Proposal No. 830929

Call H2020-SU-ICT-03-2018

Project start: 1 February 2019

Project duration: 42 months

Cyber Security for Europe

D6.4

Flagship 1

Document Identification	
Due date	31 January 2020
Submission date	24 February 2021
Revision	1.1

Related WP	WP6	Dissemination Level	CO
Lead Participant	JAMK	Lead Author	Jani Päijänen (JAMK)
Contributing Beneficiaries	UNITN, BRNO, ICITA, UPRC	Related Deliverables	D7.1, D7.3

Abstract: Flagship 1 was an online-only cyber security exercise targeted at CyberSec4Europe partners. Total 36 attendees from 22 affiliates were placed into a fictional organisation's Digital Forensic Investigation and Response (DFIR) team. Each team's task was to independently investigate a cyber-attack and respond to it. They were expected to use the documentation and procedures provided by the exercise conductor, including an organisation chart of the fictional organisation they belonged to. Attendees' backgrounds varied from cybersecurity experts to novices.

According to the received feedback and in-situ observation, the attendees found the exercise beneficial. Reportedly, they learned new tools and processes, experienced DFIR teamwork and understood the need for efficient team internal communication, need for communicating to internal and external stakeholders and interest parties. The exercise showcased that cyber security exercises can develop teamwork, the individuals' skills, knowledge, and abilities. Simultaneously it was showcased that in a cyber security exercise an organisation can test and evaluate its guidelines and procedures, their correctness and their relevance to the organisation, as well as test new tools and systems.

Since the COVID-19 situation was not showing signs of calming down in August 2020, the event was changed from on-premises to online. The change required modifications to made plans, including implementing a new method in collaboration with WP7 T7.2 for the attendees to access the technical exercise environment. The attendee method was a prepared VirtualBox virtual machine. During the exercise, new method enabled the end-users to join a cyber security exercise, and a method to enrich cyber range's features and functionalities with commercial cloud components was demonstrated and tested. The method was based on open-source SD-WAN technology. Based on the experiences of the demonstration, the technology could be considered to be used in production in cross-border cyber security exercises.

The received feedback and in-situ observations of D6.4 are taken into account in planning, implementing and conducting D6.5.

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

D6.4 (Flagship 1) was an online-only cyber security exercise for CyberSec4Europe partners. The attendant in the exercise required no previous experience in such exercises nor technical background. Attendees from 22 affiliations were placed into five teams. Each team was simulating a Digital Forensic Investigation and Response (DFIR) team of a fictional organisation. They had the task to investigate a response to a cyber security incident that the fictional employer, The University of Kybereo, had faced by using the provided incident response plans, communication guidelines and other documentation. The roles of the attendees were assigned by the exercise conductor following the expertise and wishes of the attendees collected in a questionnaire prior to the exercise.

The exercise environment was a realistic cyber arena, which was customised and exposed to the attendees as a simulated large, Internet connected business environment with well-integrated security controls available. The environment used the commercial Amazon AWS cloud environment seamlessly to enrich the exercise. During the exercise, a new connectivity method was tested in collaboration with WP7 T7.2 to provide access to the technical platform of the cyber arena and to enrich the exercise. The requirement specification of this method was documented in D7.1 PART B. The exercise showcased that the tested specification implementation, cyber range technical federation using open-source SD-WAN technology, could be considered to be used in production in cross-border cyber security exercises.

Prior to the exercise, an Online Open Course (OOC) was prepared as a preliminary voluntary task for technically oriented attendees. The OOC prepared attendees for performing a basic digital forensic investigation. The OOC was self-paced independent study. The to-be-investigated virtual machine was exported from the Flagship 1 environment. The OOC received positive feedback for providing a basic task with a large collection of background information to familiarise the attendees with the performance of a basic digital forensic investigation.

The objectives of the Flagship 1 were to introduce the benefits of cybersecurity exercises to the attendees, whom were representing an organisation, in this case fictional. Performing DFIR in an organisation require both technical and non-technical roles and skills. Also, attendees' awareness was raised about preparation for a cybersecurity incident or attack is required in order to perform effectively when an incident is detected. An objective was also to demonstrate how individuals' skills in cybersecurity can be improved in a cyber security exercise. The objectives were met. The exercise showcased several benefits of a realistic cyber arena: even in a realistic, well-equipped, and integrated environment digital forensic investigation may be slow to progress; timely communication for internal and external recipients and stakeholders is expected; an organisation may test its processes and guidelines, and as a result detect areas of improvement in a cyber security exercise.

Flagship 1 received very positive feedback from the attendees for the realism of the environment, tools, and systems available in the exercise environment as well as for raising awareness of cyber security exercises. Flagship 1 supports WP6 objectives for cyber security skills assessment and education as the implemented concept could be utilized in curriculum studies, training organisation's employees and individuals, and by showcasing that the implementation of D7.1 could support distributed cross-border cyber range collaboration.

Document information

Contributors

Name	Partner
Jarmo Viinikanoja	JAMK
Juha Piispanen	JAMK

Reviewers

Name	Partner
Chan Nam Ngo	UNITN

History

Version	Date	Authors	Comment
1.1	2021-02-24	Jani Päijänen	Modifications as noted in project management's review
1.0	2021-02-19	Jani Päijänen	Language corrections based on internal review.
0.3	2021-02-17	Jani Päijänen	Language and readability corrections according to the feedback of 2nd internal review.
0.2	2021-02-12	Jani Päijänen	Modified according to the received internal feedback.
0.1	2021-02-08	Jani Päijänen, Jarmo Viinikanoja, Juha Piispanen	1st Version

Table of Contents

List of Figures

List of Tables

List of Acronyms

C	**CISO**	Chief Information Security Officer
D	**DFIR**	Digital Forensic Investigation and Response
G	**Global DNS Hierarchy**	Is a distributed mechanism to translate domain names (e.g. www.jyvsectec.fi) to machine understandable numerical format.
N	**NTP**	Network Time Protocol is a method to synchronise clocks in network connected equipment.
P	**PKI**	Public Key Infrastructure

Glossary of Terms

B **Blue team (BT)**

Exercise attendees were placed into blue teams. In some exercises they are the defending teams.

D **Digital Forensic Investigation and Response**

Digital Forensic Investigation and Response is a set of activities the objectives of which are to investigate the detected cybersecurity incidents, identify and examine the exploited vulnerabilities, determine which assets have been exposed, respond to the incident by removing the threat-actor from the networks and communicating timely and clearly to relevant stakeholders.

G **Green team (GT)**

Green team represents the technical (engineering) team that created the exercise environment and provided technical support for Blue teams and for the White team.

V **VirtualBox**

Virtualisation software made by Oracle Corporation. The full name of the software is Oracle VM VirtualBox.

W **White Team (WT)**

White team members are exercise leaders, and they represented those roles in the exercises that were not part of any other team.

1 Flagship 1 Arrangements

Flagship 1 was an online-only cyber security exercise targeted at CyberSec4Europe partners, held on January 12 – 13, 2021. Not only were the attendees accessing the technical environment online, but also the majority of the conductors were doing it. The exercise was conducted by the employees of JAMK University of Applied Sciences' cyber security research, development, and training center JYVSECTEC.

The attendees of the exercise were assigned a role in a fictional organisation, the University of Kybereo. The roles of the attendees were assigned by the exercise conductor, following the expertise and wishes of the attendees collected in a questionnaire prior to the exercise. The participants were placed into five Blue Teams (BTs), and each BT was independently simulating Digital Forensic Investigation and Response (DFIR) team of the University of Kybereo. They had the task to investigate and respond to the cyber security incident faced by the organisation utilizing the provided incident response plans, communication guidelines, security policies, and organisation chart. The exercise environment was a realistic cyber arena, which was customised and exposed to the attendees as a simulated large, Internet connected business environment with well-integrated security controls available.

The exercise was initially planned to be held in the premises of JAMK University of Applied Sciences, located in Jyväskylä, Finland. Due to the COVID-19 situation, the conductor decided in August 2020 that the event shall be online-only, and the existing plans were modified to meet the changed situation. This created a positive challenge for the conductor: how to ensure that non-technically oriented person are able to access the exercise environment. Attending the exercise required no previous experience in such exercises nor a technical background.

The number of participants was limited, so that only one person from each affiliation was granted participation, but if there were seats available, a maximum of two seats could be permitted. Eventually some affiliations had more than two participants participating the event, levelling the number of team members.

1.1 Timeline

The planning and implementation of Flagship 1 took approximately a year. The timespan consisted of the following activities:

- Exercise planning and implementation (Exercise contents and Technical environment)
- Collaboration with WP7 T7.2
- Planning, implementation and publication of Online Open Course (OOC)
- Call for attendees
- Preparation and publication of the registration page
- Planning and publication of Event page (collaboration with WP9 T9.4)
- Posting preparation and postings on social media (collaboration with WP9 T9.4)
- Exercise test run
- Preparation, publication and testing of connectivity image with attendees
- Preparation and publication of press release materials (collaboration with WP9 T9.4)
- Flagship 1 event

The mentioned activities required work from the partners involved in the Task T6.4 in form of participation in various planning and review meetings. Collaboration with Task T7.2 included receiving

and deploying the implementation of the components of the cyber range technical federation into the exercise.

It is worth noting that the timelines of activities shown in Figure 1 represent their start-end period but do not indicate the required work-effort. The OOC, collaboration with T7.2 and Social media activities will last beyond Flagship 1 active phase. To simplify the timeline, the period of June 2020 was removed.

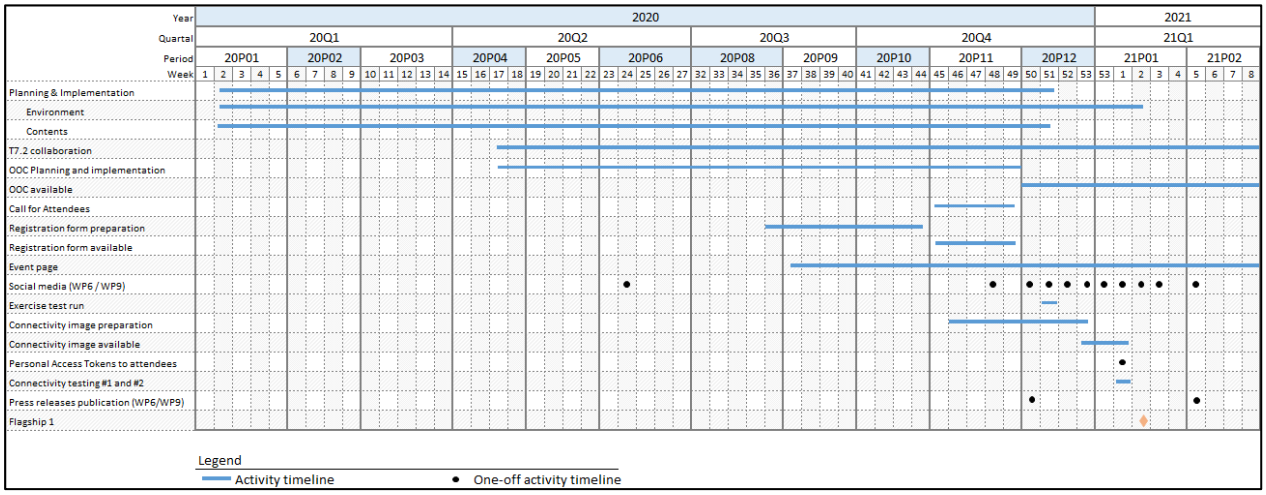


Figure 1: Flagship 1 timeline and activities

The following sections and chapters describe the activities in more detail.

1.2 Objectives of Flagship 1

The planning assumption was that some of the attendees had little hands-on experience in cyber security while some had in-depth knowledge and skills in multiple cyber security topics. Also, as no previous experience in participating in a cyber security exercise or competition was required, it was assumed that the exercise would also attract attendees with non-technical backgrounds. These assumptions set the question how both novices and experts could gain benefit from the exercise for themselves. It was planned that based on an attendee's background, she or he could find the exercise beneficial for him- or herself.

High-level objectives were to demonstrate the benefits of cybersecurity exercises to the attendees, as they require both technical and non-technical roles and skills and to raise the attendees' awareness of the fact that preparing to a cybersecurity incident or attack is required in order to perform effectively when an incident is detected. A high-level objective was also to demonstrate how individuals' skills in cybersecurity could be improved in a holistic way in a cyber security exercise. Further, these led to the following learning objectives of the exercise for the attendees:

- Development of organizational activities
    - Understanding how an organisation could prepare for a cyber incident, and which roles in an organisation could be required to get the incident resolved.
- Internal communication
    - Understanding the importance of digital forensic investigation and response (DFIR) team internal communication. Understanding how a shared vocabulary could help DFIR team to communicate internally and externally.
- Crisis communication
    - Understanding that crisis communication (launched by a cyber-attack) requires timely and correct communication to the organisation's internal and external stakeholders and

interest parties. Understanding that crisis communication should have clear guidelines and preferably premade templates for various situations.

- Clarification of responsibilities
  - Understanding that an effectively working DFIR team needs clear responsibilities, as does an organisation when the top-management is expected to provide decision making authority to support the DFIR team in its tasks.
- Identification of process deficiencies
  - Understanding that process deficiencies may exist even in well-led and managed organisations. Understanding that if deficiencies are detected in the middle of a cyber-attack, there are roles in the organisation that, if required, make the necessary decisions to support responding to the attack.
- Bringing in the authorities
  - Understanding that authorities should be contacted, especially in a case where GDPR violation has occurred. Understanding that contacting the corresponding (national) authority should be clearly mandated to one or more work roles.
- Testing new processes or tools
  - As the Flagship 1 technical environment included a set of well-integrated cybersecurity controls, and since the technical attendees were exposed to them, they could acquire experience with the use of the tools and the technical processes how they were integrated.
- Understanding the overall situation / dependencies
  - Gain understanding that working under a time pressure, performing digital forensic investigation and response (DFIR), the DFIR team members should have an understanding of each other's ongoing activities and to-be delivered results, and the DFIR team lead should have situational understanding of the whole picture. The findings and indicators found during the investigation should be linked to gain an understanding of the attack path and the initial exploited vulnerability.
- Technical ← → non-technical employees' communication with each other
  - Understanding the importance of shared vocabulary across the organisation's key actors in case of a cyber-attack, as it inevitably requires presence or action from both technical and non-technical employees.
- Impact assessment
  - Understanding that impact assessment of a cyber incident requires an understanding of the technical infrastructure, impact to the organisation's intangible technical and business assets, and understanding of the impacts to compliance requirements the organisation has committed to, whether by law, regulation or by contract.

An objective revealed to the attendees only in the feedback session was the gained understanding that by participating a cybersecurity exercise an organisation can test, for example, its procedures, processes, and guidelines. As a result, the organisation could detect areas of improvement in those.

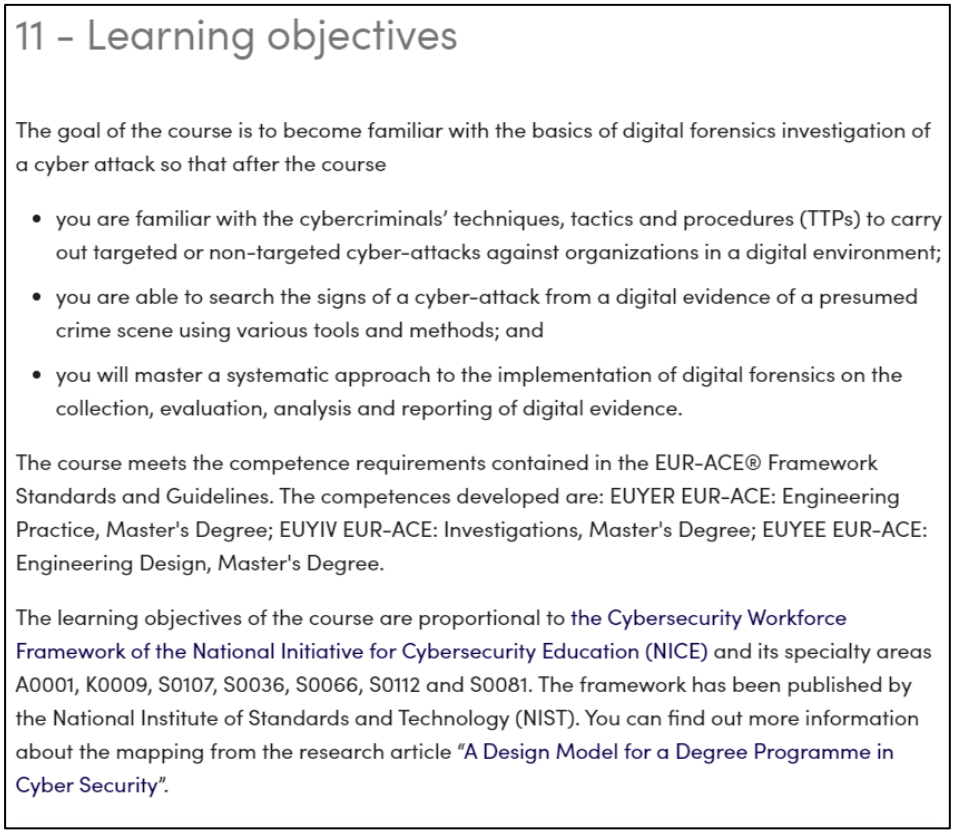
Chapter 3 Lessons learned describes how the objectives were met.

1.3 Online Open Course

Prior to the exercise an Online Open Course (OOC) (CyberSec4Europe 2020a), a basic course on digital forensic investigation was prepared. It was mainly targeted at the technically oriented attendees of the exercise, but it also included background information about the fictional organisation that the attendees were about to be placed into: the Switzerland-based University of Kybereo, which had signed a business contract with an Italian train company CyberRails to launch research and development co-operation. After the agreement had come to light, the employees of the University of Kybereo detected signs of

abnormal emails and intranet login pages or look-alikes. In the OOC, attendees investigated digital evidence provided by the conductor and, if they saw it necessary, utilised the tips provided in the course material. The digital evidence material was extracted from the Flagship 1 environment and was provided as VirtualBox 6.1 compatible virtual machine image. The Investigation used an open-source VirtualBox virtualised Linux workstation that is publically available and is provided by Offensive Security (Offensive Security 2020).

The learning objectives of the OOC (CyberSec4Europe 2020b) are shown in Figure 2.



11 - Learning objectives

The goal of the course is to become familiar with the basics of digital forensics investigation of a cyber attack so that after the course

- you are familiar with the cybercriminals' techniques, tactics and procedures (TTPs) to carry out targeted or non-targeted cyber-attacks against organizations in a digital environment;
- you are able to search the signs of a cyber-attack from a digital evidence of a presumed crime scene using various tools and methods; and
- you will master a systematic approach to the implementation of digital forensics on the collection, evaluation, analysis and reporting of digital evidence.

The course meets the competence requirements contained in the EUR-ACE® Framework Standards and Guidelines. The competences developed are: EUYER EUR-ACE: Engineering Practice, Master's Degree; EUYIV EUR-ACE: Investigations, Master's Degree; EUYEE EUR-ACE: Engineering Design, Master's Degree.

The learning objectives of the course are proportional to the Cybersecurity Workforce Framework of the National Initiative for Cybersecurity Education (NICE) and its specialty areas A0001, K0009, S0107, S0036, S0066, S0112 and S0081. The framework has been published by the National Institute of Standards and Technology (NIST). You can find out more information about the mapping from the research article "A Design Model for a Degree Programme in Cyber Security".

Figure 2: Learning objectives of the OOC

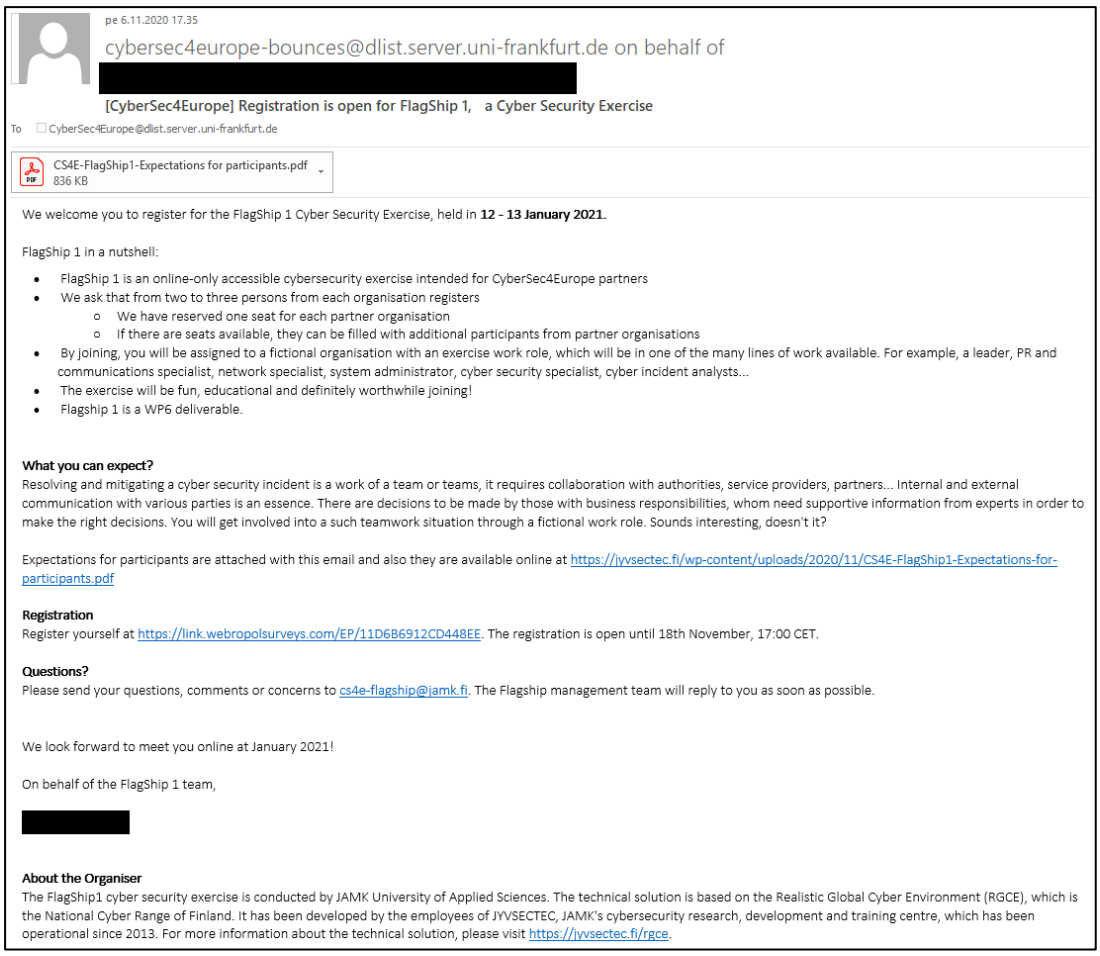
The course materials included a comprehensive amount of up-to-date information and references with which to start the digital forensic investigation. The OOC was opened on 30 November 2020 and was open until 19 December 2020. The attendees were asked to return an assignment report (CyberSec4Europe 2020c) via email. As the course was voluntary, no registration was required to access or download the materials. To attract a wider audience to the course and its subject, and as there were no technical limitations preventing to do so, the OOC was made globally available.

The received feedback from the OOC was positive. The attendees thanked for the available support materials and the easiness of the course for persons who had not performed digital forensic investigation before. Due to public request, OOC materials are available until further notice. The structure of the course materials is shown in Annex A: Online Open Course Content structure.

1.4 Call for Attendees and Registration

The Call for attendees was published in the project's internal mailing lists. The first email was sent on 6 November 2020, as shown in Figure 3. The theme in the email and in the attached Expectations for participants document was to make the event easily accessible and ensure the attendees that it is safe to

participate and work in the exercise, while facing uncertainties. The same theme was present on other materials distributed to the project partners and exercise attendees. The rationale for this empathic approach was that it could have been that the exercise attendees are not directly related to the project but to the affiliation. Then, if those closely working with the project were not able to participate, they could have passed their organisation's seat to a colleague. The registration was open 6th– 18th November 2020.



pe 6.11.2020 17.35

cybersec4europe-bounces@dlist.server.uni-frankfurt.de on behalf of [redacted]

[CyberSec4Europe] Registration is open for FlagShip 1, a Cyber Security Exercise

To CyberSec4Europe@dlist.server.uni-frankfurt.de

CS4E-FlagShip1-Expectations for participants.pdf
836 KB

We welcome you to register for the FlagShip 1 Cyber Security Exercise, held in **12 - 13 January 2021.**

FlagShip 1 in a nutshell:

- FlagShip 1 is an online-only accessible cybersecurity exercise intended for CyberSec4Europe partners
- We ask that from two to three persons from each organisation registers
  - We have reserved one seat for each partner organisation
  - If there are seats available, they can be filled with additional participants from partner organisations
- By joining, you will be assigned to a fictional organisation with an exercise work role, which will be in one of the many lines of work available. For example, a leader, PR and communications specialist, network specialist, system administrator, cyber security specialist, cyber incident analysts...
- The exercise will be fun, educational and definitely worthwhile joining!
- Flagship 1 is a WP6 deliverable.

What you can expect?
Resolving and mitigating a cyber security incident is a work of a team or teams, it requires collaboration with authorities, service providers, partners... Internal and external communication with various parties is an essence. There are decisions to be made by those with business responsibilities, whom need supportive information from experts in order to make the right decisions. You will get involved into a such teamwork situation through a fictional work role. Sounds interesting, doesn't it?

Expectations for participants are attached with this email and also they are available online at https://jyvsectec.fi/wp-content/uploads/2020/11/CS4E-FlagShip1-Expectations-for-participants.pdf

Registration
Register yourself at https://link.webropolsurveys.com/EP/11D6B6912CD448EE. The registration is open until 18th November, 17:00 CET.

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 2021!

On behalf of the FlagShip 1 team,

[redacted]

About the Organiser
The FlagShip1 cyber security exercise is conducted by JAMK University of Applied Sciences. The technical solution is based on the Realistic Global Cyber Environment (RGCE), which is the National Cyber Range of Finland. It has been developed by the employees of JYVSECTEC, JAMK's cybersecurity research, development and training centre, which has been operational since 2013. For more information about the technical solution, please visit https://jyvsectec.fi/rgce.

Figure 3: Call for attendees email

While responding to the registration form, the attendees were asked to comply with Privacy Policy and Terms of Service. Also, existing basic understanding on cyber security was enquired about with the preferred exercise role.

1.5 Event Pages

The conductor prepared event pages (CyberSec4Europe 2020d) together T6.4 partners in collaboration with and WP9 T9.4 partners. The main purpose of this was to share up-to-date information to attendees, but also to raise awareness of those interested in cyber security exercises. According to the statistics exported on 11 February 2021, the average visit time on the pages was two minutes. A total of 686 unique visitors and 859 total page views were reported at the time of reporting. The monthly statistics are shown in Annex B: Event page statistics. The existence of the event pages was raised in social media postings in Twitter and LinkedIn.

The event pages included general information about Flagship 1 and information to attendees, but they also had paragraphs containing information from topics such as “What is cybersecurity”, “What is a cyber range”, and rationale for attendees how their attendance in the event could benefit their own organisations (Figure 4).

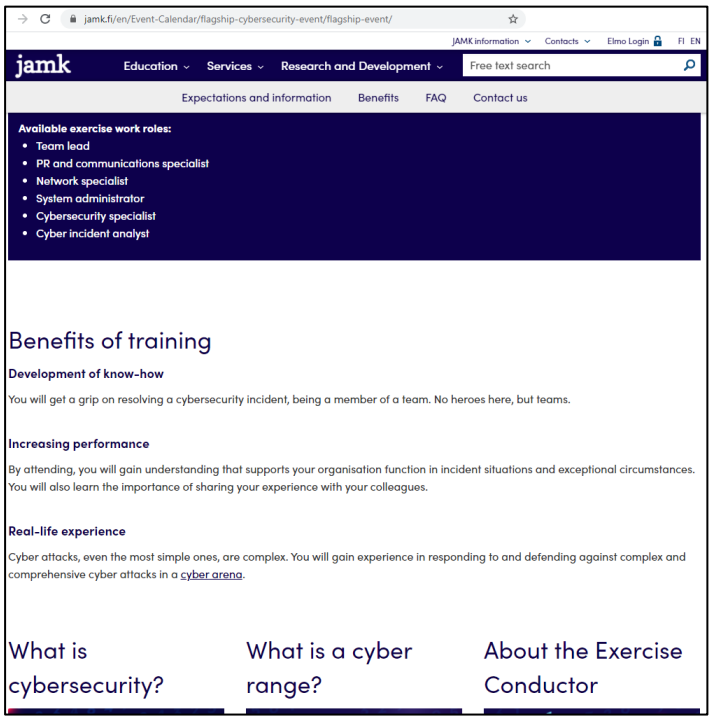


Figure 4: A snapshot from event pages

1.6 Registered Affiliations, Countries and Gender Distribution

In CyberSec4Europe there were in total 43 affiliates from 22 European countries. A total of 45 persons representing 20 affiliations from 16 European countries initially registered to the event. This number excludes the number of the employees of the exercise conductor. Detailed statistics on affiliations, countries and gender distribution is shown in Annex C: Affiliations, Countries and Gender.

1.7 Exercise Environment

The technical exercise environment was based on existing Realistic Global Cyber Environment (RGCE), a cyber arena developed and operated by JYVSECTEC, cyber security research, development, and training center of JAMK University of Applied Sciences, Institute of Information Technology (JYVSECTEC 2019). The cyber arena has in total over 6,000 virtual machines replicating the real Internet and various organisations (JAMK 2021). During Flagship 1, a dedicated part of the cyber arena was exposed to the attendees, including D6.4 specific customisations and the demonstrator of D7.2. The exposed cyber arena included the replicated Internet and its simulated services such as NTP, Global DNS hierarchy, and PKI. The high-level exercise network and environment are shown in Figure 5.

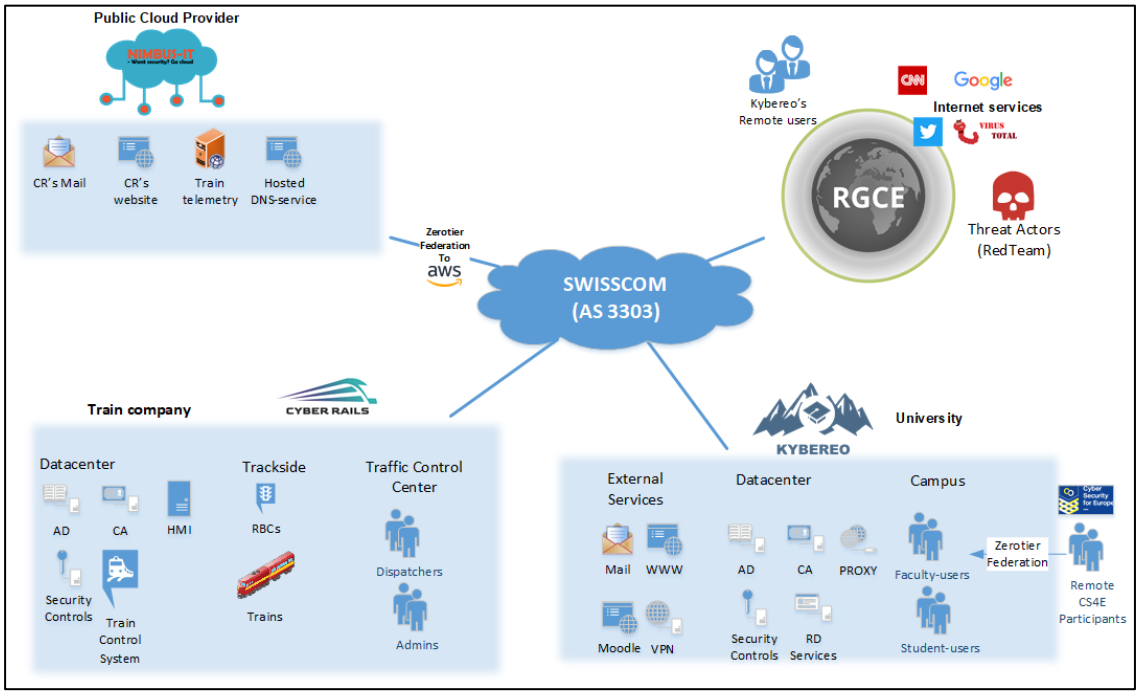


Figure 5: Flagship 1 exercise environment

Prior to the exercise the conductor performed a single day test run. During the test run the technical environment and the exercise flow were tested and verified.

1.8 A New Technical Federation Method

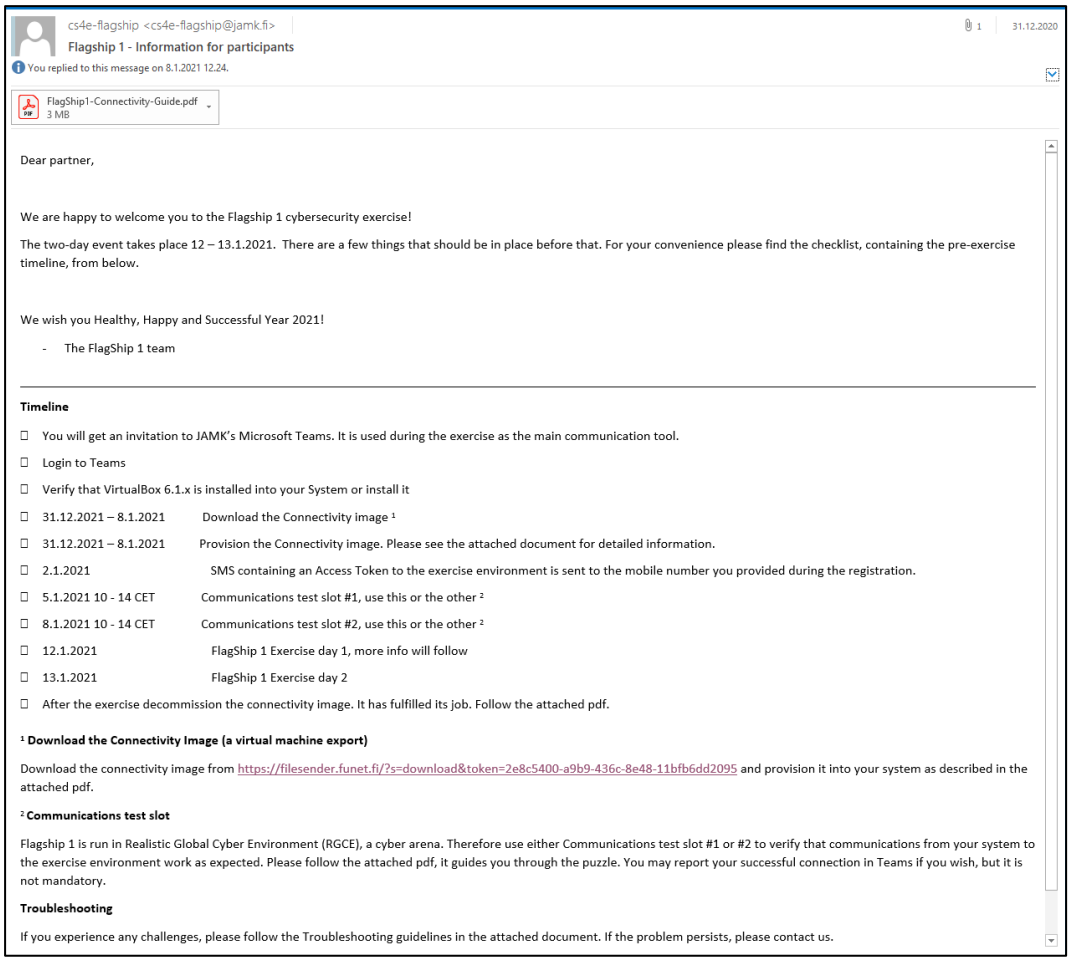
A new connectivity method, cyber range technical federation, was demonstrated in Flagship 1. It was based on open-source SD-WAN technology, and it was used for providing remote participants connectivity to the technical exercise environment as well as extending features and functionalities of the existing cyber arena by running some exercise contents seamlessly in commercial Amazon AWS cloud (Figure 5). End-user (attendee) access to the exercise environment was provided via prepared VirtualBox virtual machine image that the attendees had to deploy in their own system. The connectivity image and provisioning guide for attendees were made simple so that even the non-technical persons could easily attend the exercise.

The demonstrated implementation was based on the requirement specification documented in D7.1 PART B (CyberSec4Europe 2020e) and its results will be document in a future project deliverable, D7.3.

1.9 Connectivity Testing Slots

A week before the exercise, two slots, 5th and 8th January 2021, both between 10:00 – 14:00 (CET) were reserved for the attendees to perform a connectivity test and to register their connection to the cyber arena. This was informed to the attendees in an email sent at New Year's Eve (Figure 6). The email contained a download link to the connectivity virtual machine and the first version of the end-user connectivity guide. The virtual machine had preconfigured settings, and the attendees only had to enter a personal access token code and register their connection to the exercise environment. A Personal Access Token to was provided via SMS. In cases when SMS failed to deliver, Signal or WhatsApp was

used to deliver the access token. The attendees were asked to follow a provided step-by-step guide to pass the connection registration process.



cs4e-flagship <cs4e-flagship@jamk.fi> 1 31.12.2020

Flagship 1 - Information for participants

You replied to this message on 8.1.2021 12.24.

FlagShip1-Connectivity-Guide.pdf 3 MB

Dear partner,

We are happy to welcome you to the Flagship 1 cybersecurity exercise!

The two-day event takes place 12 – 13.1.2021. There are a few things that should be in place before that. For your convenience please find the checklist, containing the pre-exercise timeline, from below.

We wish you Healthy, Happy and Successful Year 2021!

- The FlagShip 1 team

Timeline

- ☐ You will get an invitation to JAMK's Microsoft Teams. It is used during the exercise as the main communication tool.
- ☐ Login to Teams
- ☐ Verify that VirtualBox 6.1.x is installed into your System or install it
- ☐ 31.12.2021 – 8.1.2021 Download the Connectivity image [1]
- ☐ 31.12.2021 – 8.1.2021 Provision the Connectivity image. Please see the attached document for detailed information.
- ☐ 2.1.2021 SMS containing an Access Token to the exercise environment is sent to the mobile number you provided during the registration.
- ☐ 5.1.2021 10 - 14 CET Communications test slot #1, use this or the other [2]
- ☐ 8.1.2021 10 - 14 CET Communications test slot #2, use this or the other [2]
- ☐ 12.1.2021 FlagShip 1 Exercise day 1, more info will follow
- ☐ 13.1.2021 FlagShip 1 Exercise day 2
- ☐ After the exercise decommission the connectivity image. It has fulfilled its job. Follow the attached pdf.

[1] Download the Connectivity Image (a virtual machine export)

Download the connectivity image from https://filesender.funet.fi/?s=download&token=2e8c5400-a9b9-436c-8e48-11bfb6dd2095 and provision it into your system as described in the attached pdf.

[2] Communications test slot

Flagship 1 is run in Realistic Global Cyber Environment (RGCE), a cyber arena. Therefore use either Communications test slot #1 or #2 to verify that communications from your system to the exercise environment work as expected. Please follow the attached pdf, it guides you through the puzzle. You may report your successful connection in Teams if you wish, but it is not mandatory.

Troubleshooting

If you experience any challenges, please follow the Troubleshooting guidelines in the attached document. If the problem persists, please contact us.

Figure 6: Email to attendees at New Year's Eve

Had the attendees faced unforeseeable issues during the connectivity testing, a support team formed by a Green Team (GT) and a White team (WT) representative was available in the exercises' communication platform providing personal support. The used communication platform was Microsoft Teams.

The provided connectivity guide was updated as new knowledge during issue resolution was acquired. It was made available in the communication platform of the exercise. Most issues were related to attendees' VirtualBox configuration settings in a specific operating system or outdated operating system version. The attendees and the support team were able solve all emerged issues together, either by providing assistance to modify VirtualBox configuration settings or recommending to either upgrade attendee's operating system or use a different device.

1.10 Collaboration with WP9, T9.4 Raising awareness

There was collaboration with WP9 T9.4 Raising awareness. The collaboration took form as planning, reviewing, content writing and cross-using created contents, which were:

- Project's web content (CyberSec4Europe 2020f)
- Flagship 1 Event pages (CyberSec4Europe 2020d)

- Social medial postings in Twitter and LinkedIn
- Cybersecurity newsletter of Directorate-General for Communications Networks, Content and Technology at the European Commission (European Commission 2020)
- Press releases (ePressi 2020)(ePressi 2021)
- JAMK University of Applied Sciences' new pages (JAMK 2020)

A new hashtag (#flagship1cse) was presented during Raising the awareness in social media channels (Twitter 2020) (LinkedIn 2020).

2 The Active Days in the Exercise

The exercise had two active exercise days, January 13th and 14th, 2021. During the first day the background story, starting from the phishing campaign introduced in the OOC was showed to remind the attendees of the exercise context. Procedures, guidelines, and the organisation structure (Figure 7) prepared for the attendees was introduced. The attendees were split into five Blue teams (BTs) and assigned to their work roles in the University of Kybereo. Each BT had a team leader, who was also a member of the organisation's Management board through the team leader's CISO role. Other roles were Public Relations / Communications Manager, responsible for DFIR team's communication to internal and external stakeholders and interest parties. Other roles were technical roles performing technical investigation and incident response.

Each BT had a dedicated team coach from the conducting team. The team coach's task was to support the BT to right direction, and facilitate BT's internal collaboration. Team coaches were not allowed to provide correct answers for their teams. The attendees were reminded that the event was a complex learning opportunity. With this the conductor hoped that the collective feeling and atmosphere in each team would be relaxed, and that the attendees could accept the fact the they do not know the details of the environment or tools, yet they still should collaborate and try to investigate and respond to the cyber incident.

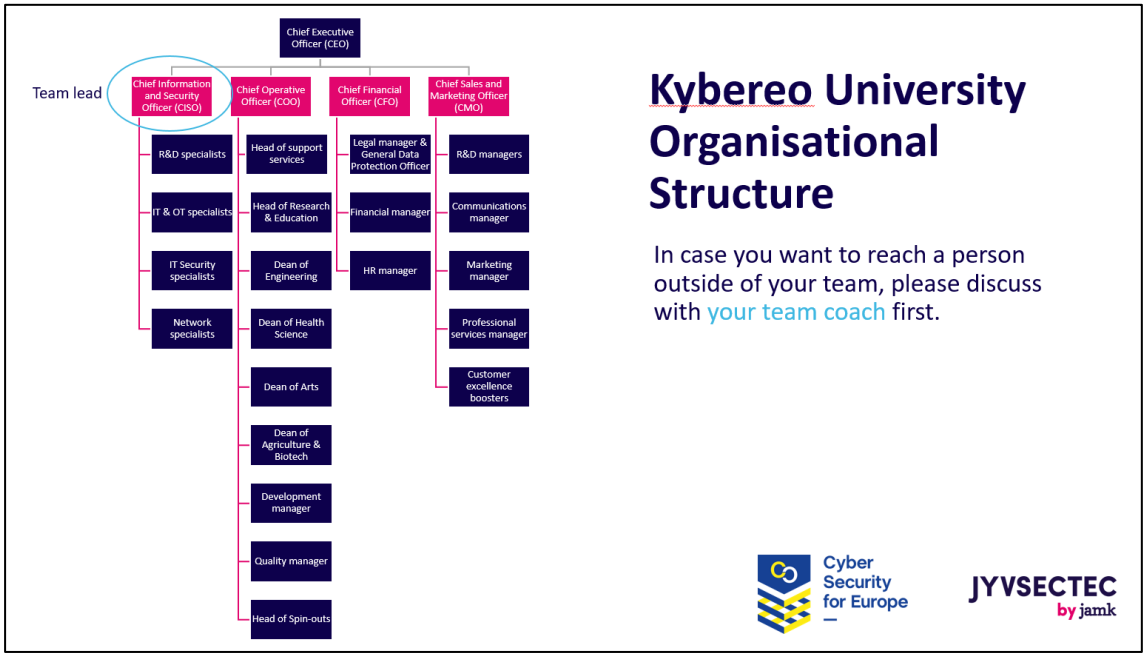


Figure 7: Organisation structure of Kybereo University

Had the attendees had technical issues or questions, the Green Team (GT) was available to resolve them and support the attendees to get back in to the exercise by offering support in the exercise's communication channels.

During the active days of the exercise, a total of nine persons from JYVSECTEC attended the event. Five of them were BT coaches, three were placed into the White Team (WT), one as the exercise leader, one as the WT leader, and one as WT communications representative. WT observed the teams' progress and played various organisational or non-related personas in the available social media and media channels during the exercise. One person represented the GT providing support for all the attendees and monitoring the exercise environment. In addition to the WT activities, software robots were used in the exercise to enrich the social media content stream.

2.1 Exercise Day 1

The first day started at 9:00 and lasted until 15.15 CET (Table 1). The day started with an opening session, followed by a guided introduction to the exercise environment and the systems and tools available in the environment. During the first day, it was expected the teams' members could get to know each other and get some hands-on experience with the exercise environment. In addition, it was expected from the teams to understand if there were victims in the phishing campaign the organisation faced and to name them. There were as little as 1.5 hours of active exercise time in the first exercise day. A few teams were able to name the victims.

Table 1: Timetable of Exercise day 1

09:00 - 10:00	**Flagship1 Kick-off** Welcome words Concept of Flagship 1 X-raying the phising campaign that Kybero faced Day 1 assignment and objectives
10:00 - 10:30	Guided introduction to the exercise environment Group formation
10:30 - 10:45	Refreshment break
10:45 - 12:00	Introduction to exercise environment, in BTs
12:00 - 13:00	Lunch
13:00 - 14:30	Exercise Active phase
14:30 - 14:45	Refreshment break
14:45 - 15:00	Day 1 summary
15:00 - 15:15	Exercise Day 1 ends

From the conductor's point of view, during the first day collaboration in each team between team members was a bit careful. It was expected, as it was the first time they were performing as a team.

2.2 Exercise Day 2

The second exercise day had the same duration as the first exercise day. It focused on the DFIR task. The teams were expected to investigate and respond to the attack, determine the attack path, the exploited vulnerabilities, and to detect what was the impact of the incident to Kybereo. Immediately after the second day started, in all teams the team internal collaboration had improved compared to the first day.

During the second day (Table 2), the available social media and email channels were used by the White Team (WT). WT activated teams impersonating as the Kybereo's CEO asking for information, impersonating as external media person or a media corporation, or some unrelated person posting negative, positive or non-related comments in the available social media channels. All BTs were close to find out the technical impact the cyber incident had caused to Kybereo, if there was a violation to one or more of Kybereo's assets' confidentiality, integrity or availability and from which country the incident originated. The potential business impact to the contract and future collaboration between Kybereo and CyberRails were not in the scope of the exercise.

During day two, one BT alerted the CEO that the organisation may have a GDPR issue due to a cyber-attack but could not eventually confirm it. Two BTs asked the CEO for decision-making support to open phishing victims' emails. Behind the scenes, the CEO approached the General Data Protection Officer, Legal manager and the victims and authorised the BTs to open the requested emails.

Table 2: Timetable of Exercise day 2

09:00 - 09:15	**Day 2 Kick-off**
09:15 - 10:30	Exercise active phase
10:30 - 10:45	Refreshment break
10:45 - 12:00	Exercise active phase
12:00 - 13:00	Lunch
13:00 - 14:30	Exercise Active phase
14:30 - 14:45	Refreshment break
14:45 - 15:00	Flagship 1 Closing Feedback Certificate of Completition
15:00 - 15:15	Flagship 1 ends

During the Flagship walkthrough the attack path and exploited vulnerabilities were revealed to the attendees; they were also informed about the originating country of the attack with remarks that a cyber-attack may use a proxy through a hijacked environment, hiding the tracks of the actual attacker. It was discussed that available virus-scanners may not detect that a scanned file contains malware, even though the scanned file may well contain one.

In the closing timeslot, the attendees gave feedback on the arrangements and the exercise contents. Criticism towards the provided Incident response team documentation and guidelines was received. As a response to the criticism, it was explained to the attendees that there were easily detectable gaps there on purpose: in a cyber security exercise, an organisation's representatives can detect areas of improvement from the used procedures and guidelines. Had there been gaps or inconsistencies in the materials used by the exercising organisation, the BTs could and should have improvised the gaps during the exercise. After the exercise, they should be corrected, honouring the organisation's review and approval process.

The technical exercise environment was accessible to the attendees on both exercise days between 8:00 – 15:00 (CET). Outside these hours, the attendees were not able to access the environment.

2.2.1 Short Survey to Attendees

During the feedback session on exercise day two, a short anonymous survey was conducted expecting free form answers to four questions, and twenty attendees responded to the survey. The Survey questions and answers are available in Annex C: Results of the Short Survey to Participants. The survey results (N=20) show that 100% of the respondents found the exercise beneficial for them and would recommend it to their colleagues or friends. The majority of the respondents 95% (19) learned something new during exercise.

The majority of the free text responses were highly positive. The few responses were forward-looking, which might support the implementation of D6.5 to be "better" than D6.4; they are shown below followed by a short discussion from the conductor. The remarks in square brackets are from the authors to support the reader with following the conductor's answers to the feedback. Spelling has been corrected by the authors.

Feedback 1

Keep up the good work. [a] I would make security policy more real world, though. [b] And it would be beneficial to go over basic tool usage before "jumping in". Though the tools on the market are similar, the differences make the progress harder with no time to get familiar with the tools.

Feedback 2

Thanks for all attempts and environment, [c] it really needs to be held physically. Virtual experience is really missing a lot! Maybe I can say virtual one can only capture 20-30% of the physical event.

Feedback 3

Very good exercise which definitely gave a realistic insight into an incident response scenario. [d] I would prefer to have the cyber range open for some night hours as well and have the flexibility to work the scenario on any given time for those two days, and also [e] be part of a team with my colleagues, so we could organize and schedule the work at our own pace and with our own methodology. Having someone to "guide" us in the team was a nice touch!

Feedback 4

[f] I would like to know a little bit better how to use tools such as SIEMs etc. before the exercise in order to be more efficient. In addition, [g] I feel that a remotely carried out exercise is more difficult to follow as you are inevitably involved in other parallel activities. But you know, this is due to the current situation :)

The above-mentioned feedback is discussed below.

Answer to Feedback 1

a) Security policy should be more real-word
This topic was discussed in the after-exercise discussion held in the communication platform. The conductor explained that the policy had inconsistencies and gaps that were deliberately placed there. An exercise using the to-be-used policies, procedures and guidelines also provides an opportunity to test those, the exercise being a safe environment, and the situation is suitable for detecting possible inconsistencies, gaps and even errors. Had those been detected, the impacted team should have had to improvise according to their best ability and knowledge, and if they had been unsure, they could have asked for a mandate to improvise. It is beneficial for the participating organisation that after the exercise the detected errors, inconsistencies and gaps

are corrected, had they used in-house materials. The attendees were not expected to perform corrections during or after Flagship 1 but to improvise, as they did.

The conductor reflects on the feedback and tries to find ways to improve the provided guidelines and documentation for D6.5 and expects that the above mentioned is criticised in Flagship 2 as well.

b) Introducing the available tools before exercise active phase starts
Cyber arenas are complex learning platforms, and cyber exercises held in those are complex learning opportunities (Karjalainen & Kokkonen 2020). The conductor had estimated that the available tools and systems may not be familiar to some of the attendees, but the exercise environment was not familiar to any of the attendees. Therefore, a period during the first exercise day was reserved to introduce the exercise environment, the tools, and the systems available for the teams. Given the exercise purpose and the limited schedule, the conductor estimates that no more time could have been used during the two days for the introduction without jeopardizing the exercise objectives. The answer to feedback 3 d) and 4 f) also covers this topic.

Answer to Feedback 2

c) Organising Flagship 1 on-premises would have been even more beneficial for the attendees
The conductor agrees with the respondent: it would have even been more beneficial for the attendees to work physically close and have natural face-to-face group conversation during Flagship 1. The following opens the rationale of having the event online-only.
The first priorities of any event organisers are the safety and health of both the attendees and organisers. Given the COVID-19 situation and the set restrictions, the only possible solution to organise the event was with online-only attendance. During August 2020, when the decision was made to offer the exercise remotely, the Rector of JAMK University of Applied Sciences had ordered that any person travelling from abroad whether a visitor, student, or an employee, should self-quarantine for two weeks before entering the campus. As there were no signs of the situation calming down, nor was the attendees' self-quarantine an option, the decision of remote access was made.

The conductor reflects the feedback with the lessons learned and tries to find ways to improve team collaboration for Flagship 2.

Answer to Feedback 3

d) Having the exercise environment accessible after office-hours and exercising at one's own pace
The exercise was planned and implemented as a team-learning event. The conductor estimated that by working in teams, the attendees could learn, not only to perform activities individually, but also from each other by discussing and watching other team members perform activities. In addition, each team had a team coach guiding them in case the coach or a White Team member observed a need for guidance.

e) Having real-world colleagues in the same team and working at one's own pace and with one's own methodology
The conductor estimated that by separating colleagues to several teams, the individual members of a team could bring their knowledge, skills and abilities into the team, advancing the team activities and learning.

Answer to Feedback 4

f) Practicing the usage of available tools and system before the exercise
It is understandable that one cannot be fully efficient using new tools or systems immediately after they have first been introduced, as is the experienced frustration by the respondent when they were not able to better utilise them. By not exposing them the tools nor systems in advance, each of the attendees, and then the teams were starting with their current knowledge, skills and abilities, which they had before the exercise. Through team collaboration and with the assistance from team coaches the teams were expected to investigate and respond to the cyber incident, gain experience of what could be required from individuals, a team and from an organisation to effectively perform DFIR. In addition, a motivation for this approach was to highlight that in a cyber security exercise new tools and systems can be tested, evaluated or demonstrated.

g) A Remote exercise is difficult to follow due to parallel activities
Having dedicated time and place without distractions to focus on something, even attending a remote cyber security exercise, is beneficial for understanding and learning.

The conductor reflects on the feedback and tries to find ways to let attendees of D6.5 have distraction free time and place for Flagship 2.

3 Lessons learned

Flagship 1 was the first of its kind, where people around Europe attended an online-only cyber security exercise utilising a cyber arena, with different cultural backgrounds and expertise in cyber security and coming from several home organisations. The exercise was excellent. A short survey was performed during the feedback session at the end of the second exercise day. All respondents found the exercise beneficial for them and would recommend it to their colleagues or friends (Annex D: Results of the Short Survey to Participants). Interpreted from the received feedback, the realistic technical exercise environment with its services and tooling was perceived very positively. The received feedback and lessons learned are taken into account when planning, implementing and conducting Flagship 2, which is project deliverable D6.5.

3.1 Online Open Course

Prior to Flagship 1, an Online Open Course (OOC) was prepared and made available. It was mainly targeted at technically oriented attendees but was globally accessible. Had some of the Flagship 1 attendees taken it, then there would have been team members who have already had some hands-on experience on basic digital forensic investigation, theory background about performing DFIR and insight to the exercise context. These attendees could have shared the knowledge and experience to their team members. A few attendees took the course. The OOC contained the theory part and a conductor prepared downloadable VirtualBox based virtual machine, which was the evidence to be investigated. It was extracted from the technical exercise environment of D6.4 and was downloaded 64 times prior the exercise. The course also contained an open-source based inspection virtual machine prepared by a third party. The course was implemented as self-paced independent study.

Due to social media algorithms, the postings did not reach globally those who might have been interested in the course outside CyberSec4Europe. This was revealed in many emails the conductor received. They had forward-looking feedback where senders stated that they expect the OOC to be open again, encouraging that the course should be informed on well in advance and be open for a longer period. The conductor has decided to the keep the course accessible until further notice, as no additional work effort or costs are required to keep it accessible.

3.2 Meeting Flagship 1 Objectives and Received Feedback

The Flagship 1 had several objectives for attendees. The implicit objectives were to introduce the first time attendees a cyber security exercise in a cyber arena. The explicit objectives topics were:

- Development of organizational activities
- Internal communication
- Crisis communication
- Clarification of responsibilities
- Identification of process deficiencies
- Bringing in the authorities
- Testing new processes or tools
- Understanding the overall situation / dependencies
- Technical – non-technical employees' communication with each other
- Impact assessment

As for the observed activities the attendees performed during the exercise, the observed discussions they had internally in their teams and with their team coaches, the received feedback and based authors experience in cyber security exercises, the topics were present and fully covered in D6.4.

The received feedback criticises some of the topics, most commonly the presence of new tools and systems that the attendees were expected to utilise during the exercise. There is a common nominator for responding to the criticism: highlight the benefits of a cyber security exercise in a cyber arena. In such exercises, an organisation or its representative can test, demonstrate or verify new tools and systems, processes, procedures, guidelines, and decision-making mandates, and other elements the organisation would need if it were experiencing a cyber incident or attack.

The criticism of the online-only arrangements had two common nominators: teamwork using the selected communication / collaboration platform, and disturbance of other non-exercise related parallel activities. A cyber security exercise conductor can select the best suitable collaboration platform that supports the attendees in the exercise and finds the ways of using it, only limited by conductor's resources. The conductor learned that either the used collaboration platform needs some new features, or it must be used differently, or another platform must be used, honouring the available resources. In this exercise, Microsoft Teams was used, and the conductor acquired an understanding of the possibilities it offers in the Flagship context.

To answer regarding the non-exercise related parallel activities or distractions is more complicated. An exercise conductor can control the technical exercise environment and the used communications platform (to an extent) but not the applications the attendees have opened in their system(s) or their physical environment. As a future improvement, the exercise conductor will send invitations and open the registration several months before the event, and in return send a (digital) letter to the attendees' home organisation about the planned participation requesting the attendee to be allowed to focus on the exercise. At the time of reporting, the COVID-19 pandemic is still with us. Persons may be working remotely from their homes; some might have their family members present in the apartment or house. Such environment may not be the best for learning fast-paced complex concepts or topics, given there were work-related matters to be to be taken care of simultaneously. Opening the registration well in advance might help attendees to make arrangements for ensuring a distraction free environment.

The conductor has received a certain amount of person-months to plan and implement two Flagship exercises, D6.4 and D6.5. The change from on-premises to online-only that occurred during planning and implementing D6.4 consumed the allocated person-month effort budget. Therefore, the D6.5 will

follow, if not replicate, D6.4. On the positive side, there was the implementation and demonstration of D7.2, which supported the exercise by providing a remote connectivity method to the attendees.

A future task is to research which specific cyber security related skills, knowledge or abilities were improved during the exercise if any.

3.3 Demonstrating Cyber Range Technical Federation

Because the COVID-19 situation neither in Finland nor in Europe in general was not showing signs of calming down at the time of August 2020, it was decided to organize the event online instead of on-premises. The change required modifications to the made plans, and a need emerged for a solution to enable remote access. This need was resolved by implementing and deploying a new method based on open-source SD-WAN technology. The method was implemented in collaboration with WP7 T7.2. A new method was also demonstrated to enrich cyber range's features and functionalities with commercial cloud components, namely the cyber range technical federation. The methods were based on open-source SD-WAN technology. A separate report will be provided by WP7 D7.3. The requirement specification of the demonstrated methods was documented in D7.1 (CyberSec4Europe 2020e). Based on the experiences of the demonstration and the conductor's experience in cyber security exercises, the demonstrated technology could be considered to be used in production in distributed cross-border cyber security exercises.

3.4 Time zones And Potential Cultural Differences in Working Hours

The existence of different time zones was revealed during planning the exercise daily timetable, when in a planning meeting someone asked if the time zones are presented in the Finnish time zone (EET) or in some other time zone. Followed by this question, future schedules are given with clear indicators of the used time zones. A similar question brought about potential cultural differences in working hours, which was also noticed during planning of the event and during the connectivity testing. Despite the schedule provided to the attendees, some connectivity tests were performed outside the officially supported hours. To get attendees onboard, support after the official working hours was provided to ensure a smooth start of the exercise. A future improvement could be to distribute the possible connectivity slots to several days with shorter duration and clearly assigned slots for attendees. That could perhaps ensure that no after-office-hours work is done neither by the conductor nor the attendees; however, planning is still needed on how no-show participants could perform the connectivity tests.

4 Conclusion

Flagship 1, or D6.4, was the first online-only cyber security exercise utilising a cyber arena, where attendees represented 22 different affiliations from 16 European countries. Some of them 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 or theoretical experience in cyber security before the exercise. The data from the quick survey shows that 100% of respondents (N=20) would recommend the exercise to their colleagues or friends and found it beneficial for them. The implemented Flagship concept and the demonstration of the implementation of D7.1 was a success.

Due COVID-19 situation, Flagship 1 was forced to be held as a remote event. Initially it was planned and implementation had been done for an on-premises event. The change happened in the middle of the implementation, and therefore unplanned work effort had to be spent to make the remote access (in collaboration with WP7) possible and modify the exercise technical environment and arrangements to provide a good exercise experience for the participants.

The OOC supported the Flagship 1 remote participants by introducing the exercise context, and provided the participants with a systematic approach to the examination of a cyber-attack within an organization when it suspects that it has been the victim of a cybercrime. Those whom had taken the course were able to use the methods during Flagship 1. Due to public request, the course is open to be taken at any time.

The implicit and explicit objectives set for Flagship 1 were met. Explicit objectives covered how individuals skills, knowledge and abilities (KSA) could be improved in a cyber security exercise in a cyber arena, and team learning by performing DFIR as a team. Implicit objective was to demonstrate that a cyber security exercise could benefit the attending organisation. An organisation can exercise their in-house procedures, processes, roles and responsibilities, and test new tools and systems in a cyber security exercise.

During Flagship 1 WP7 demonstrated the implementation of D7.1 cyber range technical federation requirement specification. The demonstrated capability was used for providing access to remote participants and conductors, and for enriching the exercise with a remote public cloud, which should be interpreted as a remote cyber range offering some service for another cyber range. The demonstrated implementation could be considered production ready. The future deliverable D7.3 will document the implementation in more detail.

The received feedback was highly positive, but some forward-looking feedback was received. The feedback will be taken into account when planning and implementing the Flagship 2. By implementing the minor improvements, the conductor expects Flagship 2 to be even more beneficial for the attendees and it is expected to offer even better cyber security exercise experience.

References

CyberSec4Europe. (2020a, November 30). Flagship 1 Online Open Course. Retrieved February 8, 2021 from https://cs4e.pages.labranet.jamk.fi/ooc/

CyberSec4Europe. (2020b, November 30). Flagship 1 Online Open Course Learning Objectives. Retrieved February 8, 2021 from https://cs4e.pages.labranet.jamk.fi/ooc/10-Course_Introduction/01-Learning_objectives/

CyberSec4Europe. (2020c, November 30). Flagship 1 Online Open Course Assignment. Retrieved January 14, 2021 from https://cs4e.pages.labranet.jamk.fi/ooc/10-Course_Introduction/02-Assignment/

CyberSec4Europe. (2020d, December 6). Flagship 1 Event page. Retrieved February 8, 2021 from https://www.jamk.fi/en/Event-Calendar/flagship-cybersecurity-event/flagship-event/

CyberSec4Europe. (2020e, August 30). D7.1 Report on existing cyber ranges, requirements. Retrieved February 8, 2021 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. (2020f, December 16). CyberSec4Europe Hosting Flagship 1: An Online Cybersecurity Exercise. Retrieved February 8, 2021 from https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/

European Commission. (2020, December 18). CyberSec4Europe hosting Flagship 1, an online cybersecurity exercise. Retrieved February 11, 2021 from https://ec.europa.eu/newsroom/dae/item-detail.cfm?item_id=696792&newsletter_id=364&lang=en

ePressi (2020, December 4). JAMK julkaisi avoimen verkkokurssin, joka vie keskelle kyberhyökkäystä – osa suurempaa kyberharjoitusta. Retrieved February 11, 2021 from https://www.epressi.com/tiedotteet/koulutus/jamk-julkaisi-avoimen-verkkokurssin-joka-vie-keskelle-kyberhyokkaysta-osa-suurempaa-kyberharjoitusta.html

ePressi (2021, February 5). Kansainvälisessä kyberturvallisuusharjoituksessa korostui ennakoinnin merkitys. Retrieved February 11, 2021 from https://www.epressi.com/tiedotteet/turvallisuus/kansainvalisessa-kyberturvallisuusharjoituksessa-korostui-ennakoinnin-merkitys.html?block=5&customer=467

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.

JAMK University of Applied Science (2020, December 11). JAMK conducts Flagship 1, an online cybersecurity exercise - part of the exercise published as an open online course. Retrieved February 11, 2021 from https://www.jamk.fi/en/news/2020/jamk-conducts-flagship-1-an-online-cybersecurity-exercise/

JYVSECTEC (2019). Cyber range overview. Retrieved February 11, 2021 from https://jyvsectec.fi/cyber-range/overview/

JAMK University of Applied Science (2021, January 13). Twitter tweet “Did you already know”. Retrieved February 11, 2021 from https://twitter.com/JYVSECTEC/status/1349339951738056706

LinkedIn. (2020). LinkedIn search results for the hashtag “flagship1cse”. Retrieved February 8, 2021 from https://www.linkedin.com/search/results/all/?keywords=flagship1cse&origin=GLOBAL_SEARCH_

Offensive Security. (2020, November 30). Download Kali Linux Virtual Images. Retrieved January 14, 2021 from https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Twitter. (2020). Twitter search results for the hashtag “flagship1cse”. Retrieved February 8, 2021 from https://twitter.com/hashtag/flagship1cse?f=live

Annex A: Online Open Course Content structure

CS4E - Preliminary task before Flagship 1.

Welcome to the course

Frequently asked questions

Release notes

10 Course Introduction

10 - Course introduction

11 - Learning objectives

12 - Flagship 1 Assignment

13 - Learning Diary (report)

20 Background

20 - Case scenario

21 - Course props

22 – Flagship 1 Environment

23 - Flagship 1 Task

30 Cyber Attack

30 - Cyber Attack

31 - Threats and Attacks

32 - Attack framework

33 - Intrusion methods

34 - Flagship 1 Task

40 Digital Forensics

40 - Digital Forensics

41 - Digital artifacts

42 - Investigating methods

43 - Basic commands

44 - Flagship 1 Task

50 Auditing

50 - Basics of auditing

51 - Auditing process

52 - Auditing methods

53 - Risk Management

54 - Known vulnerabilities

54 - Flagship 1 Task

60 Cyber Security Exercise

60 - Flagship 1 exercise

61 - What is a cyber exercise

62 - Cyber exercise scenarios

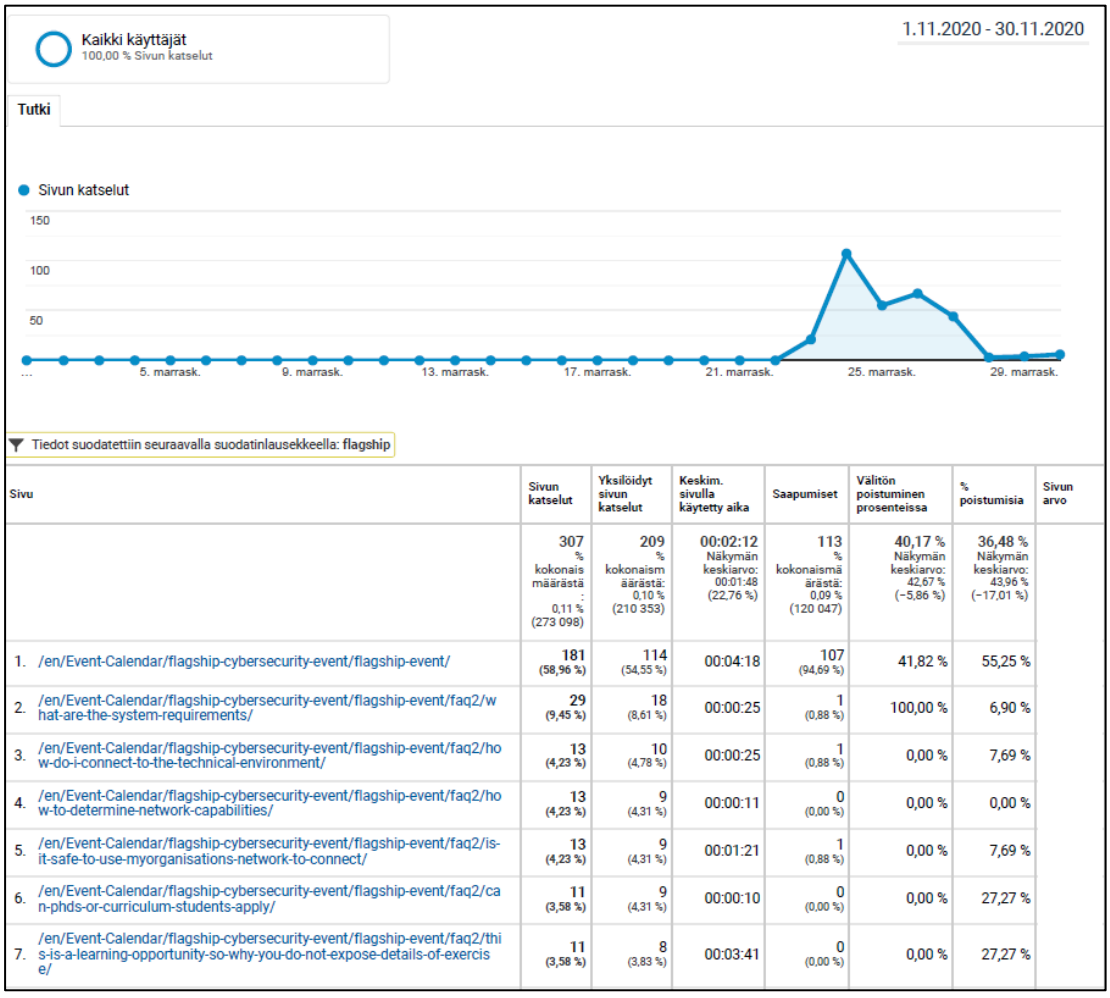
63 - What is CTF

90 Contacts

Annex B: Event page statistics

Event page statistics November 1 – 30, 2020:

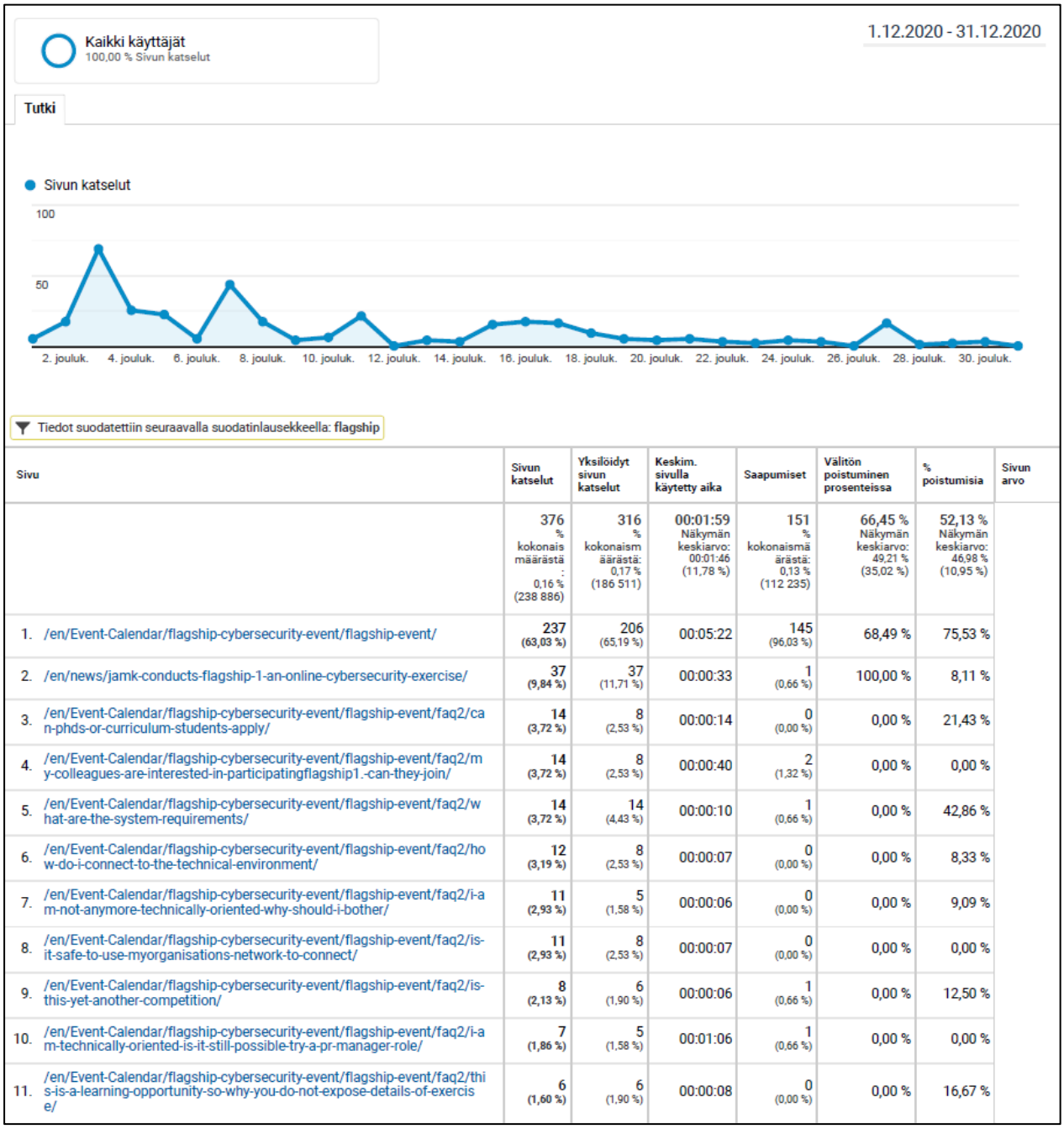
- Total page views: 307
- Unique visitors: 209
- Average time spent: 2 minutes 12 seconds



Sivu	Sivun katselut	Yksilöidyt sivun katselut	Keskim. sivulla käytetty aika	Saapumiset	Välitön poistuminen prosenteissa	% poistumisia	Sivun arvo
	307 % kokonaismäärästä: 0,11 % (273 098)	209 % kokonaismäärästä: 0,10 % (210 353)	00:02:12 Näkymän keskiarvo: 00:01:48 (22,76 %)	113 % kokonaismäärästä: 0,09 % (120 047)	40,17 % Näkymän keskiarvo: 42,67 % (-5,86 %)	36,48 % Näkymän keskiarvo: 43,96 % (-17,01 %)	
1. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/	181 (58,96 %)	114 (54,55 %)	00:04:18	107 (94,69 %)	41,82 %	55,25 %	
2. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/what-are-the-system-requirements/	29 (9,45 %)	18 (8,61 %)	00:00:25	1 (0,88 %)	100,00 %	6,90 %	
3. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-do-i-connect-to-the-technical-environment/	13 (4,23 %)	10 (4,78 %)	00:00:25	1 (0,88 %)	0,00 %	7,69 %	
4. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-to-determine-network-capabilities/	13 (4,23 %)	9 (4,31 %)	00:00:11	0 (0,00 %)	0,00 %	0,00 %	
5. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-it-safe-to-use-myorganisations-network-to-connect/	13 (4,23 %)	9 (4,31 %)	00:01:21	1 (0,88 %)	0,00 %	7,69 %	
6. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/can-phds-or-curriculum-students-apply/	11 (3,58 %)	9 (4,31 %)	00:00:10	0 (0,00 %)	0,00 %	27,27 %	
7. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/this-is-a-learning-opportunity-so-why-you-do-not-expose-details-of-exercise/	11 (3,58 %)	8 (3,83 %)	00:03:41	0 (0,00 %)	0,00 %	27,27 %	

Event page statistics December 1 – 31, 2020:

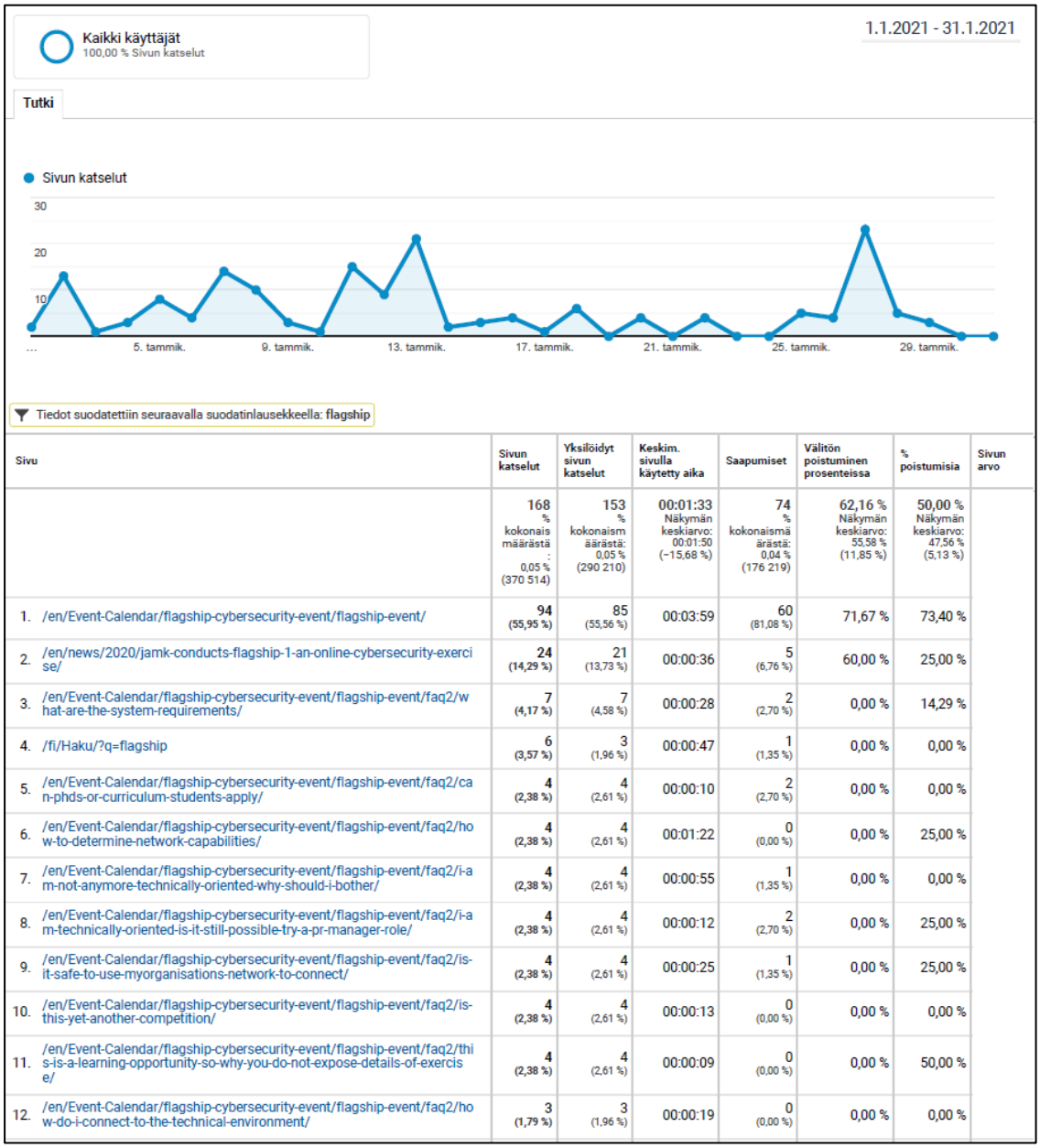
- Total page views: 376
- Unique visitors: 316
- Average time spent: 1 minute 59 seconds



Sivu	Sivun katselut	Yksilöidyt sivun katselut	Keskim. sivulla käytetty aika	Saapumiset	Välitön poistuminen prosenteissa	% poistumisia	Sivun arvo
	376 % kokonaismäärästä: 0,16 % (238 886)	316 % kokonaismäärästä: 0,17 % (186 511)	00:01:59 Näkymän keskiarvo: 00:01:46 (11,78 %)	151 % kokonaismäärästä: 0,13 % (112 235)	66,45 % Näkymän keskiarvo: 49,21 % (35,02 %)	52,13 % Näkymän keskiarvo: 46,98 % (10,95 %)	
1. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/	237 (63,03 %)	206 (65,19 %)	00:05:22	145 (96,03 %)	68,49 %	75,53 %	
2. /en/news/jamk-conducts-flagship-1-an-online-cybersecurity-exercise/	37 (9,84 %)	37 (11,71 %)	00:00:33	1 (0,66 %)	100,00 %	8,11 %	
3. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/can-phds-or-curriculum-students-apply/	14 (3,72 %)	8 (2,53 %)	00:00:14	0 (0,00 %)	0,00 %	21,43 %	
4. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/my-colleagues-are-interested-in-participatingflagship1.-can-they-join/	14 (3,72 %)	8 (2,53 %)	00:00:40	2 (1,32 %)	0,00 %	0,00 %	
5. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/what-are-the-system-requirements/	14 (3,72 %)	14 (4,43 %)	00:00:10	1 (0,66 %)	0,00 %	42,86 %	
6. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-do-i-connect-to-the-technical-environment/	12 (3,19 %)	8 (2,53 %)	00:00:07	0 (0,00 %)	0,00 %	8,33 %	
7. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/i-am-not-anymore-technically-oriented-why-should-i-bother/	11 (2,93 %)	5 (1,58 %)	00:00:06	0 (0,00 %)	0,00 %	9,09 %	
8. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-it-safe-to-use-myorganisations-network-to-connect/	11 (2,93 %)	8 (2,53 %)	00:00:07	0 (0,00 %)	0,00 %	0,00 %	
9. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-this-yet-another-competition/	8 (2,13 %)	6 (1,90 %)	00:00:06	1 (0,66 %)	0,00 %	12,50 %	
10. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/i-am-technically-oriented-is-it-still-possible-try-a-pr-manager-role/	7 (1,86 %)	5 (1,58 %)	00:01:06	1 (0,66 %)	0,00 %	0,00 %	
11. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/this-is-a-learning-opportunity-so-why-you-do-not-expose-details-of-exercise/	6 (1,60 %)	6 (1,90 %)	00:00:08	0 (0,00 %)	0,00 %	16,67 %	

Event page statistics January 1 – 31, 2021:

- Total page views: 168
- Unique visitors: 153
- Average time spent: 1 minute 33 seconds



Kaikki käyttäjät
100,00 % Sivun katselut

1.1.2021 - 31.1.2021

Tutki

Sivun katselut

Tiedot suodatettiin seuraavalla suodatinlausekkeella: flagship

Sivu	Sivun katselut	Yksilöidyt sivun katselut	Keskim. sivulla käytetty aika	Saapumiset	Välitön poistuminen prosenteissa	% poistumisia	Sivun arvo
	168 % kokonaismäärästä: 0,05 % (370 514)	153 % kokonaismäärästä: 0,05 % (290 210)	00:01:33 Näkymän keskiarvo: 00:01:50 (−15,68 %)	74 % kokonaismäärästä: 0,04 % (176 219)	62,16 % Näkymän keskiarvo: 55,58 % (11,85 %)	50,00 % Näkymän keskiarvo: 47,56 % (5,13 %)	
1. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/	94 (55,95 %)	85 (55,56 %)	00:03:59	60 (81,08 %)	71,67 %	73,40 %	
2. /en/news/2020/jamk-conducts-flagship-1-an-online-cybersecurity-exercise/	24 (14,29 %)	21 (13,73 %)	00:00:36	5 (6,76 %)	60,00 %	25,00 %	
3. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/what-are-the-system-requirements/	7 (4,17 %)	7 (4,58 %)	00:00:28	2 (2,70 %)	0,00 %	14,29 %	
4. /fi/Haku/?q=flagship	6 (3,57 %)	3 (1,96 %)	00:00:47	1 (1,35 %)	0,00 %	0,00 %	
5. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/can-phds-or-curriculum-students-apply/	4 (2,38 %)	4 (2,61 %)	00:00:10	2 (2,70 %)	0,00 %	0,00 %	
6. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-to-determine-network-capabilities/	4 (2,38 %)	4 (2,61 %)	00:01:22	0 (0,00 %)	0,00 %	25,00 %	
7. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/i-am-not-anymore-technically-oriented-why-should-i-bother/	4 (2,38 %)	4 (2,61 %)	00:00:55	1 (1,35 %)	0,00 %	0,00 %	
8. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/i-am-technically-oriented-is-it-still-possible-try-a-pr-manager-role/	4 (2,38 %)	4 (2,61 %)	00:00:12	2 (2,70 %)	0,00 %	25,00 %	
9. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-it-safe-to-use-myorganisations-network-to-connect/	4 (2,38 %)	4 (2,61 %)	00:00:25	1 (1,35 %)	0,00 %	25,00 %	
10. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-this-yet-another-competition/	4 (2,38 %)	4 (2,61 %)	00:00:13	0 (0,00 %)	0,00 %	0,00 %	
11. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/this-is-a-learning-opportunity-so-why-you-do-not-expose-details-of-exercise/	4 (2,38 %)	4 (2,61 %)	00:00:09	0 (0,00 %)	0,00 %	50,00 %	
12. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-do-i-connect-to-the-technical-environment/	3 (1,79 %)	3 (1,96 %)	00:00:19	0 (0,00 %)	0,00 %	0,00 %	

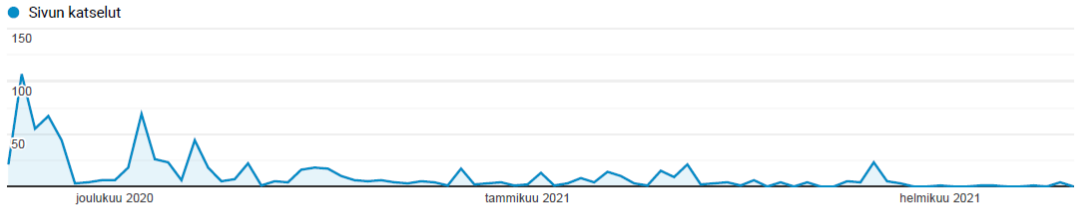
Combined event page statistics November 23, 2020 – February 11, 2021:

- Total page views: 859
- Unique visitors: 686
- Average time spent: 2 minutes

Kaikki käyttäjät
100,00 % Sivun katselut

23.11.2020 - 11.2.2021

Tutki



Tiedot suodatettiin seuraavalla suodatinlausekkeella: **flagship**

Sivu	Sivun katselut	Yksilöidyt sivun katselut	Keskim. sivulla käytetty aika	Saapumiset	Välitön poistuminen prosenteissa	% poistumisia	Sivun arvo
	859 % kokonaismäärästä: 0,11 % (787 130)	**686** % kokonaismäärästä: 0,11 % (614 707)	**00:02:00** Näkymän keskiarvo: 00:01:48 (11,49 %)	**343** % kokonaismäärästä: 0,09 % (366 470)	**56,90 %** Näkymän keskiarvo: 53,16 % (7,03 %)	**46,33 %** Näkymän keskiarvo: 46,56 % (-0,48 %)	
1. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/	**519** (60,42 %)	412 (60,06 %)	00:04:38	317 (92,42 %)	60,12 %	68,21 %	
2. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/what-are-the-system-requirements/	**51** (5,94 %)	40 (5,83 %)	00:00:23	4 (1,17 %)	25,00 %	17,65 %	
3. /en/news/jamk-conducts-flagship-1-an-online-cybersecurity-exercise/	**37** (4,31 %)	37 (5,39 %)	00:00:33	1 (0,29 %)	100,00 %	8,11 %	
4. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/can-phds-or-curriculum-students-apply/	**29** (3,38 %)	21 (3,06 %)	00:00:12	2 (0,58 %)	0,00 %	20,69 %	
5. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-do-i-connect-to-the-technical-environment/	**28** (3,26 %)	21 (3,06 %)	00:00:17	1 (0,29 %)	0,00 %	7,14 %	
6. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/is-it-safe-to-use-myorganisations-network-to-connect/	**28** (3,26 %)	21 (3,06 %)	00:00:43	2 (0,58 %)	0,00 %	7,14 %	
7. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/my-colleagues-are-interested-in-participatingflagship1.-can-they-join/	**26** (3,03 %)	18 (2,62 %)	00:00:27	2 (0,58 %)	0,00 %	7,69 %	
8. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/i-am-not-anymore-technically-oriented-why-should-i-bother/	**24** (2,79 %)	17 (2,48 %)	00:00:35	2 (0,58 %)	0,00 %	4,17 %	
9. /en/news/2020/jamk-conducts-flagship-1-an-online-cybersecurity-exercise/	**24** (2,79 %)	21 (3,06 %)	00:00:36	5 (1,46 %)	60,00 %	25,00 %	
10. /en/Event-Calendar/flagship-cybersecurity-event/flagship-event/faq2/how-to-determine-network-capabilities/	**21** (2,44 %)	17 (2,48 %)	00:00:21	0 (0,00 %)	0,00 %	9,52 %	

Annex C: Affiliations, Countries and Gender

The number of registrees below indicates the number of registered persons, their affiliations, affiliations' home country and gender distribution.

Registered persons

Affiliations

Number	Affilication		Number of registrees	Percent
1	ABI -- ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA		2	4 %
2	ATOS -- ATOS SPAIN SA		2	4 %
3	BRNO -- Masarykova univerzita		2	4 %
4	CYBER -- CYBERNETICA AS		3	7 %
5	DTU -- DANMARKS TEKNISKE UNIVERSITET		1	2 %
6	ENG -- ENGINEERING - INGEGNERIA INFORMATICA SPA		7	16 %
7	FORTH -- FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS		2	4 %
8	GUF -- JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN		1	2 %
9	KAU -- KARLSTADS UNIVERSITET		2	4 %
10	POLITO -- POLITECNICO DI TORINO		4	9 %
11	TDL -- TRUST IN DIGITAL LIFE		1	2 %
12	UCY -- UNIVERSITY OF CYPRUS		1	2 %
13	UM -- UNIVERZA V MARIBORU		3	7 %
14	UMA -- UNIVERSIDAD DE MALAGA		2	4 %
15	UMU -- UNIVERSIDAD DE MURCIA		1	2 %
16	UNILU -- UNIVERSITE DU LUXEMBOURG		1	2 %
17	UNITN -- UNIVERSITA DEGLI STUDI DI TRENTO		3	7 %
18	UPRC -- UNIVERSITY OF PIRAEUS RESEARCH CENTER		5	11 %
19	VAF -- VAF S.R.O.		1	2 %
20	VTT -- Teknologian tutkimuskeskus VTT Oy		1	2 %
Total		20	45	100 %

Countries

Number	Country	Number of registrees	Percent
1	Cyprus	1	2 %
2	Czech Republic	2	4 %
3	Denmark	1	2 %
4	Estonia	3	7 %
5	Finland	1	2 %
6	Germany	1	2 %
7	Greece	7	16 %
8	Italia	1	2 %
9	Italy	14	31 %
10	Luxembourg	1	2 %
11	Netherlands	1	2 %
12	Slovakia	1	2 %
13	Slovenia	3	7 %
14	Spain	5	11 %
15	Sweden	2	4 %
16	United Kingdom	1	2 %
Total	16	45	100 %

Gender distribution

Gender	Number of registrees	Percent
Male	40	89 %
Female	3	7 %
I prefer not to answer	2	4 %
Total	45	100 %

Total number of persons, including conductor team during active days of the exercise

Affiliations

Number	Affilication		Number of registrees	Percent
1	ABI -- ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA		2	4 %
2	ATOS -- ATOS SPAIN SA		2	4 %
3	BRNO -- Masarykova univerzita		2	4 %
4	CYBER -- CYBERNETICA AS		3	6 %
5	DTU -- DANMARKS TEKNISKE UNIVERSITET		1	2 %
6	ENG -- ENGINEERING - INGEGNERIA INFORMATICA SPA		7	13 %
7	FORTH -- FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS		2	4 %
8	JAMK -- JAMK UNIVERSITY OF APPLIED SCIENCES		9	17 %
9	GUF -- JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN		1	2 %
10	KAU -- KARLSTADS UNIVERSITET		2	4 %
11	POLITO -- POLITECNICO DI TORINO		4	7 %
12	TDL -- TRUST IN DIGITAL LIFE		1	2 %
13	UCY -- UNIVERSITY OF CYPRUS		1	2 %
14	UM -- UNIVERZA V MARIBORU		3	6 %
15	UMA -- UNIVERSIDAD DE MALAGA		2	4 %
16	UMU -- UNIVERSIDAD DE MURCIA		1	2 %
17	UNILU -- UNIVERSITE DU LUXEMBOURG		1	2 %
18	UNITN -- UNIVERSITA DEGLI STUDI DI TRENTO		3	6 %
19	UPRC -- UNIVERSITY OF PIRAEUS RESEARCH CENTER		5	9 %
20	VAF -- VAF S.R.O.		1	2 %
21	VTT -- Teknologian tutkimuskeskus VTT Oy		1	2 %
Total		21	54	100 %

Countries

Number	Country	Number of registrees	Percent
1	Cyprus	1	2 %
2	Czech Republic	2	4 %
3	Denmark	1	2 %
4	Estonia	3	6 %
5	Finland	10	19 %
6	Germany	1	2 %
7	Greece	7	13 %
8	Italia	1	2 %
9	Italy	14	26 %
10	Luxembourg	1	2 %
11	Netherlands	1	2 %
12	Slovakia	1	2 %
13	Slovenia	3	6 %
14	Spain	5	9 %
15	Sweden	2	4 %
16	United Kingdom	1	2 %
Total	16	54	100 %

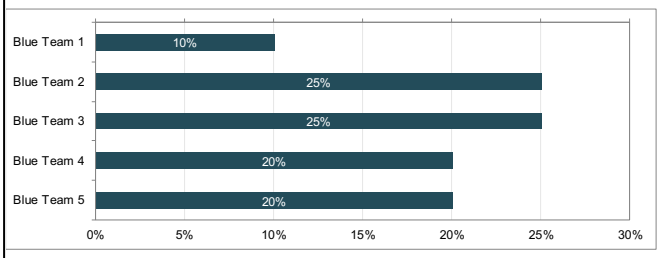
Gender distribution

Gender	Number of registrees	Percent
Male	48	89 %
Female	4	7 %
I prefer not to answer	2	4 %
Total	54	100 %

Annex D: Results of the Short Survey to Participants

Respondent's team in the exercise

Your team in the exercise?



	Blue Team 1	10 %
	Blue Team 2	25 %
	Blue Team 3	25 %
	Blue Team 4	20 %
	Blue Team 5	20 %

	n	Percent
Blue Team 1	2	10 %
Blue Team 2	5	25 %
Blue Team 3	5	25 %
Blue Team 4	4	20 %
Blue Team 5	4	20 %
	20	

Total participants 36 Answered 56 %

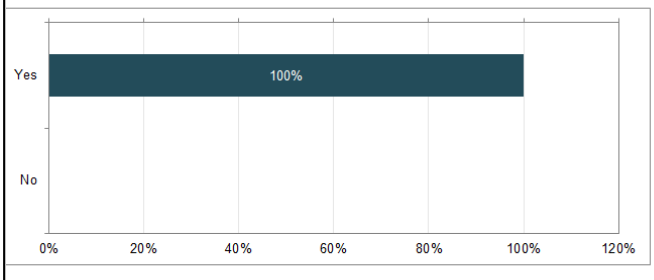
What are your feelings now?

What are your feelings now?

Responses
It's very interesting!
The challenge is very interesting and articulated. I found hard to jump from purely technical tasks to communications tasks
Anticipating and suspicious. It was fun. The time was a bit short. And I think it would have been better in person, because it was a bit difficult to get the teamwork going. We had one person who did most of the investigating and it was difficult to distribute tasks between everyone.
Very satisfied and excited.
A really nice environment.
Good, a lot of new and interesting things for only two days
Good, it was great learning experience
it was great fun
Feeling good, inspired.
I have learn some important things about forensics and I had fun. Also I think we worked really well inside the team and we get really near the end of the exercise.
Cool exercise and I think that we had absolutely the best coach! Like I mentioned in the pre-survey, I didn't have prior experience on cyber exercises so this was a really good first experience.
The exercise was funny and interesting.
Superb platform, interesting scenario, good guidance from Salo.
A bit tired, but glad that I participated.
need more!
I found the exercise really interesting.
I am really glad that I took part in this exercise. Thank you all for the hard work.
Very good!
Mixed, but with a good touch :D
I feel good. I learned something new!

Did you find the exercise beneficial for you?

Did you find the exercise beneficial for you?



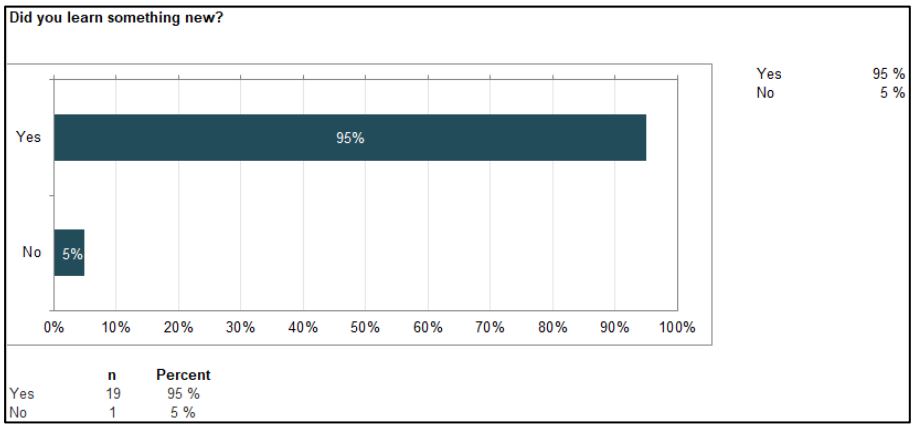
	Yes	100 %
	No	0 %

	n	Percent
Yes	20	100 %
No	0	0 %

If yes, please describe what made the exercise beneficial.

Responses
It's a great way to learn.
I am learning how to conduct forensic investigations and deal with policies like GDPR
I got a first look at the tools that can be used for finding evidence on a breach. I have no experience with such things from when I was at the University (which was some time ago) and in my day-to-day work I do not have any connection with them.
I know new and very useful tools
Learned a lot. The teamwork was perfect. Also learned a lot about specific tools which the environment included.
To learn the overall methodology and using new tools
Learned procedures, methodologies and teamwork around cybersecurity
got some ideas on various existing tools
Understanding the pressure of limited time, urgency of investigation and how exhausting such investigation is.
I've learnt a lot of things about forensics.
Now I have idea on how these exercises really work.
I learned to use new tools.
New tools and techniques + teamwork.
Practicing using log and packet analysis. Cooperating with people with different backgrounds remotely.
get a little of overall info about the subject
I had a good overview of the different aspects of incident response.
It was great to have access to the tools siam and fpcap! This is a great environment to practice reasoning about such attacks.
I was exposed to a very good cyber range.
It has been good to see how a team must collaborate and communicate to protect an organization. In addition I learnt how much is important to make the righ communication alert (like Official alert).

Did you learn something new?

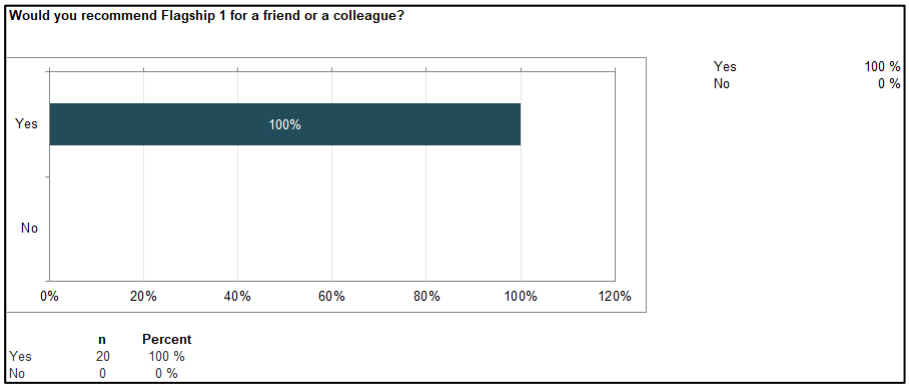


	n	Percent
Yes	19	95 %
No	1	5 %

If yes, please describe what you learned.

Please describe what?
Responses
Methodologies and tools.
I am learning how to conduct forensic investigations and deal with policies like GDPR
See answer 4.
I know new and very useful tools
Learned a lot. The teamwork was perfect. Also learned a lot about specific tools which the environment included.
Also received some important lessons - like to do adequate and up-to-date documentation of your investigation.
The idea behind incident investigations and how to approach those situations
procedures, methodologies and teamwork around cybersecurity
for the first time participated in such exercise, thus almost all for new to me
How to use elastic search
I've learnt a lot of things about forensics.
I didn't have previous experience on SIEM and my experience on FPCAP was from many many years ago. In general I learned how the SIEM and FPCAP are used to find clues, i.e. where (which servers, apps, etc.) to login and find files and other information.
Use of new tools.
New tools and techniques + teamwork.
The communication guidelines in case of cyber attack were helpful. Apart from the exercise, it also surprised me how different the skill levels of CS4E project members are. Some were quite advanced, and other lacked even the basics that I would expect them to have.
some general info
I learned the basics of many new tools (e.g. SIEM).
This was my first exercise, so there are a lot of new things I have learned and experienced. The (kind of) real world experinence, tools etc. Working in a team was also fun.
Tools siam/fpcap and reasoning within topology.
It has been good to see how a team must collaborate and communicate to protect an organization. In addition I learnt how much is important to make the righ communication alert (like Official alert).

Would you recommend Flagship 1 for a friend or a colleague?



	n	Percent
Yes	20	100 %
No	0	0 %

Free feedback about Flagship 1

Free feedback about Flagship 1
Responses
It is a beautiful experience, very informative and fun.
Really nicely prepared, Joni was a really nice coach and we all as a team worked nicely together in spite of the fact that we didn't know each other before.
Nice course! Hope to get similar courses in the future
very interesting and great fun. Thanks
Keep up the good work. I would make security policy more real-world, though. And it would be beneficial to go over basic tool usage before "jumping in". Though the tools on the market are similar, the differences make the progress harder with no time to get familiar with the tools.
Thanks for organising this and I'm really much looking forward to the Flagship 2 :-)
It is good and useful, to say something bad, it is really complicated to familiarize with all the enviroment and the tools.
Keep up the good work!
Waiting for Flagship 2 ...
Big thanks to our coach Marko for a great approach. He asked guiding questions to direct us toward the solution but at the same time did not reveal everything.
thanks for all attempts and environment, it really needs to be held physically. virtual experience is really missing a lot! maybe I can say virtual one only can capture 20-30% of the physical event.
Teemu was an excellent coach! Knowledgeable, patient and kept things moving in the right direction. I think the coach was a significant (positive) factor in the exercise.
Very good exercise which definitely gave a realistic insight to an incident response scenario. I would prefer to have the cyber range open for some night hours as well and have the flexibility to work the scenario on any given time for those two days. And also be part of a team with my colleagues, so we could organize and schedule the work on our own pace and methodology. Having someone to "guide" us in the team was a nice touch!
I'd like to know a little bit better how to use toll such as SIEMs etc. before the exercise in ordert to be more efficient. In addition, I feel that a remotely carried out exercise is more difficult to follow as you are inevitably involved in other parallel activities. But you know, this is due to the current situation :)