degree students in JAMK.

2 The Flagship 2 Exercise in Detail

Exercise participants were simulating new employees of the train operator Cyber Rails s.r.l. The narrative was that the company’s management had decided to strengthen its cybersecurity capability and capacity. The top management had learned from the Kybereo’s incident, which happened in Flagship 1, and

understood that Cyber Rails needs more in-house technical cybersecurity specialists, to proactively protect its digital and cyber-physical assets, and reactively respond and resolve possible incidents.

The objectives of the exercise were to:

- Showcase benefits how integrated security controls and logging in an organisation's network supports detecting and investigating a cyber incident,
- Raise awareness that investigating a cyber-attack requires knowledge about the environment and experience of the deployed security controls and available tools,
- Raise awareness that even modern security components, such as trusted platform modules (TPMs), may have weaknesses that a determined threat actor could exploit,
- Highlight that a realistically modelled and well-integrated cyber arena can be used to introduce various cyber security phenomena, and train people to work on them.

The exercise environment offered the employees e.g.:

- Global simulated Internet and its' core services,
- News and media sites and social media platforms,
- Networks of a simulated critical infrastructure operator,
- Realistically modelled digital services and data flows in the operator's network, including public web-pages,
- Simulated operational technology (OT) networks and systems, and data flows in the operator's network,
- Realistically modelled person data located in the information technology (IT) systems of the operator's in the network,
- Modern security controls and logging systems integrated into the operator's network

The 19 participants were placed into four teams, each team having a dedicated team coach. During the exercise, the teams had to answer questions that the team coach raised. The questions were placed to teams in stages; the coaches were in direct interaction with the teams and once the team had answered to previously raised questions, new questions were asked. Eventhough the questions were prewritten, team members had freedom interact within the team and to peek the environment and search the answers by themselves. In a large and complex environment, which is not previously known to the participants, several approaches may eventually result in finding the answers. The coach also assisted the team in using the available systems.

Had the team had questions or had they been unsure how to start acting on the current task, the team lead guided them, primary with questions, and eventully providing direct instructions. The method was initially tested in Flagship 1, and as it received positive feedback from the participants, it was applied in Flagship 2, too.

2.1 Exercise Day 1

The first exercise day started by introducing the new employees to the systems, that they would be using in their work. While introducing the environment and the security controls therein, the new employees detected that there was something weird going on in the system. On the Cyber Rails railway monitoring

system map view (Figure 1) it was visible that a train was randomly jumping between various routes and locations.

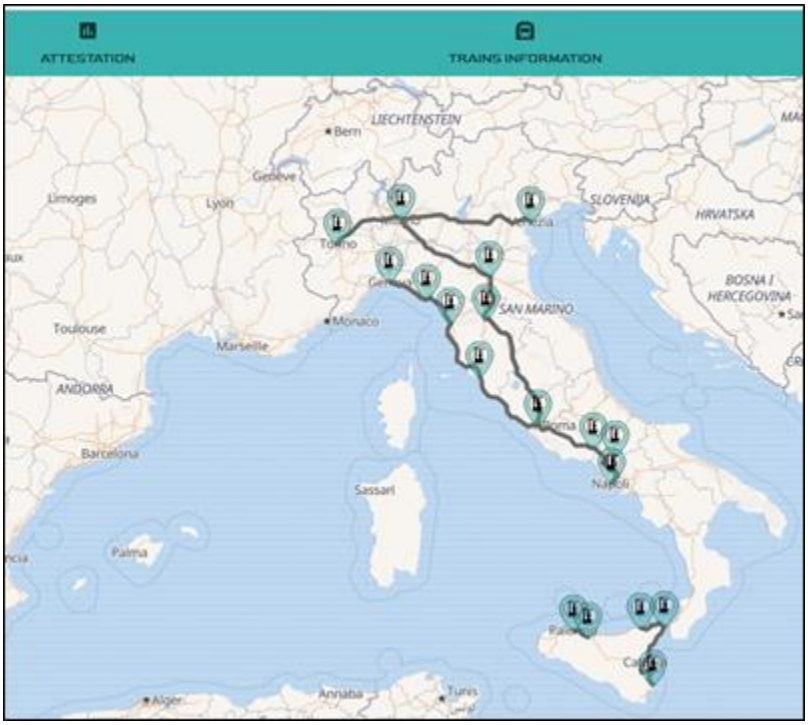


Figure 1: Snapshot of Cyber Rails railway monitoring system.

The attestations view (Figure 2) of the railway monitoring system indicated that the TPM and the traffic management system (TMS), located in the misbehaving train, were reporting error for some reason.

Figure 2: Attestation view of the railway monitoring system

Because Flagship 2 was a learning opportunity, the conductor had planned to the two exercise days so that they included lunch breaks and an afternoon break.

Before starting to operate on the security controls deployed in the Cyber Rails network, the participants had a lunch break. Returned from the lunch break, the participants detected that the workstation which had access to the railway monitoring system and which was used by a special administrator role, seemed to be locked by a ransomware and there was a ransom note visible on the screen (Figure 3).

Figure 3: Ransom note on a TMS controller server

By performing digital forensic investigation and utilising the reports the analysts had provided, the teams unlocked the server. Then the participants continued the investigation and detected the persistence of the

threat actor. Whilst teams were performing the investigation, a sample data of a customer relationship management (CRM) system was detected online, claiming the data originated from Cyber Rails.

The teams answered the following questions during the first exercise day:

- How can the ransomware can be disabled?
- Who put the ransomware there?
- Has the suspicious machine logged into any other machines?
- How to fix the jumping train on TMS?

2.2 Exercise Day 2

The second exercise day continued the investigation left open from the first exercise day, but focused to recovery and analysis of the incident. The analysts tasks included creating a timeline of the incident. During the day the exercise participants had to answer to the following questions:

- Does the dumped data belong to Cyber Rails?
- What system is the source of the data?
- Does this trigger GDPR related procedures?
- What caused the TPM alarm on the train?
- Analysts have identified and analysed a malicious document, could this be the root cause?

The employees could confirm that the online sample was from the CRM of Cyber Rails, their fictional employer during the exercise. The General Data Protection Regulation (GDPR) topic was only briefly discussed due the technical nature of the exercise and time restrictions, but it was clear that the incident would trigger the GDPR process (European Union 2016), e.g. to inform the national GDPR authority and the persons whose data had been breached.

The employees investigated the TPM alert (Figure 2), and technically analysed the firmware used in the train and learned learned that the deployed firmware was malicious. Whilst the teams built a timeline of the incident, they could confirm that a single opening of an email attachment, that was malicious, was the starting point of the incident.

2.3 The Technical Exercise Environment

The technical exercise environment was Realistic Global Cyber Environment (RGCE), which is a cyber arena (Karjalainen M. and Kokkonen T. 2020), containing several cybersecurity training environments. A new environment simulating a railway operator's IT and OT infrastructure (Figure 4) was created for Flagship 2. The fictional organisation, Cyber Rails, was connected to the simulated RGCE Internet through a simulated Internet service provider (ISP), which had the autonomous system (AS) number 3303. The organisation's environment contained several networks, e.g. an in-premises data centre, trackside systems and traffic controls systems. The trackside network included simulated radio block centres (RBCs), and the trains therein included simulated train firmware and the TPM.

The exercise participants accessed the environment using a prepared remote connection. The exercise environment had a single sign-on (SSO) portal, from where the participants could access the security controls, and the IT and OT systems deployed in to the organisational environment of Cyber Rails. More than 100 virtual machines were deployed for Flagship 2.

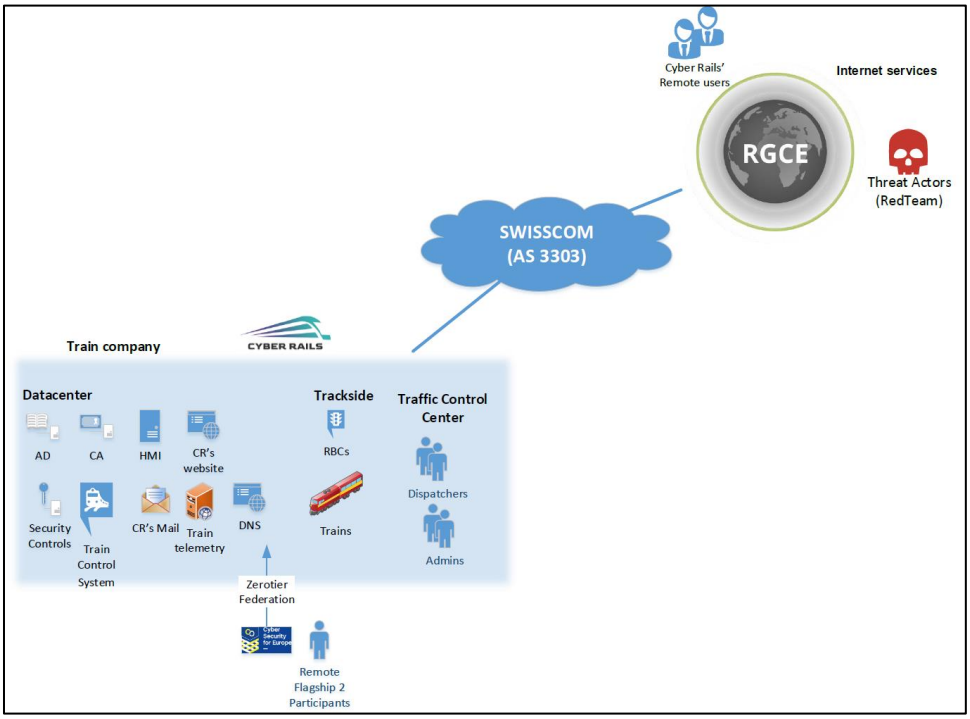


Figure 4: Overview of Flagship 2 technical environment

2.4 Cyber Range Technical Federation

The exercise participants accessed the exercise environment by using a prepared virtual machine created by the conductor. It was connected to a federation network that was created for the exercise. Technological solution to implement the federated network was ZeroTier, a software-only SD-WAN solution, developed and open-sourced by ZeroTier Inc. ZeroTier's home page is https://www.zerotier.com/.

By using a personal access token, each participant's connection was registered to a Zerotier ROOT (Figure 5), which was resided in commercial Amazon AWS cloud. Once the connection was registered, the exercise related traffic was automatically routed from participant's virtual machine to the exercise environment, trough JAMK Zerotier-2. The Zerotier controller, located in the conductor's data centre (JAMK Zerotier-2), was provisioned one CPU core and one GB RAM. All exercise participants' network traffic to the exercise environment was routed through this controller. The federation implementation reused the solution previously developed for Flagship 1 and reported in D7.3 Evaluation Report on Integration Demonstration

(CyberSec4Europe 2021c). The requirements of cyber range technical federation were documented in Part B of (CyberSec4Europe 2020b).

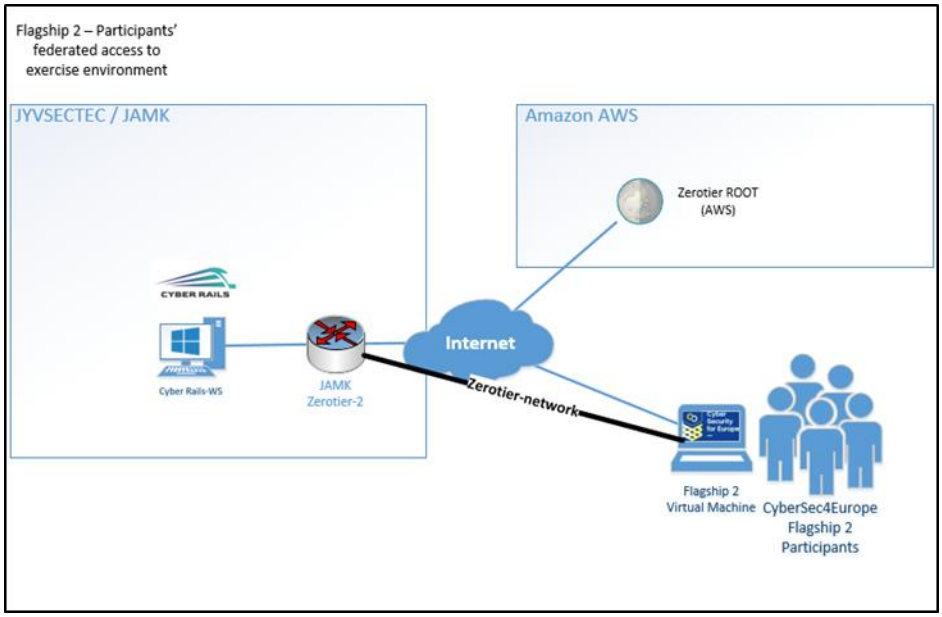


Figure 5: Overview of Flagship 2 Federation Architecture

The CPU utilisation (Figure 6) shows that the controller performed well. Peak CPU utilisation was under 20%, while the CPU's peak clock frequency was approximately 300 MHz. The controller was run in a virtual machine running a 64-bit CentOS-7 operating system.

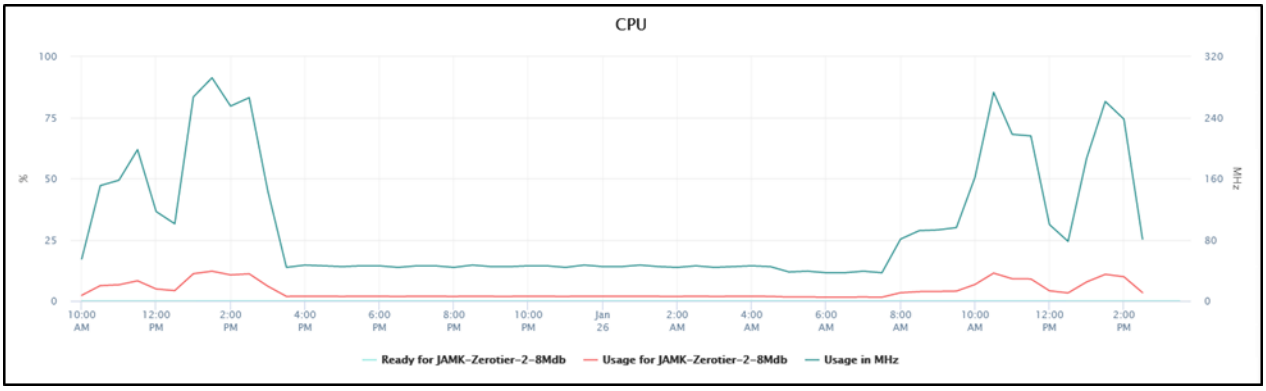


Figure 6: CPU Load on Zerotier controller located in the conductor's data center

The peak network bandwidth usage of the controller was on the second exercise day (Figure 7), remaining below one Mbps. From the point of view of recorded statistics, the controller was capable of handing the load that the participants access to the environment generated.

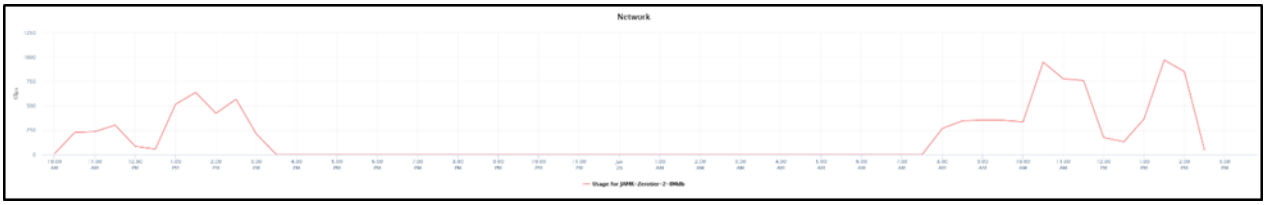


Figure 7: Bandwidth usage of Zerotier controller located in JAMK premises

A few participants reported occasional or recurring connectivity problems with the exercise environment. The conductor's monitoring or logging systems did not reveal the root cause, even though it was investigated during the exercise. An in-depth root-cause analysis about the reported connectivity issues was not performed.

The participants' remote access to the exercise environment was terminated at the end of both exercise days. This was due to the nature of the exercise. The exercise being a learning opportunity with dedicated team coaches, all participants were offered an equal opportunity to access the environment that is during the exercise active time only.

2.5 Exercise Planning Timeline

Planning and implementing a technical cybersecurity exercise is a requires skilled personnel and the technical exercise platform, but also a long timespan on personnel calendar's. The calendar slack enables more better exercise experience for participants, as the exercise learning objectives and the storyline can mature during short discussions the planners have over time. To have a solid story line for flagship 2, planning and content creation was started in parallel with Flagship 1 planning in 2020. After Flagship 1 there was a period where minimal detailed planning and development was carried out. The development activity intensified when the Flagship 2 event neared. The latest development work and environment testing were performed in January 2022. Such an on-off arrangement was possible due to the results developed in parallel with Flagship 1 and the re-use of the implemented cyber range technical federation.

3 Analyst Activity in Detail

The analyst activity, which supported the exercise and simulated a customer–cybersecurity service provider situation, was planned so that both entry level cybersecurity analysts and technically capable persons could find valuable information from the provided digital samples and report their findings their findings to the exercise. The objective of the activity was to raise awareness of an analyst's work, introduce tools that can be used by analysts, and to simulate a cybersecurity service provider activity. The method to do this was to investigate the samples exported from a suspected incident, using a virtualised analyst workstation that is safe to use for the analysis and which has modern analysis software to facilitate performing the analyst's tasks.

The analyst workstation was a prepared virtual machine containing Kali Linux with additional analysts tools pre-installed. There was also an additional virtual machine containing The Hive (The Hive Project 2022), had some of the participant decided worked in self-organised teams. Contents of the analyst's virtual machine were planned in co-operation between WP6 and WP7. The co-planned analyst virtual machine was created by BRNO using the Cyber Sandbox Creator (Masaryk University 2022).The analysts were sent a welcome email after registration to the analyst activity was ended. The email included an URL, which

contained the instructions on how to deploy the analyst virtual machine on their personal computing environment (Masaryk 2022b).

The analysts were informed several times that they must not perform network scans or other intelligence gathering operations on the real the Internet or on the IP-addresses the samples contain, nor should they share the samples to external parties. Had they done so, they could have broken laws in the location of their residence. The reason for the caution was that the IP-addresses the samples the samples contained were recorded from a cyber arena that containing simulated Internet, and thus the IP-addresses would have resolved to real nodes in real Internet. Some local laws in European countries state that it is illegal to share computer viruses or malware to persons that do not have a justification to receive it or have it in their possession. Therefore in the registration form the analysts fulfilled, they had commit to not to share the samples with externals. However, the samples did not contain computer viruses or malware.

The possibility to join to the analyst activity was marketed as a learning opportunity where the analysts would support the exercise participants. Contents of the analyst activity info set, sent to analysts as an email attachment, was created in collaboration with WP9 and WP7. The cover letter and the info set is shown in Annex C: Analyst Cover Letter and Info Set.

3.1 Analyst Tasks

The analyst activity started on the same day, but before the actual exercise. The reasoning was that it was unknown how soon the analyst can report valuable information, i.e, their findings, to the exercise. By giving them more time to analyse, the conductor hoped that analysts could provide information that could be used by the exercise participants, without the need to use the pre-prepared findings document.

In the event morning the analysts were sent an email containing their personal login information to a CTFd instance, an open-source capture the flag platform (CTFd 2022), which was commissioned on the conductor's premises solely to provide contents to the analyst activity. The email contained an URL to the technical support platform, a BigBlueButton (BBB) instance, hosted by TUDelft. The analyst could use the technical support platform to provide and ask for peer-support. The main motivator to use the BBB, a chat system hosted by an external entity towards the exercise, was to relief the deployment and monitoring needs that a running a publically available platform requires. Additionally collaborating within CyberSec4Europe and raise the awareness of the existence of BBB platform was considered important.

In the CTFd there were six challenges available, their difficulty ranging from easy to mediocre, but not hard, as estimated by the conductor. The difficulty was not presented to the analysts, and they were able take the challenges in any order. The challenges are listed in and screenshots from the CTFd platform can be seen in Annex E: Analyst Challenges.

Challenge No.	Challenge Name	Challenge Question	Challenge Category	Estimated difficulty (1: Easy – 5: Hard)
1	The dirty document	A system administrator has received an email, which has an MS Word document as an attachment. The document consists of a VBA macro, which has compromised a SysAdmin's system. Submit the name of the program being run when the VBA macro is executed.	Miscellaneous	1

Challenge No.	Challenge Name	Challenge Question	Challenge Category	Estimated difficulty (1: Easy – 5: Hard)
2	Oh no! My system is locked	A malicious program has prevented normal usage of several workstations. Find out the address of the attacker's Ethereum wallet, which is part of the ransom note. Submit the answer in form of: 0x123456789abcdef	Reverse engineering	3
3	Evil in the wire	Which IP is a participant in every TCP connection in this PCAP?	Packet analysis	2
4	What is wrong with my memory?	Malicious code is running in a compromised system's memory. Find out the name of the process Parent Process ID (PPID) of which is 7356.	Forensics	4
5	Hard times, hard drives	An attacker has dumped the customer relationship management database to the disk. Export the database and find out the number of rows in the database's contacts table.	Forensics	4
6	Why so obfuscated ?	An attacker has created a persistence mechanism to the file sharing server. A scheduled task executes an obfuscated powershell script to ensure that the malicious service exists and is running. Submit the name of the service the powershell script creates.	Miscellaneous	1

Table 1: Analyst challenges

3.2 Analysts' Resolve Statistics

There were a total of 61 registrants to the analyst activity. The statistics show that 43 (70%) submitted their findings to the CTFd platform (Table 1). Four analysts did not submit correct findings, so the number of actual users was 39. All six challenges were resolved by 19 analysts (44%), five challenges were resolved by 7 (16%), four challenges were resolved by 5 (12%), three challenges by 2 (5%), two challenges by 4 (9%) and one challenge by 2 analysts (5%).

No. correct submissions	No. analysts submitted	Percent of analysts (N=43)
6	19	44 %

No. correct submissions	No. analysts submitted	Percent of analysts (N=43)
5	7	16 %
4	5	12 %
3	2	5 %
2	4	9 %
1	2	5 %
0	4	9 %
Total	**43**	**100 %**

Table 2: Submission statistics

Total submission percentage distribution (Figure 8) shows that in total there were 522 submissions. The correct submissions count was 185 (35.4%) and there were 337 (64.6%) incorrect submissions.

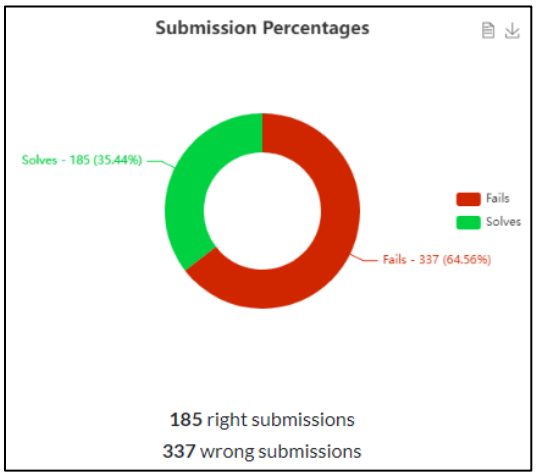


Figure 8: Submission percentages

Two analysts submitted six correct submissions without incorrect submissions, as shown in the detailed statistics in Annex F: Analyst Activity Submission Statistics.

The used platform, CTFd, allowed an unlimited number of submissions. As the analyst activity was a learning opportunity, the CTFd was configured so that no scores were rewarded for correct submission nor negative scores for incorrect submissions, and all challenges (samples) were immediately available. The reason for this approach was based on the conductor's internal discussion and decision that being an entry level learning event, the potential learning outcome was weighted more important than scores, thus letting

the analyst to test submitting their incorrect findings without penalty. CTFd provided the analysts feedback whether a submission was correct or incorrect.

Solves per individual challenges are shown in Figure 9 (n=39). The challenge “The dirty document” was resolved by 32 analysts (82.1%), the challenge “Oh no! My system is locked” was resolved by 28 (71.8%), the challenge ”Evil in the wire” was resolved by 35 (89.7%), “What is wrong with my memory?” by 34 (87.2%), “Hard times, hard drives” by 24 (61.5%) and the challenge ”Why so obfuscated?” by 32 (82.1%) analysts.

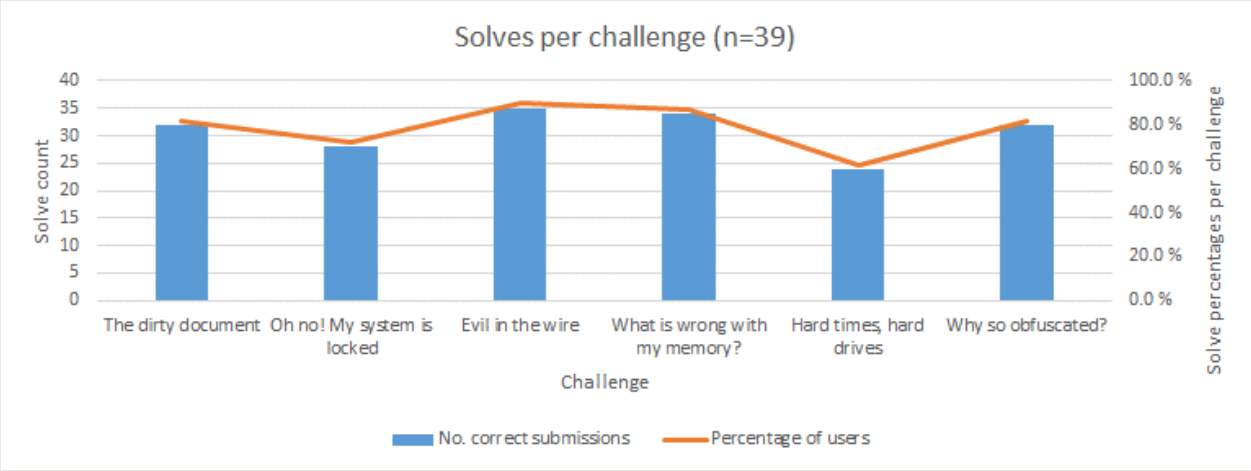


Figure 9: Solves per challenge

In a message posted to the technical support platform, an analyst reported that he or she could not fully focus to the analyst work due other commitments. A similar situation may have been with the other analysts, too. After the analyst event, the conductor received an enquiry if a walkthrough of the challenges will be published. The enquirer was told that no walkthrough exists.

3.3 Remarks from the Technical Support Platform

During the exercise days, the analysts asked a few questions from the technical support team. They were mostly related to the usage of Volatily, a forensic tool to analyse memory dumps. Also support to enlarge the hard drive that was attached to the analyst workstation was asked. Volatily had a file system level permission issue, i.e., wrong access and execution rights, which was easily detected and the fix was provided for the analysts. Another issue was that the version had some configuration errors, which the conductor did not detect when testing the analyst virtual machine. A peer-comment to circumvent the Volatily issue was published. Technical support on how to enlarge the hard drive was provided and a peer solution was received. The technical support chat log can be seen in Annex D: Chat Log from the Analyst Technical Support Platform.

The analysts’ questions on how to enlarge the hard drive were related to the challenge “Hard Time, hard drives”. That challenge had the least number of correct submissions. Although it was not researched, it could

be that performing the enlargement or attaching the disk image to the analyst virtual machine was either too difficult or was perceived as too time consuming, which could explain the low number of solves.

3.4 Analyst Activity Planning Timeline

There were several planning and status check meetings preparing the analyst workstation and to discuss the details related to the analyst activity between WP6 and WP7. In 2021, there were six meetings (March, May, June, September, November, and December). In January 2022, one meeting was held before the exercise. The conductor tested the virtual machine in December 2021. A dedicated privacy policy for the CTFd instance was created because the system was visible to the Internet. No feedback survey or discussion session after the analyst activity was conducted.

4 Participants

The possibility to participate in the exercise was primarily marketed in CyberSec4Europe mailing lists, whereas the analyst activity was marketed on social media platforms, on three webpages and by publishing two press releases.

CyberSec4Europe affiliates were reached via email on December 21st, 22nd and 29th 2021. The emails mentioned the analyst activity as an open capture the flag (CTF) event. The marketing letter is shown in Annex G: Marketing Letter to CyberSec4Europe Affiliates.

The registration form to the Flagship 2 exercise and analyst activity was opened 21st December 2021 and was open until 12th January 2022. The existence of the event was marketed on CyberSec4Europe webpages, the conductor's web pages, and in social media. A press release in Finnish was created and published by the conductor. CyberSec4Europe's WP9 created and published an English press release version. The Finnish press release was noticed by several Finnish online media services, which have a combined total weekly reach of over 1,200,000 readers as reported by the services' media cards. No page visit count is available from the media sites.

The registration form was temporarily reopened on 17th January for one affiliate person to register to the exercise. Such special arrangements require more relative work-effort than handling all the registrants *en masse*. The person was decided to enrol to the event, because the person participated in Flagship 1, so they

could compare the exercise experience between the two exercises and thus being able to provide feedback to the conductor for learning.

Quick facts about Flagship 2 registration:

- The event received total 82 registrations
- The exercise received 21 registrations (26%)
- The analyst activity received 61 registrations (74%)
- The event registrees were from 12 European countries
- The exercise registrees were from 11 European countries
- The analyst activity registrees were from three European countries
- The event gender distribution was 13% female, 84% male, 2% did not disclose.
- The exercise gender distribution was 24% female, 76% male
- The analyst gender distribution was 10% female, 87% male, 3% did not disclose.
- The analyst activity received submission from 43 registrees (70%)

More detailed statistics about affiliations, countries and gender distribution as reported by the registrees are shown in Annex H: Registration Statistics.

4.1 Timeline of Acquiring Participants

The event page describing Flagship 2 was published on 21st December 2021 (JYVSECTEC 2021). It was decided that the event page would be created under JYVSECTEC instead of JAMK, because JAMK webpages were under platform transition. By this arrangement, it was estimated that the required work effort to publish the event pages could be minimised.

CyberSec4Europe published a news item on 22nd December 2021 (CyberSec4Europe 2021d).

The Finnish press release was released 27th December 2021 (JAMK 2021). The press release was noticed by Finnish online media services TIVI (TIVI 2021), Uusiteknologia (Uusiteknologia 2021), Mikrobitti (Mikrobitti 2021), Kauppalehti (Kauppalehti 2022) and Talouselämä (Talouselämä 2022). Kauppalehti and Talouselämä are financial and investment media, while the others are technology oriented. Indicators exists that two local radio stations in the Jyväskylä area, where the conductor is located in, broadcasted a summary the press release, but no evidence exists.

Several posts on social media platforms, Twitter, LinkedIn, and Instagram were published by JYVSECTEC, JAMK, CyberSec4Europe and BRNO.

4.2 Quick Survey after the Exercise Active Phase

After the exercise active phase, but before a free form feedback and discussion session, the participants were requested to answer an anonymous quick survey. The survey was implemented on Webropol, a survey tool that JAMK offers to its employees and students. There was approximately 15 minutes time to answer to the survey.

A total of 19 persons participated in the exercise. From the participants 15 (79%) answered the survey. Free form feedback collected in the survey was highly positive, but also minor critique was raised. The conductor received critique from a participant that there were trails in the environment from a testing session. The

critiques was justifiable and correct: without the team coach, the team would probably have followed wrong trails.

Below is a single pick from the free form survey response, which illustrates the benefits the respondent acquired from Flagship 2:

> *Flagship 1 gave me a good idea about what "real" cyber exercises are about and Flagship 2 increased my interest towards them even more. In addition, the exercise gave me at least a general insight on what the technical people face after a cyber-attack, which helps me conduct research and perhaps even help them in their work.*

The quantitate questions, "Your team in the exercise", "Did you find the exercise beneficial for you?", "Did you learn something new?", and "Woud you recommend Flagship 2 for a friend or a colleague?" shows that the 15 (n=15) respondents representing all four exercise teams found the exercise beneficial for themselves, learned something new and would recommend Flagship 2 exercise for a friend or a colleague. In the free text question "Free feedback about Flagship 2", two respondents requested that an unplanned event, Flagship 3, with either Flagship 1 or Flagship 2 contents could be conducted on-site, so that people could work and network face-to-face. The anonymised survey questions and answers can be seen in

Annex I: Short Survey to Participants.

5 Lessons Learnt and Conclusions

Implementing a cybersecurity exercise and an analyst activity (a kind of a capture the flag) in parallel with aligned contents requires a certain kind of discipline from the event planners. The main challenge the conductor faced was the open analyst activity participants, as they had no contractual relationship with the conductor: how their (unknown) expectations could be met while simultaneously respecting the contractual commitments and global intellectual property rights (IPR) regulation.

In Flagship 2 the priority was the exercise. However, during planning the exercise and developing its contents, the persons involved had to take into account the analyst activity and keep a few questions active, such as:

- What are the key exercise events and what could be the digital samples related to the events that the analyst could investigate?
- Can the conductor legally provide a sample without breaking a law or a regulation? If it can, under which circumstances?
- Can the analysts legally investigate the sample? If they can, are there any conditions?
- Can the conductor provide a sample to a third party, which has no contractual relationship with the conductor, without committing an IPR violation? If it can, under which circumstances?
- Is the difficulty level of analysing a planned sample in alignment with the event difficulty level and with the estimated participants' knowledge, skills and abilities? If not, how can they be supported?

The conductor has organised cybersecurity exercises since 2013 (JYVSECTEC 2017). Flagship 2 was the first exercise the conductor offered a simulated railway environment, including the domain specific systems and processes therein. The conductor learned that even limited contents of an cybersexercise may not directly convert to analyst targets of an open analyst activity. To fullfill contractual commitments and legislation requirements, including global IPR legislation, the digital samples that was offered to the analysts, had to be very carefully implemented.

5.1 Meeting Flagship 2 Exercise Objectives and Received Feedback

The Flagship 2 exercise was technical in nature. The exercise participants, simulating new employees in a fictional critical infrastructure operator, investigated a misbehaviour of a train detected in a monitoring

system. The investigation revealed that a cyber incident had started before the exercise but evolved during the exercise and turned out to be a hostile in the system. The exercise participants mitigated the incident to an extent, as planned.

The objectives of the Flagship 2 exercise were:

- Showcase the benefits of how integrated security controls and logging in an organisation network supports detecting and investigating a cyber incident,
- Raise awareness that investigating a cyber-attack requires knowledge about the environment and experience of the deployed security controls and available tools,
- Raise awareness that even modern security components, such as TPMs, may have weaknesses that a determined threat actor could exploit,
- Highlight that a realistically modelled and well-integrated cyber arena can be used to introduce various cyber security phenomena to people, and train them to work on these.

The concept of teams having a dedicated coach received positive feedback. Based on the conductor's experience, a two-day cybersecurity exercise that aims to be beneficial for the participants and is held on a realistic cyber arena, requires dedicated coaches. Even there was a SSO portal for the participants, learning to navigate the large exercise environment and to operate the security controls and the tools in the environment might consume the limited exercise time so much that the real learning outcomes could be missed. Learning to use the core features of a system in a short time could be trivial for some, but learning to use several systems' core features to complete a task was not in the scope of the exercise.

Interpreted from the participant's feedback and survey responses the exercise objectives were met.

5.2 Meeting Flagship 2 Analyst Activity Objectives

The objective of the entry-level cybersecurity analyst activity was to simulate a cybersecurity service provider – customer activity. The analysts investigated samples exported from a suspected incident, using a virtualised analyst workstation that is safe to use for the analysis, and by using modern analysis software for performing the analyst tasks. The analyst activity was planned to be entry level in diffculty.

Based on the number of incorrect submissions from the analysts and time spent between first and last submission, the conductor concludes that there were a high number of junior analysts or persons not familiar with digital forensic investigation and response (DFIR). Based on the submission statistics and time spent resolving the samples, we conclude that there were also person who are specialised in DFIR.

The technical support platform for the analysts and its usage as peer-support platform served the analysts reliably and benefitted the analysts.

There were minor tooling challenges and a use-case that were not detected during testing the analysts workstation. It is not purposeful to have technological errors or challenges in a learning situation, but fortunately workarounds were found to circumvent the detected challenges.

There was no similar quick survey for the analysts as was offered to exercise participants, from where facts could be extracted. Based on the chat log, the resolve statistics, the background information the analysts provided in the registration form, and the enquiries the conductor received, the conductor estimates the analyst activity objectives were met.

5.3 Remarks from Online Cybersecurity Learning Opportunities

An analyst reached out to the conductor after the event enquiring a walkthrough of the challenges solutions. The simulation continues: a customer does not have the understanding to provide guidance. From the

analysts' learning outcome perspective, having such walkthrough, a systematic set of instructions to analyse the samples, could have been beneficial. However, based on the conductors experience in the subject and considering the event was entry-level, using Internet search engines, the correct tools and ways to operate them could have been found within the timeframe of the analyst activity.

Some analysts reported that they could not fully focus on the activity due other commitments. Based on the conductor's experience, distractions may severely affect the learning outcomes from a cybersecurity exercise, or in this case, the analyst activity. One of the reasons why the analyst activity was planned as a solo event was to mitigate the impact of potential distractions from a larger group of people.

For future online cybersecurity learning opportunities, the possibility of distractions a learner may face must be kept in mind during planning an event and its impact should be minimised. Should there be more distractions or perceived stress during a learning event, those should planned and ideally controlled by the conductor.

5.4 Demonstrating Cyber Range Technical Federation

The Flagship 2 exercise was conducted as an online event. Due to the possibility of travel restrictions set on short notice, the decision to conduct the event as online was easier than it was for Flagship 1. In Flagship 1 the conductor demonstrated cyber range technical federation. The technology was re-used in Flagship 2 and from the conductor's point of view worked reliably, consumed only little computing capacity and network bandwidth. A few exercise participants reported occasional loss of connectivity to the exercise environment, but the root-cause could not be found.

The conducted two Flagship exercises showcased that online, cross-border CSEs can be securely organised and participated utilising open-source SD-WAN technology. The used technology did not require configuration changes to participants' equipment nor did it require acquiring a separate network device, but installing VirtualBox virtualisation software and commissioning a prepared virtual machine into it.

5.5 Identified Opportunities

The contents of both Flagship 1 and Flagship 2 could potentially be used for training and education. They are safe environment to experience a cybersecurity incident and respond and mitigate it. Flagship 1 has contents for technical, communications, GDPR and top management roles. The value proposition for organisations (and companies) could be to understand the value of exercised cybersecurity incident response and mitigation plans, and improve such plans based on findings from the training. With improved plans the organisation could potentianlly more efficiently and promptly respond to and mitigate an incident. Having trained in Flagship 1, they could signal to their ecosystem that they have exercised their business continuity. For companies this could potentially help acquiring new and keep existing customers. There are examples that a cybersecurity incident can cause long-term financial harm or even bankrupt a company (YLE 2021), if it is a cybersecurity incident is not responded appropriately. The value proposition for the Flagship 2 could be to understand the benefits of various well-integrated security controls that supports investigating an incident, train them to use them, and introduce the learners an example of an organisational environment that has such controls.

Bachelor's level cybersecurity students could benefit attending to either of the exercises operating the security controls, performing the technical investigation, and analysing the incident. The Flagship 1 contents could be used in Master's level studies, e.g. by students from various degree programs, e.g. cybersecurity, computer science, communications, law, business administration and management. They could jointly plan the cybersecurity incident response and mitigation plans and participate as a team into the exercise following plans they created. The learning outcomes could be to understand cybersecurity incidents and how an organisation could respond and mitigate them and what could be the appropriate level of details the plans should have. Being technical in nature, the Flagship 2 contents could be used by e.g. cybersecurity students,

to investigate and analyse the cybersecurity incidents, and propose improvements on how the incident could be prevented or made more costly to the attacker, and propose improvements to the deployed security controls.

The analyst activity could also be used in training and education. Those already in work-life, but thinking of moving to the field of cybersecurity could benefit from the entry-level contents by first learning the basic concepts that are presented in the activity and then participating to the analyst activity. A requirement is sufficients skills in English language, as the open-source analyst tools are natively in English. A tailored (self) study material about the concepts should be created. For the career changers, there should probably be support available during the activity to overcome any challenges and answer learners' questions. A digital forensic and investigation subject matter expert could provide the support.

In education, Bachelor and Master's students the contents of the analyst activity could be used to assess technical skills of the learners, being potentially suitable for cybersecurity and computer science students. The students could be asked to analyse and report the methods they used and the activities the threat actor(s) had performed. Would there need of using the analyst activity in the education, the Universities and education providers could collaborate by opening the analyst courses to external students, defined pass or fail criteria and award study credits to students. If opening the courses would not be an option, then the education providers could exchange the digital samples and support materials with each other, or buy them from a commercial provider, if such exists.

There is potential to use the contents of Flagship 1 and Flagship 2 in training and education, but in order to productise or commercialise the contents, some work is needed.

5.6 Future Improvements

The analyst activity in Flagship 2 was a solo work with no guidance nor support available to analyse the digital samples. It could be researched if assigning a red team (RT) specialist(s) to support the analysts would provide improved learning outcomes. A technological solution, e.g. an artificial intelligence based chat bot, for supporting the analysts learning and offloading RT specialist workload could be researched. A future research could study to the effects of various kinds of tips to analysts impact to e.g. correctness or analysis time. A common pre- and post-exercise and analyst activity survey pattern to measure the learning outcomes could be researched and studied.

The analysts were third parties, as the conductor had no contractual relationship with them. Sharing software vendor's binaries, or parts of them, with such third parties may explicitly be denied, or it can not be interprepted as allowed by the software licence. For training sessions, such as the analyst activity, software vendors could by default grant sharing snippets of the vendor binaries, configurations, and data to the learners and allow performing digital forensics activities on them, even reverse engineering. The shared artefacts could be in the form of files from disk images, network packet capture or memory dumps.

The Flagship CSE concept developed in CyberSec4Europe requires a team coach, who as an RT expert, has good knowledge about the exercise storyline, the technical exercise environment and threat actors tactics, techniques and procedures (TTPs). It could be researched and studied whether the team coach could be mimicked by a technological solution and to which extent. Using a technological solution to mimic or offload a team coach could help to scale the Flagship concept to mass-training of persons.

The analysts' challenge "Hard times, hard drives" had the lowest number of correct submissions. A future improvement would be to provide instructions on how to attach a disk image into a virtual machine.

For the technical support platform, a publically available hosted chat service that respects privacy and supports threaded discussions would be more valueable than the platform used in Flagship 2, which had no threaded discussions.

A future project could research the used CRTF technology or other emerging open-source technology with more participants and in more complex federation scenarios, which have been presented in the PART B of CyberSec4Europe 2021c.

Would there be need or demand to the utilise the Flagship 1 or Flagship 2 contents in education or training, some work needs to be done as discussed in the previous paragraph.

5.7 Conclusion

Flagship 2 was the second two-day, online-only cross border cybersecurity exercise utilising a cyber arena. The participants were from 10 European countries representing 13 CyberSec4Europe affiliates. Some of the participants had no previous experience in cyber security exercises or cyber arenas (or ranges), some of them were cyber security professionals, some were juniors, and some had only little hands-on experience in cyber security before the exercise. Some of the participants had participated into Flagship 1. The data from the Flagship 2 quick survey shows that 100% of the survey respondents (N=15) would recommend the exercise to their colleagues or friends and found it beneficial for them.

The Flagship 2 exercise and the analyst activity had contents that are in need in real-life organisations. The exercise participants investigated a possible cybersecurity incident and found the initial weakness that was exploited by a threat actor. With the acquired understanding of the situation, the exercise participants could suggest improvements of the security controls and training contents for the fictional organisation they were placed into.

Flagship 2 included an open entry-level cybersecurity analyst activity, where students, junior analysts and high-performing experts individually analysed samples exported from the exercise environment. They simulated a cybersecurity analyst service provider for the exercise. There were 61 registrants to the analyst activity, from three European countries. A total of 43 of the registrees submitted any findings. Based on the *in-situ* chat messages and concluded from the submission statistics and the time the analysts spent with the provided samples, there was demand for such event.

The implement Flagship 2 was a success.

6 References

BigBlueButton (2021, December 31). Big Blue Button. Retrieved January 30, 2022 from https://bigbluebutton.org/open-source-project/about/

CTFd. (2022, January 30). CTFd: The Easiest Capture the Flag Platform. Retrieved January 30, 2022 from https://ctfd.io/.

CyberSec4Europe. (2020a, December 30). D7.2 Virtual lab for open-source tools education and research. Retrieved January 30, 2022 from https://cybersec4europe.eu/wp-content/uploads/2021/01/D7.2-virtual_lab-v0.2_submitted.pdf.

CyberSec4Europe. (2020b, August 30). D7.1 Report on existing cyber ranges, requirements. Retrieved January 30, 2022 from https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf.

CyberSec4Europe (2021a, February 24). D6.4 Flagship 1. Retrieved January 30, 2022 from https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf.

CyberSec4Europe. (2021b, November 30). Flagship 1 Online Open Course. Retrieved January 30, 2022 from https://cs4e.pages.labranet.jamk.fi/ooc/.

CyberSec4Europe. (2021c, August 4). D7.3 Evaluation report on integration demonstration. Retrieved January 30, 2022 from https://cybersec4europe.eu/wp-content/uploads/2021/08/D7.3-Evaluation-report-on-integration-demonstration-v1.3_submitted.pdf.

CyberSec4Europe. (2021d, December 22). JAMK To Conduct Flagship 2: An Online Cybersecurity Exercise Activity. Retrieved Janurary 30, 2022 from https://cybersec4europe.eu/jamk-to-conduct-flagship-2-an-online-cybersecurity-exercise-activity/.

ECSO. (2020, March 30). Understanding Cyber Ranges: From Hype to Reality. Retrieved January 30, 2022, from https://ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf.

European Union. (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved 14.3.2022 from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Kauppalehti. (2022, January 2). Kuinka kyberhyökkäystä tutkitaan? Avoin harjoitus päästää kiinnostuneet kokeilemaan. Retrieved January 30, 20220 from https://www.kauppalehti.fi/uutiset/kuinka-kyberhyokkaysta-tutkitaan-avoin-harjoitus-paastaa-kiinnostuneet-kokeilemaan/437f4f6a-47b3-472a-9918-301283f171d8.

Masaryk University. (2022a, January 30). Cyber Sandbox Creator. Retrieved January 30, 2022 from https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator.

Masaryk University. (2022b, January 25). Flagship 2 Sandbox. Retrieved January 30, 2022 from https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox.

Mikrobitti. (2021, December 27). Jyväskylän ammattikorkeakoulun harjoitus päästää kiinnostuneet kokeilemaan kyberhyökkäyksen torjumista. Retrieved January 30, 2022 from https://www.mikrobitti.fi/uutiset/jyvaskylan-ammattikorkeakoulun-harjoitus-paastaa-kiinnostuneet-kokeilemaan-kyberhyokkayksen-torjumista/3a248add-ba95-4ab9-b462-27240c955bc0.

NIST. (2022, January 13). Glossary. Retrieved January 30, 2022 from https://csrc.nist.gov/glossary/term/Autonomous_System

The Hive Project. (2022, January 30). The Hive Project Home Page. Retrieved January 30 2022 from https://thehive-project.org/.

JYVSECTEC (2017, February 13). JYVSECTEC success story. Retrieved 15.3.2022 from https://jyvsectec.fi/2017/02/jyvsectec-success-story/

JYVSECTEC. (2021, December 21). Flagship 2 Event Page. Retrieved January 30 2022 from https://jyvsectec.fi/2021/12/flagship-2/.

JAMK. (2021, December 27). Flagship 2 Press Release (in Finnish). Retrieved January 30 2022 from https://www.epressi.com/tiedotteet/tietoturva/mita-kyberanalyytikko-tekee-kyberhyokkayksen-aikana-osallistu-avoimeen-kyberharjoitukseen-ja-kokeile.html.

Karjalainen M. and Kokkonen T. (2020). "Comprehensive Cyber Arena; The Next Generation Cyber Range," 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 11-16, doi: 10.1109/EuroSPW51379.2020.00011.

Talouselämä. (2022, January 2). Oletko aina halunnut tietää, mitä kyberanalyytikko tekee hyökkäyksen aikana? Retrieved January 30 2022 from https://www.talouselama.fi/uutiset/oletko-aina-halunnut-tietaa-mita-kyberanalyytikko-tekee-hyokkayksen-aikana-avoin-harjoitus-paastaa-kiinnostuneet-kokeilemaan/664c08ee-86bf-472c-9574-835a91e5ed67.

TIVI (2021 December 27). Mitä kyberanalyytikko tekee hyökkäyksen aikana? Retrieved January 30 2022 from https://www.tivi.fi/uutiset/tv/ff5473ce-c4f7-4ec5-b1b3-09342693080e.

Uusiteknologia. (2021 December 27). Tammikuussa järjestetään verkossa avoin kyberharjoitus. Retrieved January 30 2022 from https://www.uusiteknologia.fi/2021/12/27/tammikuussa-jarjestetaan-avoin-kyberharjoitus/.

YLE (2021 February 11). Hacked psychotherapy centre Vastaamo files for bankruptcy. Retrieved April 8 2022 from https://yle.fi/news/3-11785891.

Annex A: Concept Map of Flagship 2

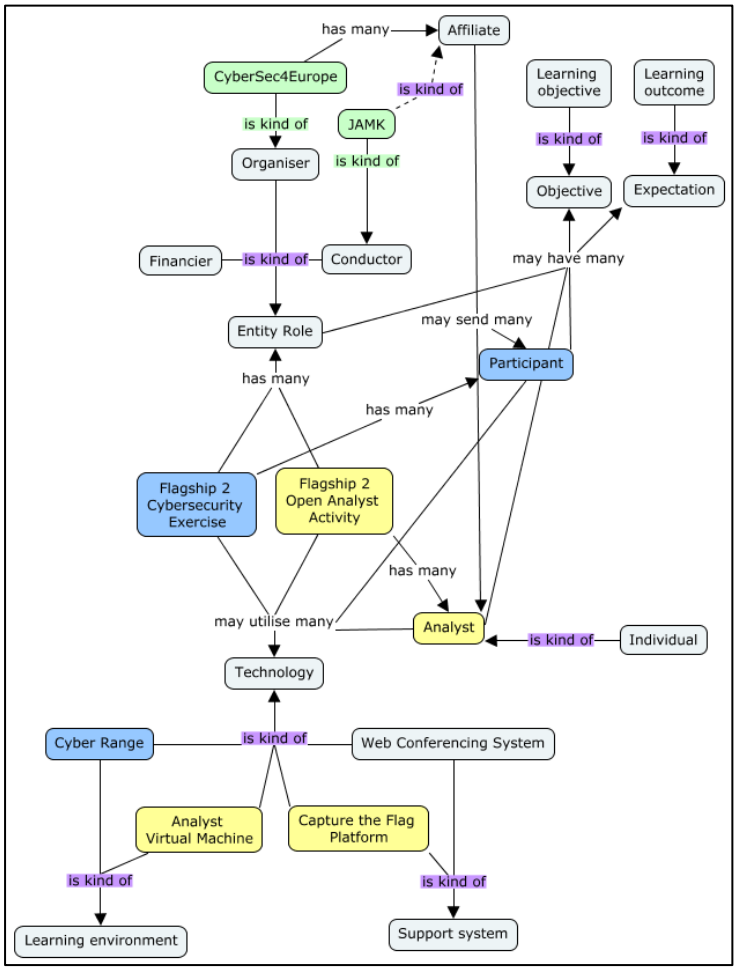
The figure below shows the concept map of the Flagship 2 event. The concepts (rectangles) are written in singular form. The concepts are linked together with a relationship (a line with an arrow). The concept map was created using CMapTools, available from https://cmap.ihmc.us/.

Color legend of concepts:

- Green is a concerete instance
- Blue is a exercise related concept
- Yellow is a analyst actitivy related concept
- Grey is a neutral concept, or a concept that is shared by both the exercise and analyst activity.

Color legend of relationships (lines between concepts)

- Green relationship describes an concrete instance of an concept
- Purple relationship describes an abstract instance of an concept
- White relationship describes cardinality the linked concepts have



Annex B: Subject Matter Questions from the Application Form

6. Self-evaluation: I believe that I have excellent knowledge and skills in...

Please evaluate your current knowledge (1: Strongly Disagree, 2: Disagree, 3: Undecided, 4:Agree, 5: Strongly Agree)

	1	2	3	4	5
Linux command line tools	◯	◯	◯	◯	◯
Open-source Cyber Security Analysis tools	◯	◯	◯	◯	◯
Cyber Kill Chain	◯	◯	◯	◯	◯
Reverse engineering	◯	◯	◯	◯	◯
Cyber Security Incident Management and Response (Communications or team lead role)	◯	◯	◯	◯	◯
Cyber Security Incident Management and Response (Leadership or managerial role)	◯	◯	◯	◯	◯
Cyber Security Incident Management and Response (Technical role)	◯	◯	◯	◯	◯
Threat hunting	◯	◯	◯	◯	◯
Networks and firewalls	◯	◯	◯	◯	◯
System administration	◯	◯	◯	◯	◯
EDRs and SIEMS	◯	◯	◯	◯	◯
Virtualbox or Vagrant virtualisation software	◯	◯	◯	◯	◯
Other, what	◯	◯	◯	◯	◯

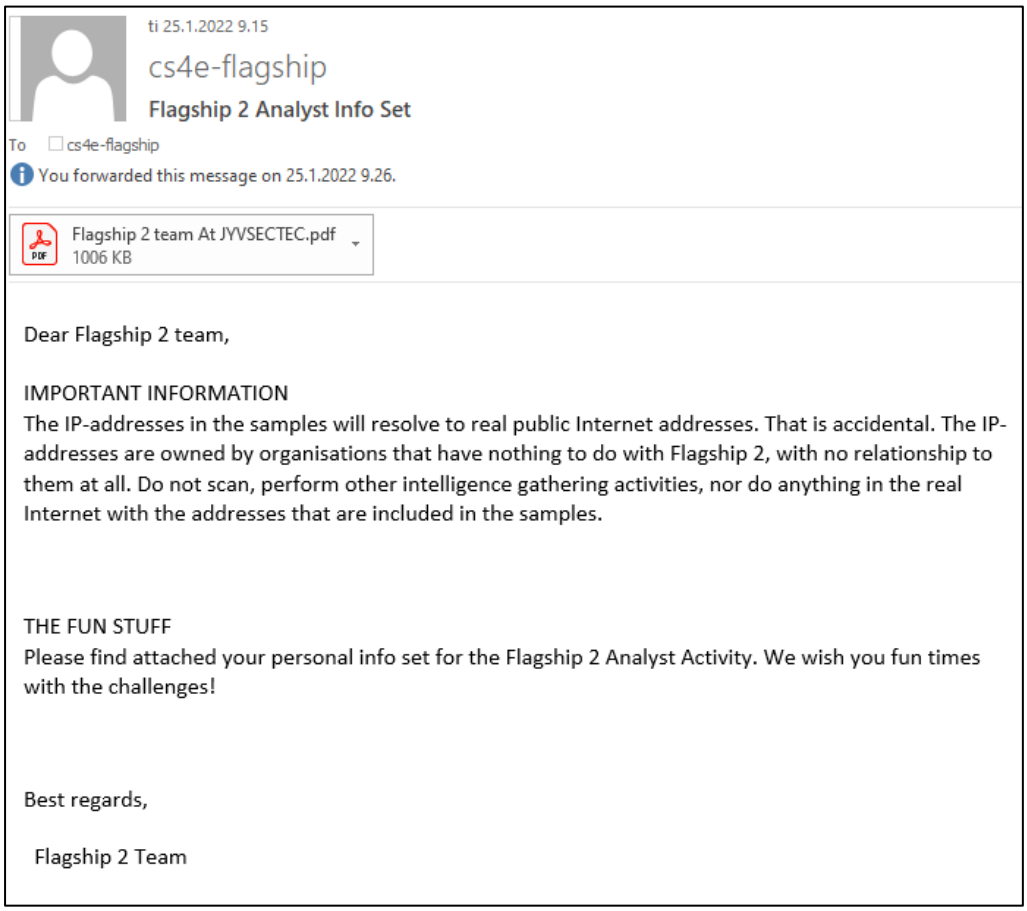
7. Previous experience of Cyber Security Excercises (CSE) and competitions *

- ☐ I participated to Flagship 1
- ☐ I have planned or participated to some other cybersecurity exercise
- ☐ I have planned or participated in a table top cybersecurity exercise
- ☐ I have planned or participated in a capture the flag
- ☐ I have no previous experience in cybersecurity exercises or capture the flags

Annex C: Analyst Cover Letter and Info Set

The recipient's name of the email and the Info Set in this annex is "Flagship 2 team at JYVSECTEC". All participants received a personalised cover letter and info set.

Cover Letter



ti 25.1.2022 9.15

cs4e-flagship

Flagship 2 Analyst Info Set

To cs4e-flagship

You forwarded this message on 25.1.2022 9.26.

Flagship 2 team At JYVSECTEC.pdf
1006 KB

Dear Flagship 2 team,

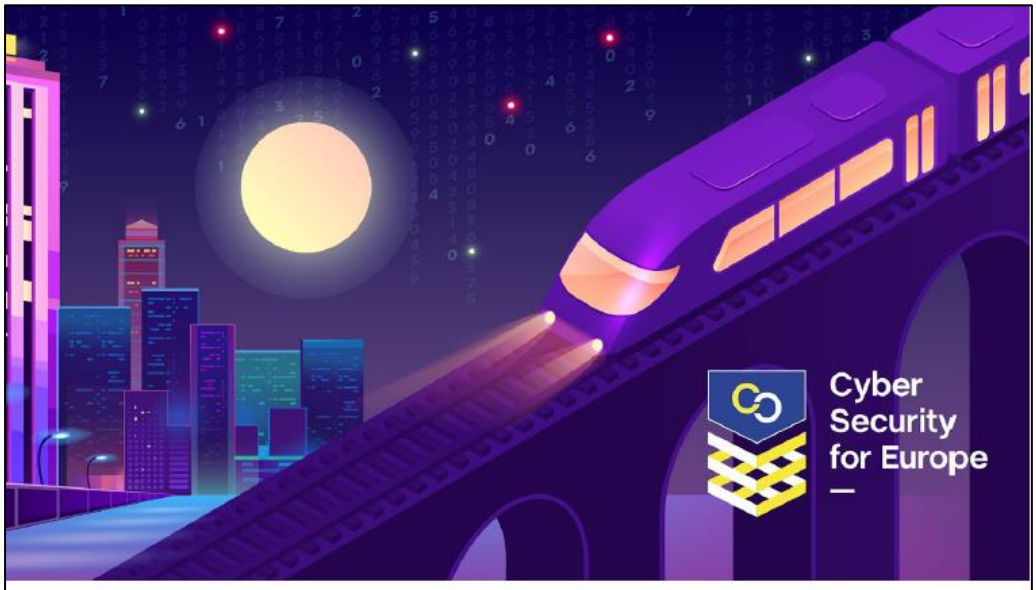
IMPORTANT INFORMATION
The IP-addresses in the samples will resolve to real public Internet addresses. That is accidental. The IP-addresses are owned by organisations that have nothing to do with Flagship 2, with no relationship to them at all. Do not scan, perform other intelligence gathering activities, nor do anything in the real Internet with the addresses that are included in the samples.

THE FUN STUFF
Please find attached your personal info set for the Flagship 2 Analyst Activity. We wish you fun times with the challenges!

Best regards,

Flagship 2 Team

Cover page



Flagship 2

Cybersecurity Analyst Activity Info Set

Offered by CyberSec4Europe

25 – 26 January 2022

CyberSec4Europe is funded by the European Union under the H2020 Programme
Grant Agreement No. 830929

Page 1 (Table of Contents)

Contents

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 2

0x01 Foreword

Dear Flagship 2 team,

Your cybersecurity analyst work is about to start. With your username and password, you can now access the samples that have been recorded from the exercise environment. The samples may have tracks or evidence of a cybersecurity incident that a fictional organisation faced. Besides the tracks, the samples may contain real malware or computer viruses. Therefore, you must only use the provided virtual machine to analyse them. If they are analysed in another environment, the malware may escape to your local network (*) or even the public Internet (*). Also, please do not share the samples with anyone who is not participating to Flagship 2 (*).

0x02 Important Note

The IP-addresses in the samples will resolve to real public Internet addresses. That is accidental. The IP-addresses are owned by organisations that have nothing to do with Flagship 2, with no relationship to them at all. Do not scan, perform other intelligence gathering activities, nor do anything in the real Internet with the addresses that are included in the samples (*).

0x03 About the Source Environment

The samples were recorded from an exercise environment called Realistic Global Cyber Environment (RGCE). It contains, besides other features, public IP-addresses. That means that the public IP-addresses used in the environment resolves to real hosts in the real Internet. But the IP-addresses in the real Internet have nothing to do with what is happening in RGCE or in the samples that you will soon have in your possession.

0x04 Analyst Workstation

Using the Analyst workstation

- The analyst workstation is connected to the Internet.
- Use the analyst workstation to download the samples from the provided URL and analyse them. Do not handle the samples outside the Analyst workstation! (*) The samples may contain real malware or computer viruses that are meant to live in the workstation only.
- The download URL is on the real Internet, please do not hack it, thanks :) (*)

Provisioning the analyst workstation

Please follow the instructions at https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox to provision the analyst workstation on your device. First time setup of the environment might take from 10 minutes up to an hour, depending on your Internet connection speed. Be sure the provision the environment well in advance before the exercise.

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 3

0x05 The Analyst Workflow

You can analyse the samples (challenges) in the order you wish. Due to the nature of the Flagship 2 exercise, all samples (challenges) are immediately available for download and analysis, once the download URL is published. As analysts provide findings (flags), the exercise participants get information for their investigations.

The analyst workstation nor the URLs therein are not targets for analysts. Do not hack them (*) but resolve the samples that you will soon download.

0x06 (*) The Asterisk

If, for whatever reason, you behave contrary to the information we have provided you with, you are most probably breaking the law(s) applicable in your place of residence. Please, do not take that that risk ❤

0x07 Analyst Schedule

DAY 1 - 25th January 2022

- 08:00 (CET) Usernames and URLS delivered via email
  - Usernames, passwords and URL for downloading samples and report findings delivered.
  - Technical support channel URL for analyst workstation is delivered
  - Note: We don't mind if you decide to use the technical support platform as a peer-support, asking and providing support for your peers.
- 08:00 (CET) All samples available for download
  - You may download the samples (challenges) and report your findings (flags) in any order
  - Note: If you are doing a team effort you must figure out yourself which real-time collaboration tool you will use, if any.
- 08:03 (CET) Analyst work begins
  - You can start working with the samples (challenges) and report your findings (flags) to the service where you downloaded the samples
  - Due to the nature of the Flagship 2 exercise, all samples are immediately available for download and analysis, once the download URL is published.
  - Depending on the reporting speed of the analysts, their findings will be provided to the exercise participants.
- 08:03 onwards
  - Perform analyst work at your own pace.

The Flagship 2 exercise that you will be supporting starts at 09:00 (CET). The first exercise day activity ends at 14:00 (CET). You may continue your analyst work beyond this schedule.

DAY 2 - 26th January 2022

- After good night's sleep, perform analyst work at your own pace.
- 14:00 (CET) Flagship 2 ends
  - The exercise no longer uses the provided findings (flags).
  - The service used to download the samples and report analyst findings may be accessible for a short period after the exercise. It might be taken offline without further notice.

The second exercise day starts at 09:00 (CET), and ends at 14:00 (CET).

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 4

0x08 Frequently Asked Questions (FAQ)

Q: How long are the samples download and findings reporting URL available?

A: We can guarantee that they will be available from 25 January 2022 07:00 CET to 26 January 2022 14:00 CET. It may be the case that the URL will remain available for a short period after the exercise, but they might be taken down without further notice.

Q: I have problems with the analyst workstation. Help me?

A: Please see the next Q&A.

Q: Can I get peer support somewhere, other than <insert your favourite search engine here>?

A: There is technical support for the analyst workstation available at https://bbb.tbm.tudelft.nl/b/jan-gb3-27q-bwf. A CyberSec4Europe partner, TUDelft (https://www.tudelft.nl/en/), hosts the service. We do not mind if you happen to use that as a peer-support platform to ask and provide support for your peers on working with the samples.

Q: Where are the samples (challenges), and where to report the findings (flags)?

A: Access the URL only from your analyst workstation (*). Do not hack it (*). The URL is https://ctf.jyvsectec.fi. If there are new sample download URLs, do not hack them either (*).

Q: What are my username and password?

A:

Name	Username	Password
Flagship 2 team At JYVSECTEC	example	example

Q: There is a black screen on the analyst virtual machine. What can I do?

A: When you are about to stop for the day, please shutdown the analyst virtual machine. There is a hibernate issue which we could not resolve. If you forgot to shut down the virtual machine, before a good night's sleep, you will face a black screen in the following morning. Unfortunately, the black screen sticks like a gum in one's hair. If you face the black screen, you must reboot the analyst virtual machine.

Q: I am a full time student. How many credits it is possible to gain by solving some or all of the challenges?

A: Unfortunately, we at JAMK / JYVSECTEC cannot give you any study credits.

0xFF Raising awareness

Q: Tell me about the analyst workstation?

A: The analyst workstation was created by a CyberSec4Europe partner, Masaryk University, Czech Republic (https://www.muni.cz/en). They used the Cyber Sandbox Creator (CSC) to orchestrate it for you. If you want to know more about the concepts behind the analyst workstation, please see https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator.

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 5

Q: Where were the samples recorded?

A: The samples were recorded from a cyber arena, RGCE. It is planned, developed and operated by JYVSECTEC. JYVSECTEC (Jyväskylä Security Technology) is a cyber security, data analytics and artificial intelligence research, development and training centre located in the Institute of Information Technology at JAMK University of Applied Sciences, Finland. There is a whitepaper available describing RGCE in more detail at https://jyvsectec.fi/rgce.

Q: What is a cyber arena?

A: It is a realistic large-scale technical environment for researching, developing, and training complex cybersecurity phenomena. For more information, please see https://jyvsectec.fi/2020/10/comprehensive-cyber-arena-the-next-generation-cyber-range/.

Q: What is CyberSec4Europe anyways?

A: CyberSec4Europe is one of four pilot projects funded by the EU under the H2020 programme. CyberSec4Europe's 43 partners, from 22 EU Member States and Associated Countries, are addressing key cybersecurity domains, critical technology/application elements and several key vertical sectors, including finance, education, smart cities, healthcare, supply chain and maritime transport.

Q: Err..?

A: CyberSec4Europe's long-term goal and vision are of a European Union that has all the capabilities required to secure and maintain a healthy democratic society, living according to European constitutional values, with regard to, for example, privacy and data sharing, and being a world-leading digital economy.

Better that you check out the About page yourself!

Q: What has CyberSec4Europe accomplished?

A: Well, if by accomplishing you meant

- Project deliverables
- Scientific publications
- Recommendations
- Project web pages
- Project social media presence, please @CyberSec4Europe in Twitter and CyberSec4Europe in LinkedIn

If you wish to have more info, please get in touch with the project through the social media accounts or by using the contact form.

Q: This is Flagship 2. Was there Flagship 1?

A: : Flagship 1 was conducted in January 2021. It was a cybersecurity exercise targeted at CyberSec4Europe partners. That too utilised RGCE, a cyber arena. There were several roles for participants: team lead, PR and communications specialist, network specialist, system administrator, cybersecurity specialist, cyber incident analyst. Someone had to deal with GDPR topics, too. Some relevant archived pages:

- https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/
- https://www.jamk.fi/en/Event-Calendar/arkisto2/flagship-cybersecurity-event/flagship-event/

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 6

We also prepared an open online course for the Flagship 1 attendees: https://cs4e.pages.labranet.jamk.fi/ooc/, but it is now archived., If you wish find out more about Flagship 1, please take a look at deliverable, D6.4 Flagship 1: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf.

Q: Why can't non-CyberSec4Europe related people participate in the Flagship exercises?

A: The conductor (JAMK) has limited resources to offer the Flagship cybersecurity exercises. By focusing on CyberSec4Europe partners, we hope to spread the idea that cyber ranges and arenas could be used to train individuals and teams with no shared background on cybersecurity phenomenon in a safe environment and in a supportive way. Also, we hope that by extrapolating the concept to single organisation's or company's representatives, the organisation or company can benefit from trainings and exercises held in a cyber arena.

Q: What is out there regarding to Flagship 2?

A: Some deliverables, i.e. documents are in the writing at the time of publishing this document, but something that exists is re-used or re-applied. Please find the following deliverables:

- **Deliverable D7.1: Report on Existing Cyber Ranges, Requirements,** https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf. Requirements from Part B are implemented to provide connectivity for the exercise participants to the exercise environment (RGCE).
- **Deliverable D7.2: Virtual Lab for Open Source Tools Education and Research,** https://cybersec4europe.eu/wp-content/uploads/2021/01/D7.2-virtual_lab-v0.2_submitted.pdf. The deliverable presents the requirements for Cyber Sandbox Creator, a tool for creating open-source, portable, and lightweight virtual labs for cybersecurity education, testing, and certification.
- **Deliverable D7.3: Evaluation Report on Integration Demonstration,** https://cybersec4europe.eu/wp-content/uploads/2021/08/D7.3-Evaluation-report-on-integration-demonstration-v1.3_submitted.pdf. The deliverable is an evaluation report of the implemented requirements documented in D7.1 PART B.

Web pages that directly relate to Flagship 2:

- https://cybersec4europe.eu/jamk-to-conduct-flagship-2-an-online-cybersecurity-exercise-activity/
- https://jyvsectec.fi/flagship

Q: Who conducts the analyst activity that I am now participating?

A: It is conducted in CyberSec4Europe by JAMK University of Applied Sciences, Finland

Q: All this sounds interesting. What are the social media accounts I could follow?

A: There a few social media accounts to follow.

CyberSec4Europe

- @CyberSec4Europe in Twitter
- CyberSec4Europe in LinkedIN

JYVSECTEC

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Page 7

- @JYVSECTEC in Twitter
- JYVSECTEC in LinkedIN

Masaryk University's Cybersecurity Laboratory

- @cybersecmuni in Twitter
- csirt-mu in LinkedIN

ECSO - European Cyber Security Organisation

Although ECSO is not part of the CyberSec4Europe, we do co-operation and want to raise awareness of their existence and the good and important work that they, too, do for the European cybersecurity.

- ecso-cyber-security in LinkedIN
- @ecso_eu in Twitter

CyberSec4Europe is funded by the European Union
under the H2020 Programme
Grant Agreement No. 830929

Annex D: Chat Log from the Analyst Technical Support Platform

This annex contains the chat log of the analyst activity technical support platform. Usernames have been anonymised.

========= **DAY 1** =========

Conductor representative

9:34 AM

Good morning all! Are you able to access the ctf platform and see the challenges there?

Participant 1

9:39 AM

Good morning

Participant 1

9:39 AM

yes

Conductor representative

9:39 AM

Excellent!

Participant 1

9:50 AM

Platform seems to work just fine and the challenges open nicely! Just had a small problem with the Kali linux keyboard layout. :)

Analyst workstation technical support representative

9:51 AM

Hi <participant 1>, thanks for the report! What kind of problem with the keyboard did you have? And did you manage to fix it or is it still an issue?

Participant 1

9:54 AM

I didn't realize it was set to US english as default. Some special characters are quite different between it and Finnish layout. I was able to change it, but the xfce keyboard switcher didn't work right away. Tiny bit of

googling revealed that this is some sort of a Kali issue. Switching the toggle "use system defaults" on and off did the trick and now I have Finnish layout.

Analyst workstation technical support representative

9:56 AM

Oh, I see. The sandbox readme also includes a way to change the keyboard, did you miss this info or did it not work for you?

https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox#change-the-keyboard-layout-in-kali

Participant 1

9:58 AM

I missed that part of the document. Sorry about that.

Analyst workstation technical support representative

9:58 AM

No problem, good that you found an alternative solution :)

Participant 2

12:09 PM

here´s a dumb question since i seem to be derping... what are the kali credentials?

Analyst workstation technical support representative

12:09 PM

It's: kali /// kali

Participant 2

12:09 PM

see when it´s too easy...

Analyst workstation technical support representative

12:09 PM

See also step 4 in the 1st section: https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox#1-setup-instructions

Participant 3

12:23 PM

FWIW, I had some issues with the disk filling up in the "Hard times, hard drives" forensics challenge but resizing the disk was fairly straightforward with these instructions: https://stackoverflow.com/questions/49822594/vagrant-how-to-specify-the-disk-size/60185312#60185312 (the plugin check part can be skipped, and the 'config.disksize.size' should be 'device.disksize.size' and under 'config.vm.define "kali"' since we are not changing the global parameter)

Analyst workstation technical support representative

12:32 PM

Thanks! I will add this info to the sandbox readme so that others can use it as well

Participant 4

12:37 PM

Without giving too many spoilers, is there a way to run vba scripts (or part of them) in the test enviroment?

We're are looking at the shell command in The dirty document but since its encrypted we dont actually know what the name of the command is.

Analyst workstation technical support representative

12:44 PM

Hmm, not sure since I did not prepare the challenges. I have notified <conductor>. In the meantime, maybe this might help? https://stackoverflow.com/questions/29028381/how-to-run-a-vba-macro-on-linux-machine (Though I doubt that installing new tools should be needed to complete the challenges, there should be another way)

Conductor representative

12:51 PM

Well, the idea is to decrypt the encryption, but not to run a potential malware...

Participant 4

12:56 PM

Fair point, its just that our decrypting attemps havent been that succesful. But I quess we just need to keep trying.

Conductor representative

1:02 PM

If executing a vba macro is needed, then Wine could be one approach, one could be LibreOffice. May be there are others too, who knows...

Conductor representative

2:04 PM

If you need technical assistance with the environment, you may ask it here in public or in a private chat with <technical support representative>. Public is preferred, as others may have the same issue and it helps them to know about the issue and its resolution

Participant 4

2:15 PM

Volatility plugins (or most of them) crash with this kind of error:

Unable to validate the plugin requirements: ['plugins.Maps.kernel']

Is there something I could do with this?

Conductor representative

2:23 PM

It may have permission problem...

Try sudo chown kali:kali -R /home/kali/Desktop/Volatility

Participant 5

2:50 PM

Do we get any more challenges when the event progresses?

Participant 5

2:51 PM

Volatility issues are most likely related to missing symbols.

Participant 6

2:52 PM

Hey, any problems with insufficient hard disk memory? Can't extract the other forensic package since me and a colleague dont have enough.

Conductor representative

2:52 PM

All the challenges are available from the ctf services, so no new challenges for you :)

Participant 5

2:52 PM

I see. This was fun, great distraction from daily work routines. Thank you very much from this opprotunity. 👆

Conductor representative

2:53 PM

You're most welcome! It was to fun to create

Analyst workstation technical support representative

2:53 PM

@Participant 6 Try this: https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox#increase-the-disk-size-in-kali

Participant 5

2:53 PM

There seems to be multiple mentions about the disk size, I personally feel like the fastest fix was to create additional 80gb virtual hard disk and mount it as /data into kali.

Analyst workstation technical support representative

2:54 PM

@Participant 5 This is a good solution as well

========= **DAY 2** =========

Analyst workstation technical support representative

9:26 AM

Hi, did you first install the plugin via vagrant plugin install vagrant-disksize?

Participant 6

10:01 AM

any help with the disksize issue?

Participant 6

10:01 AM

oh sorry, I didnt see you comment!

Participant 6

10:02 AM

no I did not, and that of course must be it.. :D thank you

Analyst workstation technical support representative

10:44 AM

Ok awesome! No problem

Participant 6

10:51 AM

in the instructions it says SSH to vagrant box -> now Im unsure about this. which is the host name I should use?

Analyst workstation technical support representative

10:57 AM

Do you mean in the step 4. here? https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox#1-setup-instructions The SSH connection is an alternative solution in case the GUI login does not work for you. However, via SSH, you won't be able to use certain analytical tools that only have a graphical interface. Did you have any issues with the primary way of logging in (the first bullet point in step 4)?

Participant 6

11:24 AM

no sorry, I mean in step 3. https://stackoverflow.com/questions/49822594/vagrant-how-to-specify-the-disk-size/60185312#60185312

in increasing disk size

Analyst workstation technical support representative

11:43 AM

vagrant ssh kali

Participant 6

12:47 PM

I keep getting "Unsatisfied requirement plugins.Info.kernel: Windows kernel

Unable to validate the plugin requirements: ['plugins.Info.kernel']

Analyst workstation technical support representative

1:01 PM

This seems like an issue directly with Volatility (https://github.com/volatilityfoundation/volatility3/issues/427), not with the sandbox itself. I'm unfortunately not familiar with troubleshooting Volatility, maybe <conductor> or someone from JAMK could help?

Conductor representative

1:02 PM

yesterday there were peer comments related to Volatility:

https://github.com/volatilityfoundation/volatility3#symbol-tables

Conductor representative

1:04 PM

Volatility may have also a permission problem. which could be solved by issuing sudo chown kali:kali -R /home/kali/Desktop/Volatility

Participant 6

1:30 PM

No luck with the permissions.

Participant 6

1:30 PM

or the symbols, they were moved in to the folder.

Conductor representative

1:41 PM

umm... does this peer-comment help? https://volatility3.readthedocs.io/en/latest/symbol-tables.html

Participant 7

2:17 PM

I've managed to capture all the flags by now, but there were two exercises where the tools were various tools were not behaving as expected. First, the cincan/volatility was not able to dump the process tree of the memory exercise, no matter what I did; not even after I used the proprietary VMware tool to convert that dump to a more standard dump. When I _finally_ understood that I'll have to use Volatility 3 instead, I solved it in minutes.

Likewise with the ransomware exercise: I installed PE Tree – a really nice Python module for exploring PEs, but it failed to extract the bitmap resource in a readable format. When, as a last resort, I fed the binary to cincan/manalyze, it did the job properly and I got the flag. Still, I've no idea why. How does it differ from saving the RT_BITMAP (0x000140a0) with PE Tree or extracting the resources with the Pefile (github.com/folbricht/pefile) Go tool, both of which created a file that was recognisable as DIB with file, but not presentable with any image viewer? I wish to understand that!

Participant 8

3:41 PM

Thank for making this exercise! I had fun. Couldn't focus while working enough but managed to solve everything :) Thanks!

Conductor representative

3:41 PM

Thanks!

I hope that you have had balance with the difficulty and easiness of the samples

Conductor representative

3:41 PM

Hi! The flagship 2 exercise has come to an end, and will no longer utilise provided findings.

Conductor representative

3:45 PM

However, you may still continue to work with the samples (challenges)

Participant 9

5:39 PM

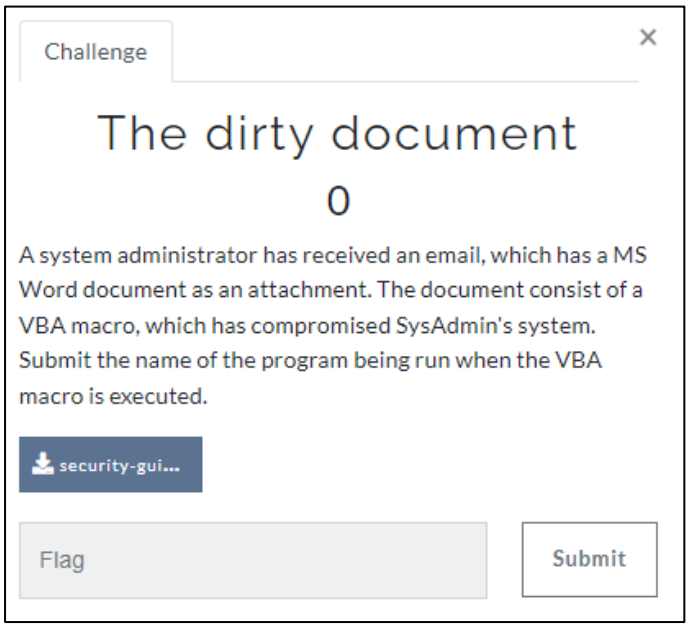
Hi, Thanks. This was fun! Over and out!

Annex E: Analyst Challenges

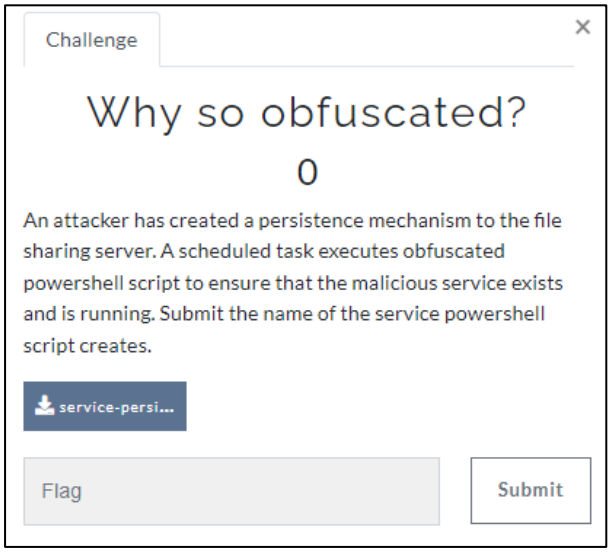
List of challenges and challenge categories

ID	Name	Category	Value	Type	State
10	The dirty document	Miscellaneous	0	standard	visible
11	Oh no! My system is locked	Reverse engineering	0	standard	visible
12	Evil in the wire	Packet analysis	0	standard	visible
13	What is wrong with my memory?	Forensics	0	standard	visible
14	Hard times, hard drives	Forensics	0	standard	visible
15	Why so obfuscated?	Miscellaneous	0	standard	visible

Challenge “The Dirty Document”

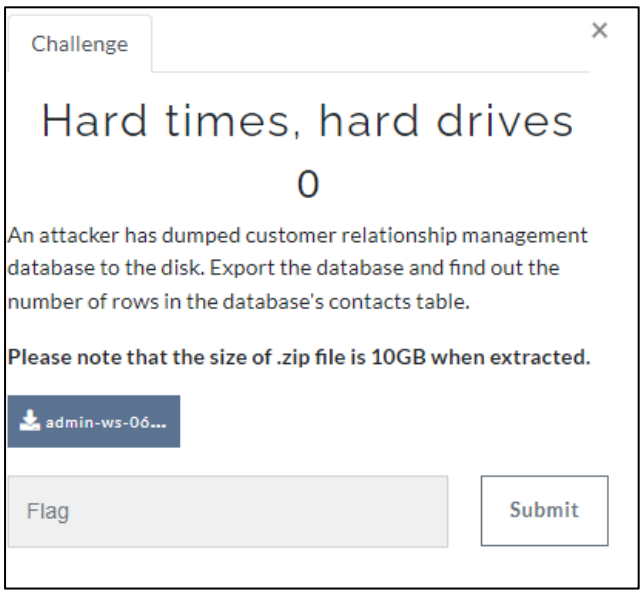


Challenge "Why so obfuscated?"

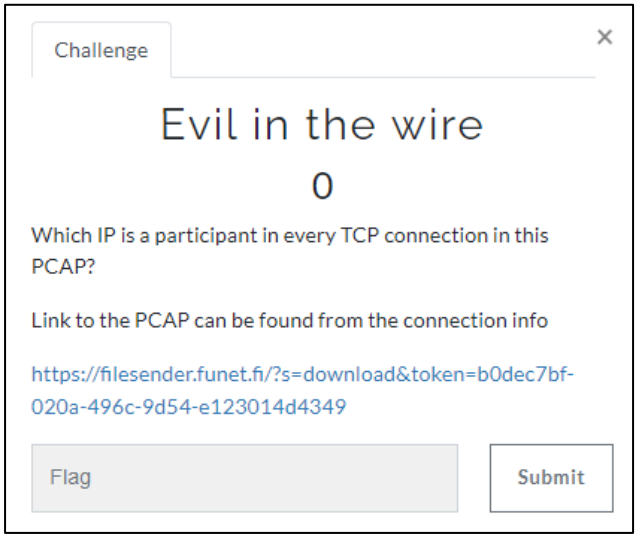


Challenge "What is wrong with my memory?"

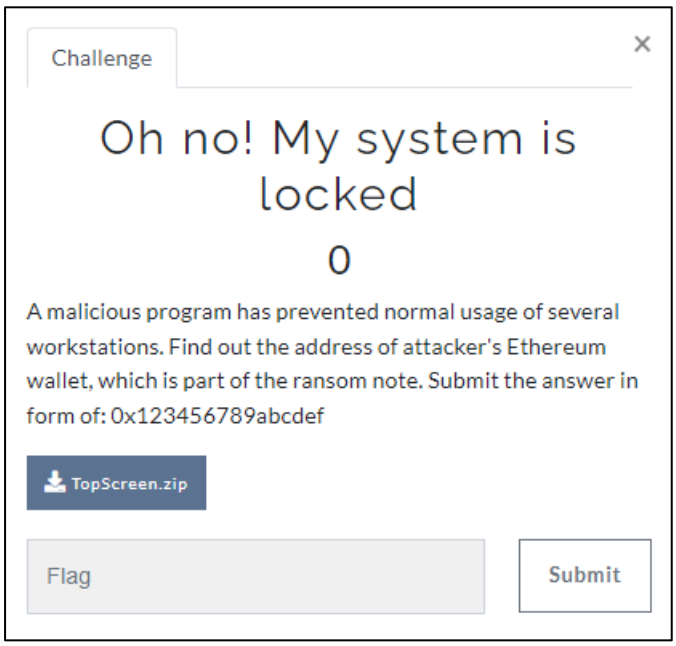
Challenge "Hard times, hard drives"



Challenge "Evil in the wire"



Challenge "Oh no! My system is locked"



Annex F: Analyst Activity Submission Statistics

The table below contains only the entries with one or more correct submissions. In total five rows having zero correct submissions were removed, totalling 31 removed incorrect submissions.

Total Ratio (correct: incorrect)	No. Registered persons	No. Correct submissions	No. Incorrect submissions	Total submissions	Shortest time between first and last submission
1 : 1	1	1	1	2	0:00:22
1 : 0	1	1	0	1	0:00:00
2 : 17	1	2	17	19	21:14:29
2 : 2	1	2	2	4	20:26:43
2 : 0	2	2	0	4	0:04:35
3 : 19	1	3	19	22	4:39:30
3 : 0	1	3	0	3	1:08:05
4 : 20	1	4	20	24	29:39:03
4 : 8	2	4	8	24	5:57:22
4 : 6	1	4	6	10	3:19:12
4 : 1	1	4	1	5	10:13:59
5 : 96	1	5	96	101	29:07:22
5 : 22	1	5	22	27	20:49:27
5 : 21	1	5	21	26	26:33:18
5 : 2	3	5	2	21	20:36:38
5 : 0	1	5	0	5	27:37:16
6 : 15	1	6	15	21	24:20:18
6 : 9	1	6	9	15	26:25:24
6 : 8	1	6	8	14	25:48:58
6 : 7	1	6	7	13	27:34:17
6 : 5	2	6	5	22	24:39:20
6 : 4	3	6	4	30	4:23:06
6 : 3	3	6	3	27	26:02:03
6 : 2	4	6	2	32	2:49:49
6 : 1	1	6	1	7	15:50:52
6 : 0	2	6	0	12	3:00:28
Total	**39**	**115**	**269**	**491**	

Annex G: Marketing Letter to CyberSec4Europe Affiliates

To: CyberSec4Europe (CyberSec4Europe@dlist.server.uni-frankfurt.de) <CyberSec4Europe@dlist.server.uni-frankfurt.de>
Cc: CyberSec4Europe@m-chair.de
Subject: D6.5 Flagship 2, two parallel tracks - Registration opens Tue 21 December 2021

Dear CyberSec4Europe colleagues,

We welcome you to an online two-day learning opportunity, Flagship 2. This time the event has two tracks: a Cyber Security Exercise targeted at CyberSec4Europe partners, and an open Capture the Flag (CTF). The two-day events are held in **25th – 26th January 2022.** The exercise is scheduled for both days between 10–15 CET.

Detailed expectations for participants are attached with this email, highlights are listed below.

FlagShip 2 cybersecurity exercise:

- FlagShip 2 is an online-only accessible cybersecurity exercise intended for CyberSec4Europe partners
- As this is a learning opportunity, the level of expertise is relaxed
- Previous experience in cyber security exercises or CTFs is not required
- Interest to technical issues, hands-on tool usage and knowledge of common cyber security terms and concepts is a plus
- By joining, you will be assigned to a fictional organisation with an exercise work role, which will be a technical role
- We ask that at least two employees from each organisation applies
    - We have reserved one seat for each partner organisation
    - If there are seats available, they can be filled with queuing participants
    - The event conductor will place the participants into teams
- Flagship 2 is a WP6 deliverable

What you can expect from the Flagship 2 cybersecurity exercise?
Flagship 2 is a continuum of Flagship 1. In the Flagship 1 an organisation faced a cyber incident. The case was fully resolved and properly responded. Or was it after all? Could it be that the attacker used that organisation as a stepping stone to gain access another organisation's networks? It could be that something new is at stake at this time…

Analysing a cyber security incident requires technical skills. Together with a team and a dedicated team coach, you will be able to analyse the case. As this is a learning opportunity, the level of expertise is relaxed. You will be assigned a technical work role in a fictional organisation, and you will have colleagues from the consortium learning how to analyse a detected cybersecurity incident.

Flagship 2 open capture the flag (CTF)

- Registered participants of the open CTF will receive samples that are exported from the exercise environment
- The participants should analyse the samples and report their findings
- The findings may be used by the exercise
- Analysts will use a virtualised analyst platform, created in CyberSec4Europe by BRNO in WP7
- Participating to the open CTF requires previous Linux command line tools experience
- Persons must be 18 years or older when registering

Where to apply or register?
The exercise application form and the registration form for the capture the flag will be open from 21st December 2021 to 12th January 2022.

Questions?
Please send your questions, comments or concerns to cs4e-flagship@jamk.fi. The Flagship management team will reply to you as soon as possible.

We look forward to meet you online at January 2022!

On behalf of the FlagShip 2 team,

Annex H: Registration Statistics

Registrees per Affiliation

Participants not affiliated with CyberSec4Europe are counted in the "—Other" affiliate.

Number	Affiliate	Total	Registered to Analysts Activity	Registered to Exercise
1	ABI -- ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA	1	-	1
2	ATOS -- ATOS SPAIN SA	1	-	1
3	CNR -- CONSIGLIO NAZIONALE DELLE RICERCHE	1	-	1
4	CYBER -- CYBERNETICA AS	1	-	1
5	FORTH -- FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	1	-	1
6	GUF -- JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN	2	-	2
7	KAU -- KARLSTADS UNIVERSITET	3	-	3
8	NTNU -- NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET	1	-	1
9	SIE -- SIEMENS AKTIENGESELLSCHAFT	1	-	1
10	TDL -- TRUST IN DIGITAL LIFE	1	-	1
11	UM -- UNIVERZA V MARIBORU	2	-	2
12	UNILU -- UNIVERSITE DU LUXEMBOURG	1	-	1
13	UNITN -- UNIVERSITA DEGLI STUDI DI TRENTO	4	1	3
14	VTT -- Teknologian tutkimuskeskus VTT Oy	2	-	2
15	-- Other	60	60	-
Total	15	82	61	21

Registrees per Countries

		TOTAL		Registered to Analysts Activity		Registered to Exercise	
		No. Persons	% Total	No. Persons	% Analysts	No. Persons	%
Country	Finland	61	74 %	59	97 %	2	10 %
	Greece	1	1 %	0	0 %	1	5 %
	Germany	3	4 %	0	0 %	3	14 %
	Sweden	3	4 %	0	0 %	3	14 %
	Romania	1	1 %	1	2 %	0	0 %
	Slovenia	2	2 %	0	0 %	2	10 %
	Italy	6	7 %	1	2 %	5	24 %
	Estonia	1	1 %	0	0 %	1	5 %
	Norway	1	1 %	0	0 %	1	5 %
	Spain	1	1 %	0	0 %	1	5 %
	Luxembourg	1	1 %	0	0 %	1	5 %
	United Kingdom	1	1 %	0	0 %	1	5 %
TOTAL	12	82	100 %	61	74 %	21	26 %

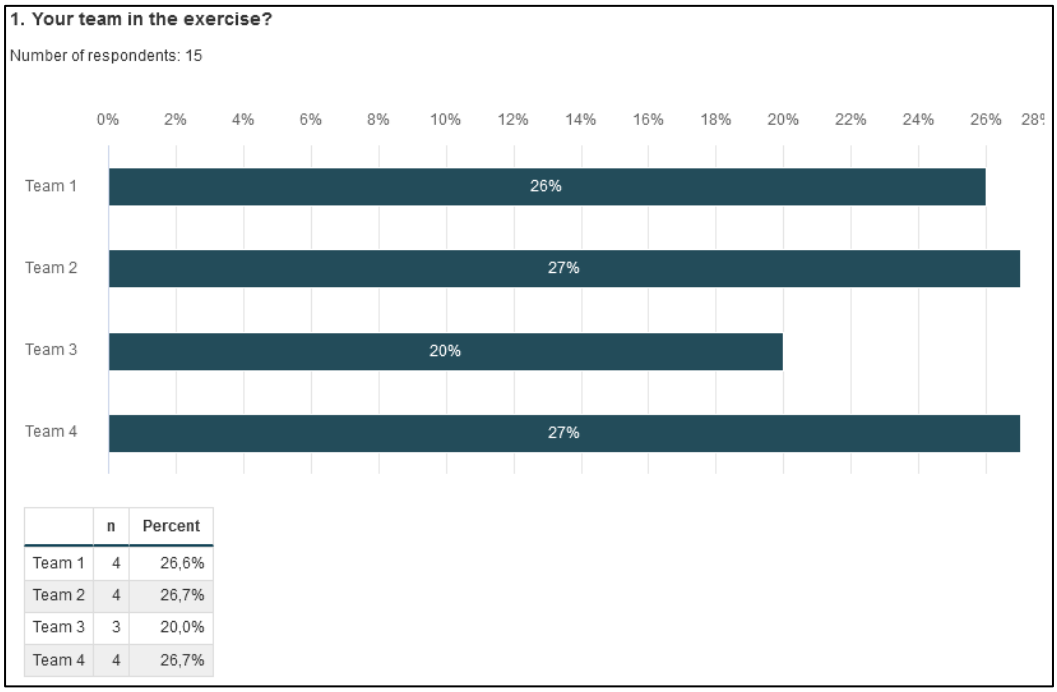
Gender distribution of registrees

		TOTAL		Registered to Analysts Activity		Registered to Exercise	
		No. Persons	% Total	No. Persons	% Analysts	No. Persons	% Participants
Gender	Female	11	13 %	6	10 %	5	24 %
	Male	69	84 %	53	87 %	16	76 %
	I prefer not to answer	2	2 %	2	3 %	0	0 %
	TOTAL	82	100 %	61	74 %	21	26 %

Annex I: Short Survey to Participants

A short survey after the exercise active phase, but before the feedback discussion was offereded to the participants. Some texts are covered to protect person names or other potentially sensitive information.

Respondent's team in the exercise



	n	Percent
Team 1	4	26,6%
Team 2	4	26,7%
Team 3	3	20,0%
Team 4	4	26,7%

What are your feelings now?

2. What are your feelings now?

Number of respondents: 13

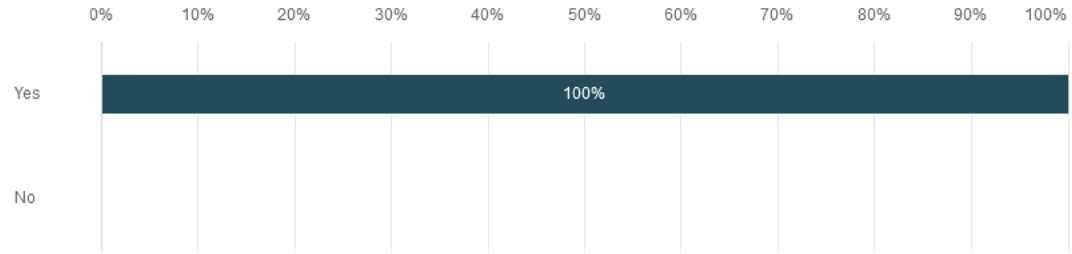
Showing 13 out of 13 responses Show less **or see all text answers in** Word **or** PDF

	Responses
	Very happy that I decided to participate. Coach was very helpful, watched that the team was following the scope and everyone would understand what is happening. Also great teamwork, everyone in team was interested to understand what is happening.
	Very pleased! A good first cyber exercise experience for me.
	very good, I had a great time, had a lot of fun, and learned so much. Thanks for managing everything smoothly.
	I'm truly impressed with the environment used. As a participant with little knowledge on cybersecurity operations it was a great learning experience to see the various tools that are used and how cybersecurity specialists would go about investigating the attack. Excellent impression overall.
	I am really happy that I joined the exercise.
	I am very happy and pleased
	It was a fun exercise, I am happy that I participated.
	really excited about the Flagship event. learned a ton. Really looking forward a new (physical) event.
	Very good. I learned a lot. I'm interested to learn more.
	- Happy - Excellent exercise and cyber-range
	Even though the technical nature of the exercise surprised me, I feel that there was really good development from Flagship 1.
	Sad... I have to go back to work. Overall, I think we were in over our heads and it would take us considerably longer to do anything without [redacted]. But because of that, we probably learned more (or at least seen more new things) than the other teams.
	Fine

Did you find the exercise beneficial for you?

3. Did you find the exercise beneficial for you

Number of respondents: 15



	n	Percent
Yes	15	100,0%
No	0	0,0%

If yes, please describe how.

4. Please describe how?

Number of respondents: 13

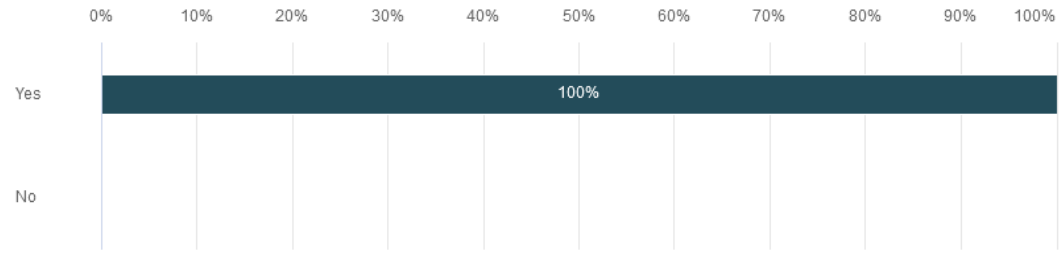
Showing 13 out of 13 responses Show less or see all text answers in Word or PDF

	Responses
▼	New skills, learned more to analyze a cyber attack.
▼	Got more insight into how a blue team works, and how some logging tools work.
▼	Learned a lot about cybersecurity operations
▼	This helped me understand the requirements for logging/siem systems.
▼	I learned new things and spent my time constructively
▼	It was good to do some more practical things again.
▼	I had basic knowledge of cyber attacks and possible related investigations but this guided event allowed me understand the big(ger) picture.
▼	Exposure to tools and IT/OT environment resembling real life.
▼	It's the first time that I have participated in a cybersecurity exercise and it was very interesting and engaging. Special thanks to our coach who guided us really well through the exercise.
▼	Flagship 1 gave me a good idea about what "real" cyber exercises are about and Flagship 2 increased my interest towards them even more. In addition the exercise gave me at least a general insight on what the technical people face after a cyber attack, which helps me conduct research and perhaps even help them in their work.
▼	gained some insight on how these breach investigations could be done
▼	I have basically no experience with this type of exercise (so the majority of it was new/beneficial to me).
▼	I can experience how incident response work in "real-life"

Did you learn something new?

5. Did you learn something new?

Number of respondents: 15



	n	Percent
Yes	15	100,0%
No	0	0,0%

If yes, please describe what.

6. Please describe what?

Number of respondents: 12

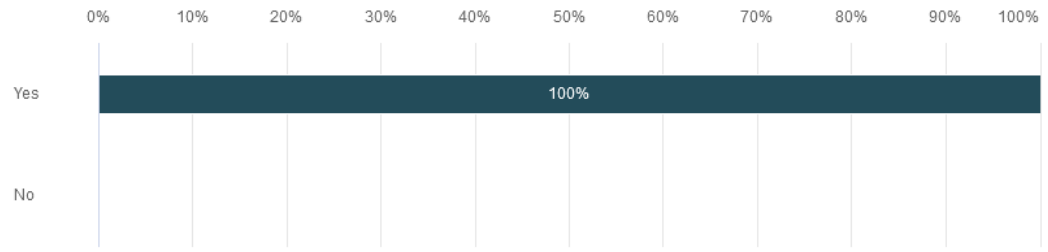
Showing 12 out of 12 responses Show less **or see all text answers in** Word **or** PDF

	Responses
	How to manage systems and how all pieces make together a big picture.
	Yes, various tools used by the security operations teams and the process of investigation.
	a little bit about cmd, and powershell, siem, firewalls
	Attack techniques and tactics commands tools for investigating attacks
	Since I am a linux user, I learned some tricks on windows machines :)
	I learned the complexity of having multiple tools with multiple sources of information and how to try to correlate those info.
	Like answered above, tools and network environment.
	The environment and all the tools used were new for me so it was a nice introductory look at some specific tools like Elastic and FireEye.
	I would say that I mostly refreshed my memory on many things like fcaps, firewalls, linux commands etc. but I feel that my knowhow on SIEM improved quite a lot.
	how to use the tools (beginner level)
	My work is very theoretical, and I do not get to see the practical sides of system protection much. I think I have a good understanding of what can/should be done but very little of how that is actually achieved, which is probably the most important thing I took away from the exercise.
	How to decode/encode texts, reading powershell scripts

Would you recommend Flagship 2 for a friend or a colleague?

7. Would you recommend Flagship 2 for a friend or a colleague?

Number of respondents: 15



	n	Percent
Yes	15	100,0%
No	0	0,0%

Free feedback about Flagship 2

8. Free feedback about Flagship 2

Number of respondents: 9

Showing 9 out of 9 responses Show less or see all text answers in Word or PDF

	Responses
	Great exercise, Thanks
	I think that fully online environment that you have set up is incredible. It would be great to do the exercise onsite, but even with the MS Teams and VMs everything went smoothly.
	I think most participants are looking forward for a Flagship3 on site and not remotely this time. I guess that this interaction will be beneficial for all participants. Thank you guys for this experience!
	The flagship was greatly organized and I in particular liked that we had a team coach, so we didn't get stuck. On the other hand, he was also needed, because we found some artifacts from testing and setting everything from time to time. I.e. the traffic analysis tool suggested that ADMIN-WS-06 had already sent packets to the [redacted] IP on Jan 22nd and before, thus clearly before the word document was opened. However, this didn't keep us from finding what was thoroughly hidden and really liked that our coach was guiding us, but not pushing and leaving us lots of freedom to investigate interesting things. Thanks a lot for this fun exercise!
	I did not attend Flagship 1, but what I'm sure of is that Flagship 2 has been great. It wasn't easy, and that's good. It's stimulating. Of course, the only problems are the initial difficulty of grasping the usefulness of the several available tools (and for that I think that a few pages guide to read before the event could be useful) and the slow performance of siem nodes and recurrent disconnections.
	Thanks for your effort. It was great! Some small connection issues but that did not reduce the joy by much. Keep up the excellent work!
	I want to send my thanks especially to the facilitators since after all they are the core people generating the desired impact.
	Well theoretically, I would recommend Flagship 3 to a friend or a colleague ;)
	It was not as challenging as I thought it would be, but I think its level of challenge is just right. The scenario was great and reflects a real situation that might happen but we don't face in daily life, so it makes this really meaningful. The only thing that I didn't agree with is that in the description we were told that "no technical knowledge required" but apparently I think we do need some technical knowledge to get the full experience of this event. Other than that, I can't say enough about how amazed I was looking at the environment preparation, all those efforts and dedication put in this was huge and I really appreciate that.