Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

Cybersecurity cOmpeteNCe fOr Research anD InnovAtion[†]

Work package 3: Community impact and sustainability

Deliverable D3.3: 3rd year report on community building and sustainability

Abstract: D3.3 provides an overview of the key CONCORDIA WP3 achievements in Y3. We present an overview of the status and the key results we attained in each of the four tasks, and our way forward for Y4.

Contractual Date of Delivery	*Dec 31, 2021*
Actual Date of Delivery	*Dec 22, 2021*
Deliverable Dissemination Level	*Public*
Editors	*Marco Caselli (T3.1)* *Cristian Hesselman (T3.2)* *Thijs van den Hout (T3.2)* *Reinhard Gloger (T3.3)* *Felicia Cutas (T3.4, D3.3)*
Contributors	*Siemens* *DFN-CERT* *SIDN* *CODE/MUNI/BADW-LRZ* *EIT Digital*
Quality Assurance	*DFN-CERT* *Telecom Italia* *University of Lorraine* *RISE*

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as replacement for EFACEC Energia)	Portugal
ARTHUR’S	Arthur’s Legal B.V.	Netherlands

LEGAL		
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia

Document Revisions & Quality Assurance

Internal Reviewers
Christian Keil, DFN-CERT (review lead)
Paolo De Lutiis, Telecom Italia
Thibault Cholez, University of Lorraine
Shahid Raza, RISE

Revisions:

Ver.	Date	By	Overview
1.0	*2021-11-12*	*Felicia Cutas*	*Send file for internal review phase 1*
1.1	*2021-11-30*	*Felicia Cutas*	*Send file for internal review phase 2*
1.2	*2021-12-15*	*Felicia Cutas*	*Submission*
2.0	*2022-05-05*	*Felicia Cutas*	*Ready for publication*

Disclaimer:
The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

Executive summary

The goal of WP3 is to reinforce Europe’s cybersecurity leadership by developing and evaluating building blocks for a European cross-sector cybersecurity infrastructure, specifically for collaborative threat handling, technology and service experimentation, training and education. WP3 utilizes WP1’s technology developments and WP2’s industry pilots in some of the tasks. This inter-WP cooperation has been successfully enhanced in Y3.

The overall Year 3 WP3 achievements include the following:

- Task 3.1 “Building a Threat Intelligence for Europe” has successfully met Y3 targets by establishing and deploying the basic technological components for implementing services related to threat intelligence. Examples of these services are sharing threats, early notification of incidents, etc.. The employed technologies include a variety of open-source software (e.g., MISP) and solutions developed by partners in previous projects (e.g., the ICH). The aforementioned components, together with the DDoS-CH of Task 3.2, make the core of the “CONCORDIA Platform for Threat Intelligence”, namely the project’s central point of contact for all services related to threat intelligence. The scope of the platform, together with a preliminary description of the related operational requirements and processes, has been comprehensively discussed over the last year and organized within its “Code of Engagement” presented in T4.2
- Task 3.2 “Piloting a DDoS Clearing House for Europe” is on track toward carrying out our pilots in the Netherlands and Italy, which is the task’s ultimate objective. Our key accomplishments in Y3 were: (1) we developed a distributed testbed to test the DDoS Clearing House prototype in a realistic, production-like environment (TRL6), (2) we further improved the individual components of the DDoS Clearing House, resulting in a stable framework, and (3) we finalized the technical preparations for the pilots.
- Task 3.3 “Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Training” is on track to create a cybersecurity ecosystem to validate and demonstrate CONCORDIA’s results and to foster cybersecurity trainings. A steadily growing inventory of tools, cyber range platforms, and training offerings have been created. KYPO Cyber Range Platform is released as open source. Topology and training content across cyber range platforms in CONCORDIA have been prototyped and integrated in cybersecurity education and certification.
- Targeting the development of an EU-wide cybersecurity educational ecosystem, Task 3.4 “Establishing an European Education Ecosystem for Cybersecurity” ran the pilot and the first open course targeting cybersecurity consultant profile and the associated skills certification scheme. Task 3.4 also collected input regarding the Teach-the-Teachers activity from teachers, students, parents of students from the high-school level via survey and interviews. The courses map was revamped and the collaboration with the other 3 pilot projects (SPARTA, ECHO, CyberSec4Europe) under the CCN Education cross pilots' group continued.

Contents

1. Introduction

The goal of CONCORDIA's WP3 is to develop building blocks for a *European cross-sector ("horizontal") cybersecurity infrastructure*, specifically for:

- Collaborative threat handling (T3.1, T3.2),
- Developing and evaluating new technologies and services (T3.3),
- Training and education (T3.3, T3.4).

Table 1 provides an overview of the key building blocks that WP3 provides and the tangible forms that they take:

- *Technical designs (TD)*, such as for cybersecurity platforms (e.g., for threat intelligence), labs, testbeds, and tools (e.g., simulating adversary behaviour)
- *Methodologies (M),* for instance for setting up pan-European cybersecurity courses, trainings, and start-ups.
- *Use cases (UC)* of the technical designs and methodologies, for instance through actual cybersecurity courses and technical pilots.

For example, the DDoS Clearing House (T3.2) consists of a technical design that we will use twice through a pilot in the Netherlands and in Italy and that will also result in a "cookbook" (methodology) that discusses how to develop, setup, and govern a DDoS Clearing House. Similarly, CONCORDIA's educational actions (T3.4) focus on developing methodologies and frameworks to design, certify, and teach courses for cybersecurity professionals, mid-managers, executives, and teachers as well as describe processes for using them.

Table 1: Key building blocks of CONCORDIA's cross-sector cybersecurity infrastructure.

WP3 key building block	Output	Task
An *intelligent decision support system* for incident response teams using a shared threat intelligence platform	TD, M, UC	T3.1
A *DDoS Clearing House* for proactively and collaboratively handling DDoS attacks using DDoS fingerprints	TD, M, UC	T3.2
A *virtual lab* for other CONCORDIA WPs, trainings, and (smaller) European cybersecurity companies in a post-CONCORDIA era	TD, M, UC	T3.3
Hands-on *trainings for operational teams*, for instance based on the concept of "cyber ranges"	TD, M, UC	T3.3
Cybersecurity *educational instruments* such as courses and curriculums for professionals and high-school teachers (as part of the EEEC)	M, UC	T3.4

The rest of this report provides an overview of the main results of WP3 in 2021 and outlook for 2022, with a separate section for each of WP3's tasks (Sections 2 through 5). The individual tasks related sections are organized by following the same structure: after stating the task objective we briefly introduce the results of the previous year and then move to describing the work performed in Y3 before closing with listing the activities planned for Y4, The document concludes with the overall status of WP3 and next steps in Section 6.

1.1 Covid-19 Pandemic Effects in Y3

The overall impact of COVID-19 on WP3 activities was well contained. Despite the shutdown effects, the WP3 activities were adapted to achieve the task/WP objectives. Overall WP3 sustained its activity cooperation with the expanded use of virtual project management tools such as Confluence, Github, Teams and others.

- T3.1 - With the transition to the new working conditions completed in 2020, there has been no further impact on the task activities due to Covid-19.
- T3.2 - The implementation of the DDoS Clearing House pilot in Italy suffered from 6 months delay due non-core activities at TIM being put on hold as a result of the lockdowns there. In the meantime, we worked on the preparations of the two pilots and the development of a testbed. Other than that, no results of the pandemic had a negative impact on the activities in the task.
- T3.3 - Training activities planned in 2020 have been postponed successfully to year 2021. Beyond that, activities have been realized with strict sanitary restrictions (or electronically). Labs development was delayed (appr. 3 –4 months) due to access problems (esp. remote access for the cybersecurity ecosystem), but partners will regain lost time.
- T3.4 - The task continued to run the CONCORDIA course "Becoming a cybersecurity consultant" fully online thus replacing the face-to-face module with live webinar. This approach had positive effects in ensuring the participation of a large and diverse group of participants but offered a lower than desired level of interaction and networking.

1.2 Addressing the comments of the reviewers from the M24 review report

Following the general recommendations received from the reviewers, we are summarizing below the main elements linked to the individual tasks efforts toward going beyond the state of the art in the task specific domain, the collaboration with the other pilots and the engagement with the stakeholders. Details could be found in the tasks' specific chapters.

- Going beyond the state-of-the-art
    - T3.1 - We augmented Security Metrics with a statistical method (ARIMA) facilitating forecasting future values and detecting anomalies. This work has been published as a scientific contribution in WP1 where we demonstrated the achievements of this approach. Furthermore, we deepened the research on incident response formats and standards to be leveraged in the "incident response automation" sub-task. This effort has been condensed and published in a scientific paper at "IEEE Communications Surveys and Tutorials" under the title "A comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective". Also in this case, the paper has been included within WP1 scientific contributions.
    - T3.2 - The DDoS Clearing House was selected for the Innovation Radar of the European Commission. We elaborate further about progressing the state-of-the-art in section 3.4.
    - T3.3 - The task addresses Cyber range infrastructures with an approach based on cooperation by creating the content ecosystem rather than creating a tight integration of cyber ranges. It means CONCORDIA delivers a format for sharing content between cyber ranges and encourages organizations inside and outside the consortium to use it. This approach is supported by an open-source cyber range - KYPO Cyber Range Platform.

    - T3.4 - The task deployed two instances of the course and the associated skills certification scheme addressing the Cybersecurity Consultant, a role profile not previously defined in the EU.
- Collaboration with other pilot projects
    - T3.1 - Besides the already existing continuous collaboration with CyberSec4Europe, CONCORDIA's Platform for Threat Intelligence now also shares information with CyberSane and AI4HealthSec.
    - T3.2 - This task did not collaborate with the other EU pilot projects in Y3, because, to the best of our knowledge, the other pilot projects do not work on DDoS mitigation.
    - T3.3 - We continue in cooperation with the other pilots (ECHO, SPARTA, CyberSec4Europe) and H2020 projects (THREAT-ARREST) in the area of cyber range platforms and cyber range based trainings. Furthermore, T3.3 participates in CCN's Cyber Range Focus Group and leads one of the activities in the group.
    - T3.4 - CONCORDIA is leading the cross-pilots group on Education strand; during Y3 the group had quarterly meetings exchanging on pilots' priorities. Between the common activities: support ENISA's effort in validating a cybersecurity skills framework; finalize the transfer of courses databases to ENISA map; participate in online open events.
- Engagement with stakeholders
    - T3.1 – Many exchanges and a dedicated workshop have been organized with CIRCL and the developers of MISP to discuss current challenges and ways forward (especially in the sharing of threat intelligence related to telecommunication). The result of this collaboration was the development of a MISP Galaxy and some new MISP features to be integrated in the new releases.
    - T3.2 - This task intensely collaborates with the Dutch anti-DDoS coalition; a group of 16 organizations that will run the DDoS Clearing House in production after CONCORDIA. We are also in close contact with the Italian stakeholders with whom we will pilot the Clearing House as well. We actively share the results of T3.2 with the cybersecurity community; see section 3.9 for our dissemination results.
    - T3.3 - The Collaboration in virtual Labs and cyber ranges will be increased to enhance functionality and the cyber range community to exchange scenarios is built up to create added value.
    - T3.4 - The task engaged with stakeholders on different levels, from social-media campaigns and surveys to direct interviews and online events. A special attention was given to the project website where the Education specific section was periodically populated with new content and further disseminated via newsletter. The specific interaction with ENISA and ECSO is reported as part of the work under the CCN Education focus group.

2. Building a threat intelligence platform for Europe (T3.1)

2.1 Task objective

The aim of Task 3.1 is to build and operate the **CONCORDIA Platform for Threat Intelligence**, a logically centralized system that enables players from different sectors to **share and work on threat intelligence** in a trusted way. On a technical level, the platform will be able to store, analyze, and distribute threat intelligence. On an operational level, the platform will organize and guide the consortium work on threat intelligence through its **"Code of Engagement"** and foster the development of new services.

The CONCORDIA Platform for Threat Intelligence will be based on open source as well as previously existing components, such as the Malware Information and threat Sharing Platform (MISP) and the Incident Clearing House developed in the project "Advanced Cyber Defence Centre" (ACDC). Furthermore, it will leverage components developed within other tasks such as the "Distributed Denial of Service Clearing House" in T3.2.

2.2 Preamble

All contributions provided within the first two years of the project (and, thus, already included in D3.1 and D3.2) have been summarized in Section 2.3. This decision has been made to keep the deliverable self-contained and let the reader focus on the new outcomes and achievements while easily placing them in the context of the overall task's activities. Information related to the platform scope (as requested by Milestone 3.8 "Finalization of Threat Intelligence Platform Scope") is instead addressed in a dedicated section (Chapter 8).

2.3 Status

Task 3.1 is on track and fulfilled the envisioned targets of Y3. In the first two years of the project, we defined and developed all key architectural components of the CONCORDIA Platform for Threat Intelligence and described several possible use cases. In addition, we comprehensively discussed and advanced several complementary topics defined in the description of work such as "incident response automation". In Y3, we shifted the focus on the operationalization perspective with a strong focus on use cases (e.g., how is the CONCORDIA Platform for Threat Intelligence going to be used?) and on the "Code of Engagement", namely a set of rules and guidelines driving the use of the CONCORDIA Platform of Threat Intelligence as well as its future developments. In the last year of the project, we plan to complete all development activities and ensure that all CONCORDIA partners can smoothly integrate T3.1 solutions with their own security toolchains as well as easily align their internal processes related to threat intelligence to the principles of the "Code of Engagement".

2.3.1 CONCORDIA Platform for Threat Intelligence

In the context of T3.3 ("Developing the CONCORDIA's Ecosystem: Virtual Lab, Services and Training"), task 3.1, as well as task 3.2, fits the concept of delivering CTI-related services and support to the CONCORDIA stakeholders. For this reason, in Y2, together with task 3.2 (in the context of the so-called “T3.1/T3.2 Liaison”), we focused on aligning the respective contributions within the broader landscape provided by T3.3. The main outcome of this effort is the joint technological architecture view for the CONCORDIA Platform for Threat Intelligence.

Figure 1 provides a schematic overview of the platform with its main components, their interactions, and the key involved technologies.

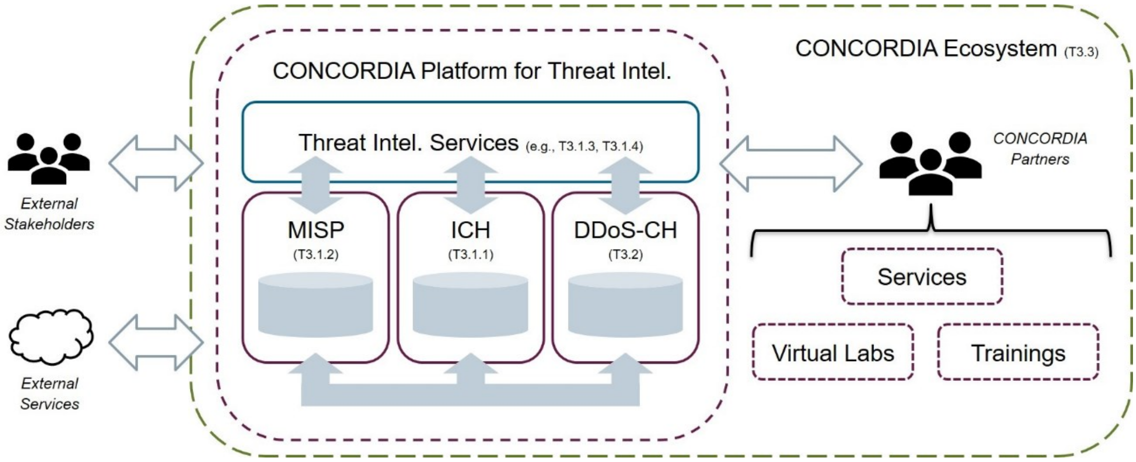


Figure 1: CONCORDIA Platform for Threat Intelligence

The CONCORDIA Platform aims at *building one central point of contact for all services related to Threat Intelligence.* The idea develops along with three main principles or guidelines:

- ***A virtual platform***: the CONCORDIA Platform will consist of a collection of software solutions running on heterogeneous technologies and providing different services.
- ***Compatible models and structures****:* services provided by the platform will take advantage of each other, mutually exchanging information and jointly contributing to support possible new features.
- ***Uniform engagements rules****:* policies to access services and data should be aligned and integrated as much as possible to guarantee straightforward and trustworthy interactions to the users of the platform.

The main technological components, aka **core components**, corresponds to three solutions developed within T3.1 and T3.2. The former task focuses on threat intelligence sharing and contributes with a platform allowing the creation and retrieval of "Indicators of Compromise" (MISP) as well as an infrastructure to deliver cyber incident notifications and support (the "Incident Clearing House"). The latter task focuses instead on Denial of Service attacks and delivers a platform implementing a proactive, coordinated, and distributed DDoS defense strategy (the "DDoS Clearing House"). Together, the core components form the backbone of the CONCORDIA Platform for Threat Intelligence. Beyond the core components, the CONCORDIA Platform envisions the development of **accessory components** or, simply, **services**. Those components will come from ideas and contributions collected within T3.1 and T3.2 by both the responsible project partners (Siemens, DFN-CERT, SIDN) and the supporting ones (e.g., FORTH, Telecom Italia, etc.).

The accessory components will interact with the core ones to deliver increasingly complex services eventually becoming a fully interconnected infrastructure supporting all CONCORDIA stakeholders in dealing with threat intelligence information and making the best use of it to improve their security postures.

Core Components

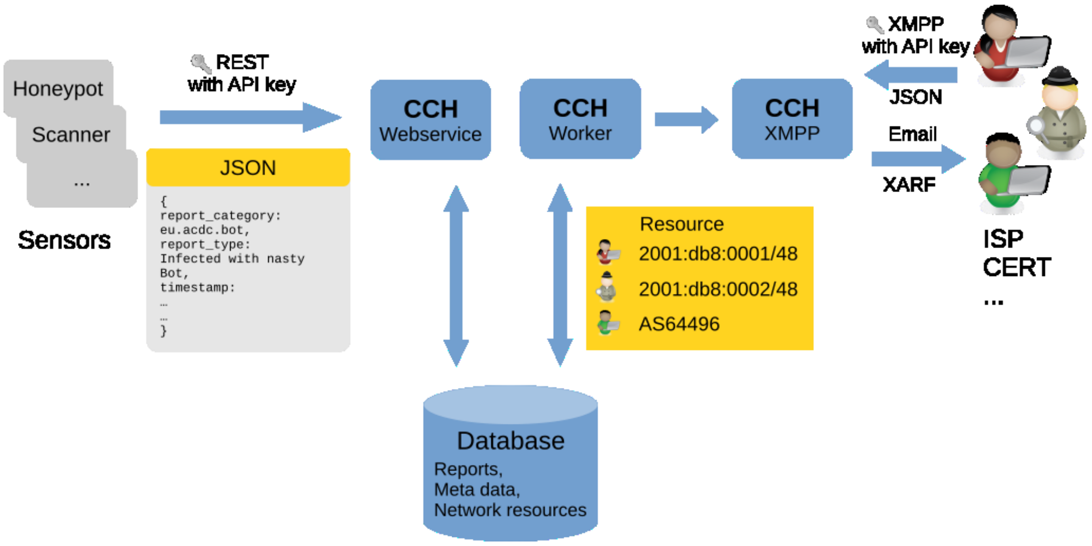
MISP –Within CONCORDIA, the central MISP instance represents one of the core components of the envisioned CONCORDIA Platform for Threat Intelligence sharing. MISP was deployed at DFN-CERT in Y1 and is currently managed cooperatively by Siemens AG (principal and formal responsible) and DFN-CERT itself. Besides its custom configuration, the central MISP instance is envisioned to expose new features and functionalities developed within CONCORDIA.

For what concerns the current use of the platform, a selected number of CONCORDIA participants (mostly related to the CONCORDIA "Telecom" and "Finance" pilots) started testing and interacting with the central MISP instance in Y1 paving the way to the official roll-out face in Y2. Among the active partners, it is worth mentioning that, over Y2 FORTH worked on customizing and deploying security solutions (e.g., honeypots and firewalls) with the goal of providing all results produced by these systems to the CONCORDIA Platform for Threat Intelligence. To share data easily and effectively, FORTH decided to deploy a local MISP instance and populate this with information retrieved by the aforementioned security solutions. FORTH was able to daily produce a "top 10" of notable IP addresses (potentially attackers) and transfer those IPs to the CONCORDIA MISP instance to make them eventually available to all partners.

As a principal advantage, MISP follows and implements important standards and norms in information security. An important role in providing trust in information sharing by MISP[1] plays the ISO/IEC 27010:2015 norm which implements information security management. Support of open technical standards such as STIX[2], Yara[3], and multiple formats of IDS signatures fosters interoperability with common security tools including frequently deployed SIEM (Security Information and Event Management) and IDS (Intrusion Detection System) solutions such as Splunk, QRadar, Exabeam, Snort, Suricata, and Bro/Zeek.

Incident Clearing House (ICH) – The Incident Clearing House notifies subscribers to the platform of security related information regarding their registered network resources. This mainly includes outgoing network activities from their resources – like password guessing attacks, spam emails, or connections to a botnet sinkhole – that indicate compromised or misused systems, but also vulnerable set-ups like running services that expose known vulnerabilities to the internet.

[1] https://www.misp-project.org/compliance/ISO-IEC-27010/
[2] https://oasis-open.github.io/cti-documentation/stix/intro
[3] https://yara.readthedocs.io/en/stable/



```
{
report_category:
eu.acdc.bot,
report_type:
Infected with nasty
Bot,
timestamp:
…
…
}
```

Figure 2: Incident Clearing House architecture

The architecture of the ICH can be seen in Figure 2. Incoming data from sensors is consumed by a web service and stored in a database. From there it is picked up by a worker process, attributed to the correct subscriber according to their registered network resources, and forwarded over the preferred connection.

DDoS-CH – is discussed in Chapter 3

2.3.2 Incident Response Automation

Among its main objectives, CONCORDIA aims at enhancing current approaches to threat intelligence sharing, identified as a key enabler to support and advance cybersecurity in Europe. As cyberattacks keep increasing both in time and complexity, security teams such as CSIRTs and SOCs face the challenge of improving the exchange of threat intelligence to respond to these threats quickly and effectively. In this regard, one of the aspects CONCORDIA proposes to tackle relates to the use of threat intelligence information describing “incident response activities”. Specifically, T3.1 investigates the representation of these activities as a standardized “course of actions” (or “playbooks”) that can be easily interpreted and shared within the cybersecurity community. Furthermore, T3.1 explores the possibility of taking advantage of this representation to automate the incident response process, improving state-of-the-art orchestration approaches. The overall approach, named "Course of Action (CoA) Deployment Architecture" is shown in Figure 3.

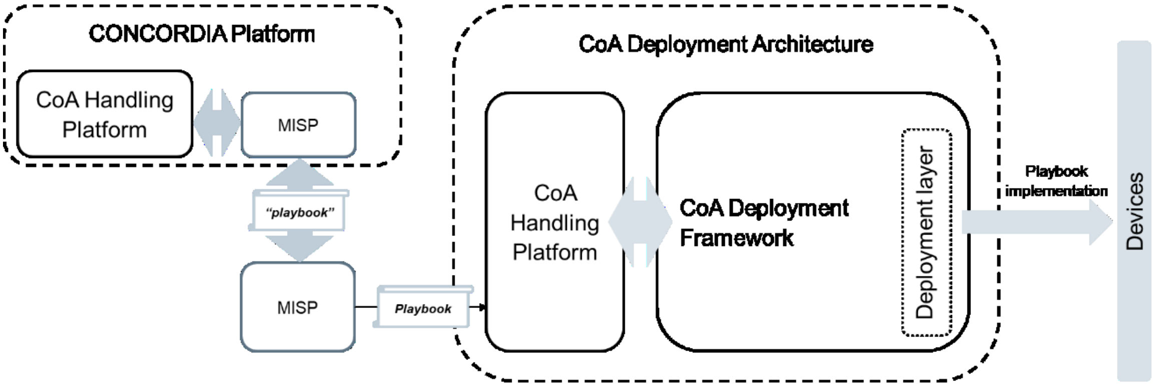


Figure 3: Incident Response Automation Overview

2.4 Key achievements Y3

2.4.1 Enhancements to MISP

One key activity of Y3 was the improvement of the intrusion detection export functions in order to accommodate the DDOS signatures defined in T3.2. These new features and functionalities have been aligned with CIRCL and are currently under assessment to become part of the next MISP releases and, thus, will be deployed world-wide together with the official platform.

2.4.2 Use Cases

Besides the technical development, during Y3, a few use cases have been drafted to explain possible ways the CONCORDIA Platform for Threat Intelligence could operate and, even more importantly, to identify further requirements and constraints that might have been overlooked at the beginning of the project. The use cases were also useful to foster a discussion on possible new accessory components or services to be developed on top of the core components. What follows is a major example discussed over dedicated workshops with selected partners.

Support against DDoS Booters

In this scenario, we describe the usage of the CONCORDIA Platform for Threat Intelligence in response to the emergence of a new DDoS Booter service and the related cyberattack campaigns. DDoS Booters (also "IP Stressers") are tools legitimately employed to test the robustness of IT networks. Malicious actors can however misuse tools of this kind to generate Denial of Service attacks. In some cases, these tools can be sold in the dark web (as Saas) to support cyberattack campaigns of third parties. In the development of this scenario, the three main core components operate and interact with each other.

In the context of a cyber-security improvement program, a team of the company "José Arcadio" (a company participating to the CONCORDIA Ecosystem) starts gathering information about new Booter services sold in the dark web. All collected information is pushed to their local MISP instance and, consequently, synchronized with the central CONCORDIA MISP instance (Figure 4). Among this information, a report of a new exceptionally effective Booter service called "Prudencio" informs of emerging DDoS campaigns taking advantage of this tool and targeting financial companies.

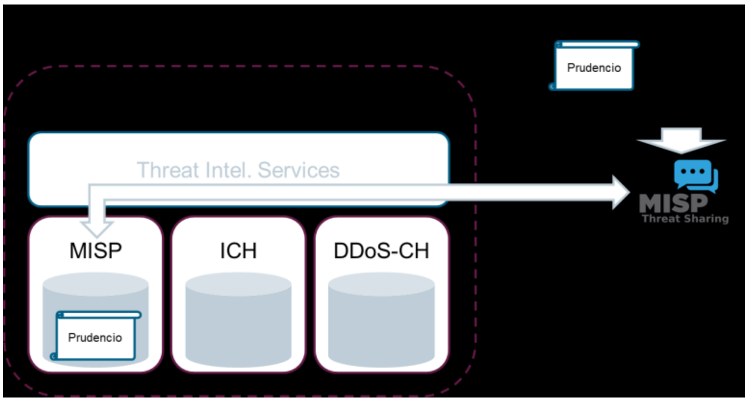


Figure 4: Information about DDoS Booter pushed to MISP

Meanwhile, the Incident Clearing House starts receiving notifications of compromised systems having used the "Prudencio" attack framework to launch DDoS attacks on the

Internet (Figure 5). Among these notifications, one forensics investigation reveals that a specific compromised server refers to an IP registered with the Incident Clearing House and belonging to another company of the CONCORDIA Ecosystem, the investor group "Ursula IG". Immediately after receiving the notification, the Incident Clearing House automatically warns the security team of "Ursula IG" security team and references any useful information currently available in the central CONCORDIA MISP instance (Figure 6). At the same time, the DDoS Clearing House also observes the last developments of Denial of Service campaigns related to "Prudencio" and begins collecting fingerprints to detect and, thus, neutralize the attack (Figure).

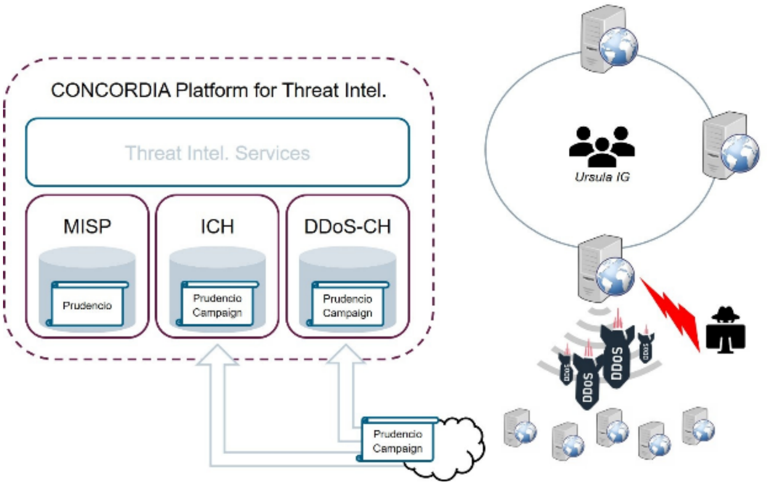


Figure 5: Observations of malicious activities on the Internet

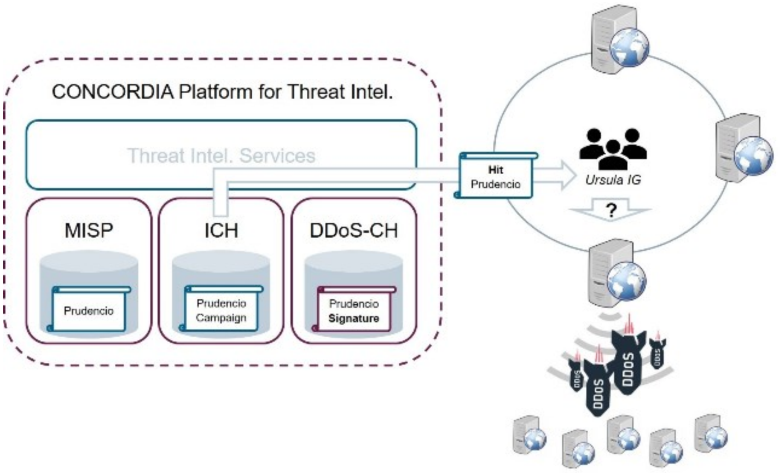


Figure 6 : Notification of the Incident Clearing House

After the notification from the Incident Clearing House, the security team of "Ursula IG" verifies the problem and confirms the incident: one of their web servers has been compromised. At this point, the team checks all available threat intelligence accessible on the central CONCORDIA MISP instance and starts organizing incident response (Figure 7). While checking, the team receives one extra notification from the DDoS Clearing House signaling the availability of detection signatures for "Prudencio"-related Denial of Service campaigns. The incorporation of those signatures within the previously deployed security toolchains (e.g., intrusion prevention and detection systems) allows "Ursula IG" to protect its other web servers against the same attack while the compromised one undergoes recovery (Figure 8).

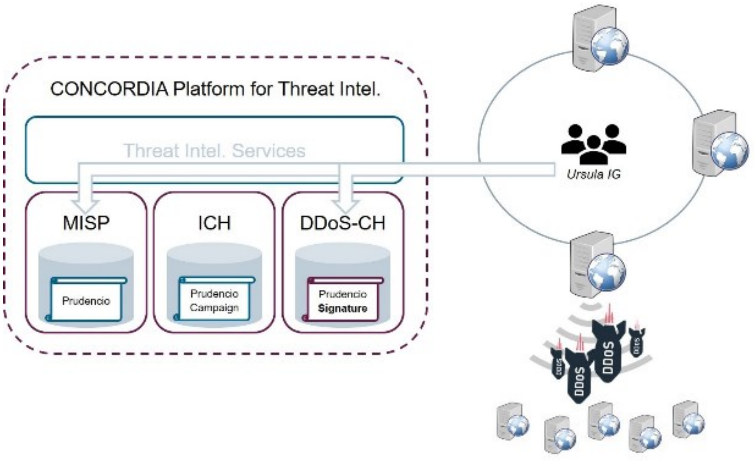


Figure 7: Request for information about the on-going incident

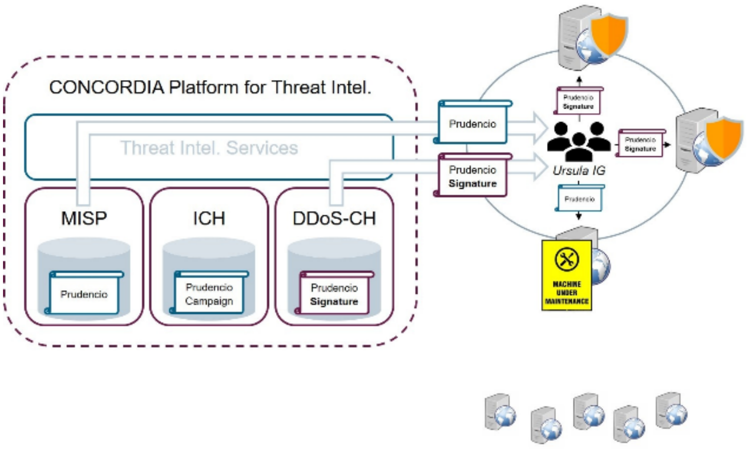


Figure 8: Retrieval of information about the on-going incident

The described scenario emphasizes the coordinated action of the core components and outlines their different roles and direct communication with the users (driven by the "virtual platform" principle). These aspects also highlight the importance of integrating the services of the platform with the security toolchains employed user-side. This is particularly visible in the fairly transparent deployment of detection rules once a given threat has been identified and recognized. As mentioned at the beginning of the chapter, integrating the CONCORDIA Platform for Threat Intelligence with tools used by the CONCORDIA partners has been continuously discussed over Y2 and Y3 and some of the outcomes are already deployed and discussed in the following section (the point related to Flowmon) and in Chapter 3 (where the technical details of the deployment of DDoS signatures are described in depth).

2.4.3 Cross-Task/Work Package contributions

Besides the already mentioned collaborations with T3.2 and T3.3, T3.1's stakeholders hold monthly alignments with the other partners involved in WP3. In this regard, it is worth mentioning the cross-task collaboration with T3.3 on aligning the design and development of the CONCORDIA Platform for Threat Intelligence with the ramp-up of a broader and heterogeneous CONCORDIA ecosystem as well as the possible touching points with the CONCORDIA Cyber Ranges (e.g., the use of ad-hoc instances of the CONCORDIA Platform for Threat Intelligence for learning purposes as well as within blue-team/red-team training activities).

Beyond the scope of the working package, we have been active in sharing results across the whole CONCORDIA project and leveraging competences and results coming from all partners and even beyond the project (e.g., cross-pilot collaborations). Among the most prominent collaborations, it is worth mentioning the ones with:

- T2.1 on the definition of cyber threat intelligence data structures (related to the telecommunication domain) as well as the generation of ad-hoc detection rules based on the shared information. This activity has been integrated by a continuous exchange with CIRCL culminating in a dedicate workshop in which CONCORDIA telecommunication partners proposed their ideas towards a novel “Mobile Threat Modeling” Framework. These concepts have been eventually organized within a MISP Galaxy that, once finalized, will be pushed into the official CIRCL repository.
- T2.2 on the definition of cyber threat intelligence data structures (related to the finance/banking domain) as well as the definition of the related exchange processes. This activity has also benefited from a continuous exchange with CyberSec4Europe and, specifically, with the partners of the consortium involved in the financial sector as well. This activity is currently aiming at extending the respective boundaries of threat sharing and implement a stable cross-pilot flow of information.
- T4.1 on the definition of cyber threat intelligence taxonomies and ontologies to be integrated with the solutions proposed within T3.1 (e.g., MISP galaxies and taxonomies). This activity paved the way to the one discussed in T2.1 in which approaches, and processes have been taken as example during the instantiation of the “Mobile Threat Modeling” Framework.
- T4.2 on the definition of the “Code of Engagement” and, thus, the legal and processual framework to regulate the overall use of the CONCORDIA Platform for Threat Intelligence by the partners and pave the way to its extension beyond the end of the CONCORDIA project. This activity is a key achievement of Y3 and provides a description of the platform’s scope from the operational perspective.
- Further EU projects to broaden the sharing of data and experiences in the context of threat intelligence. This activity corresponds to the already mentioned exchange with CyberSec4Europe as well as the established communication with CyberSane[1] and AI4HealthSec[2] implemented by interconnecting the corresponding MISP instances and agreeing on the related information flows.

2.4.4 Incident Clearing House

With the focus on the legal and processual framework of the Threat Intelligence Platform in the Code of Engagement, development work on the Incident Clearing House (ICH) was limited in Y3. As part of the ongoing improvement of interactions between the core components, access keys to the ICH can now be associated with CONCORDIA. This enables further processing and annotating of reports submitted for the network resources

[1] https://www.cybersane-project.eu/

[2] https://www.ai4healthsec.eu/

registered for these keys. Reports including botnet activity are thus automatically linked to information on the involved malware in the platform's MISP instance.

2.4.5 Security Metrics for Threat Intelligence

Following the definition of the NIST Institute[1], the main objective of a Metric is to "facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT Security Metrics are metrics based on IT security performance goals and objectives". This perfectly aligns with the overarching goal of Threat Intelligence to refine threat information to provide the necessary context for decision-making processes[2]. Thus, Security Metrics are an ideal tool for producing Threat Intelligence based on the CONCORDIA Platform for Threat Intelligence.

The Security Metric computation prototype has developed in Y3 into a basic version of a situational awareness view on the data in the ICH and MISP. Data from the DDoS Clearing House is planned to be included in this view via the integration between the DDoS Clearing House and MISP. Following the idea of a virtual platform, this follows the concept of a Threat Intelligence service built on top of the core components, expanding CONCORDIA's Platform for Threat Intelligence.

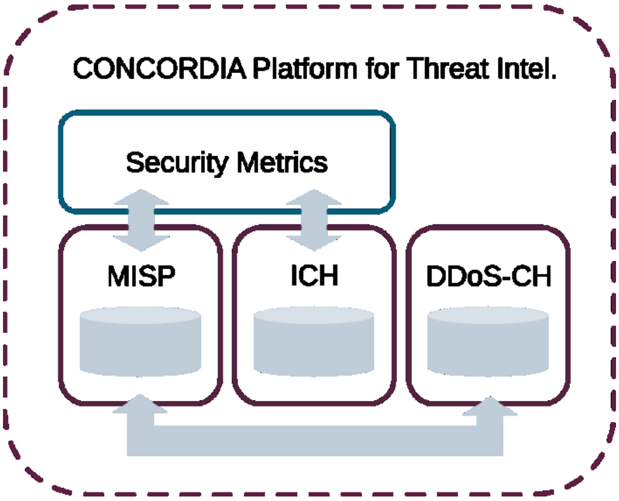


Figure 9: Security Metrics for Threat Intelligence

To provide the situational awareness view, the Security Metrics component consumes information from the ICH and MISP, computes time-based metrics, and visualises the results in multiple dashboards. The metrics essentially count how often certain features appear in the consumed information and track the development of the count over time. Features here can be port numbers in ICH reports, hashes shared as indicators in MISP, or fingerprints in the DDoS-CH. Metrics can also be computed on derived features like a geo location lookup of IP addresses. Top N views directly follow from the feature counts.

The security events ingested by the ICH and MISP provide a solid statistical overview of the current numbers of attacks and threats. A major or global threat on the Internet (e.g., a global malware outbreak) will likely result in a significant increase in these events. Thus, the data can be leveraged to detect such severe threats. Going beyond the state-of-the-art,

[1] NIST SP 800-55: Performance Measurement Guide for Information Security, https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final
[2] NIST SP 800-150: Guide to Cyber Threat Information Sharing, https://csrc.nist.gov/publications/detail/sp/800-150/final

we complemented the Security Metrics by a prototype of a statistical anomaly detection that forecasts future metric values based on previous data and flags values that diverge from the expected values. These anomalies provide an indicator for a deeper inspection by analysts (e.g., in a SOC) to identify a corresponding threat.

The Security Metrics can be used to provide information in different granularities and thus support

- obtaining a general overview of quantities and properties of data in the platform;
- investigating properties of current attacks like prevalent attack types, ports, or services;
- detecting emerging threats via metric anomalies like increasing attacks against specific ports;
- observing trends and developments in vulnerability exploitation and malware usage;
- sector-specific views for suitably annotated information.

To accomplish these objectives, information is presented graphically via dashboards. Such dashboards are a common representation of the results of Security Metrics and other metrics and became very familiar during the Covid crisis. The targeted user groups are Threat Intelligence analysts in SOCs, CSIRTs, or other security teams. It is important to note, that dashboards are used for the same reason by SIEMs and other security products.

The view provided by the Security Metrics component is related to but distinct from the Threat Landscape view developed in WP4. The Threat Landscape classifies threats into six domains and subdivided threat groups. While the Threat Landscape provides a static overview of the current state of the art on threats and cybersecurity, the Security Metrics support a dynamic overview of the landscape as observed by CONCORDIA's Platform for Threat Intelligence. This leads to two major differences in the provided information:

1. Not all threat domains in WP4 are related to Threat Intelligence. This applies, for example, to legal and organisational threats such as skill shortage, which are not considered by Threat Intelligence focussing on cyberattacks and malware families.
2. There is a large overlap with taxonomies used in MISP and the ICH that especially applies to the attack and network domains. Such domains and associated threat groups can be adopted for the computation of Security Metrics, which facilitates, for example, to derive statistical data about the frequency of specific attacks or malware families (e.g., ransomware). But even for suitable threat domains, the view provided by the Security Metrics might be biased if the available data does not reflect the global threat landscape but only some subset observable by the Threat Intelligence Platform.

2.4.6 Incident Response Automation

The work of T3.1 on incident response automation can be divided into three main building blocks:

- The first focuses on techniques to coherently represent incident response activities. In Y3 we deepened the discussion related to the representation of incident response actions. Available standards such as "Open Command and Control" Language (OpenC2[1]) and newly proposed ones such as the "Collaborative Automated Course

[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2

of Action Operations" (CACAO[1]) have been further investigated and integrated within custom threat intelligence processing toolchains. Most importantly, we examined how these standards fit the use of the MISP threat intelligence sharing platform. The result of this research has been accepted for publication in a scientific paper at the "2021 IEEE International Conference on Big Data (Big Data)".

- The second building block corresponds to the so-called "CoA Deployment Architecture" and consists of two parts. The first one focuses on retrieving and organizing courses of actions. To achieve this, we extract available courses of action from MISP and add them to a dedicated database in a consistent format. The reason behind this approach is twofold. First, it avoids directly working on courses of action that, in MISP, may be represented in different formats (e.g., courses of action could use other formats rather than OpenC2 and CACAO or be expressed by taking advantage of MISP features such as "tagging"). Second, it allows enriching courses of action with extra information (e.g., versioning).

  The aforementioned elements are implemented within the so-called "CoA Handling Platform" (shown in Figure 10). In the "CoA Handling Platform", the "CoA Consumer" is the software component responsible for communicating with any CTI sharing platform (corresponding to MISP in the CONCORDIA use case). The "CoA Handler" is the one responsible for validating the "course of actions" information, correcting (wherever needed) and storing it in a database. Finally, the "CoA Producer" is the software component used both to access the database (e.g., an operator checking or modifying the available data) and pushing data back to a sharing platform whenever a "course of action" should be shared externally.

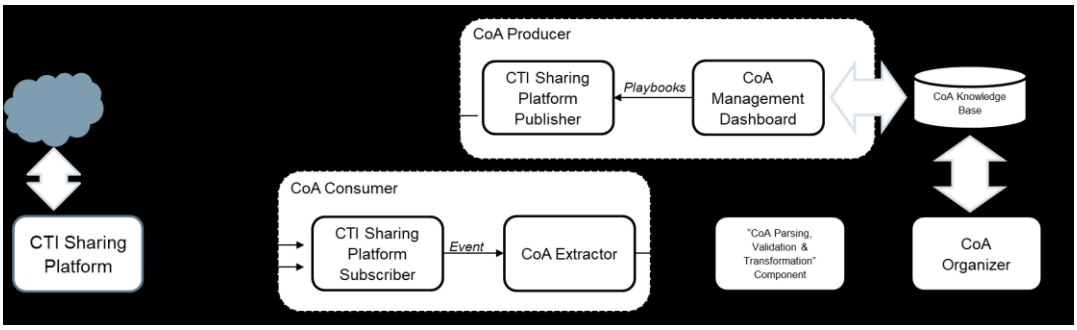


Figure 10: Overview of the "CoA Handling Platform"

The second part of the "CoA Deployment Architecture" is the "CoA Deployment Framework" and implements the process of retrieving "courses of action" and deploy them into a target infrastructure.

[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao

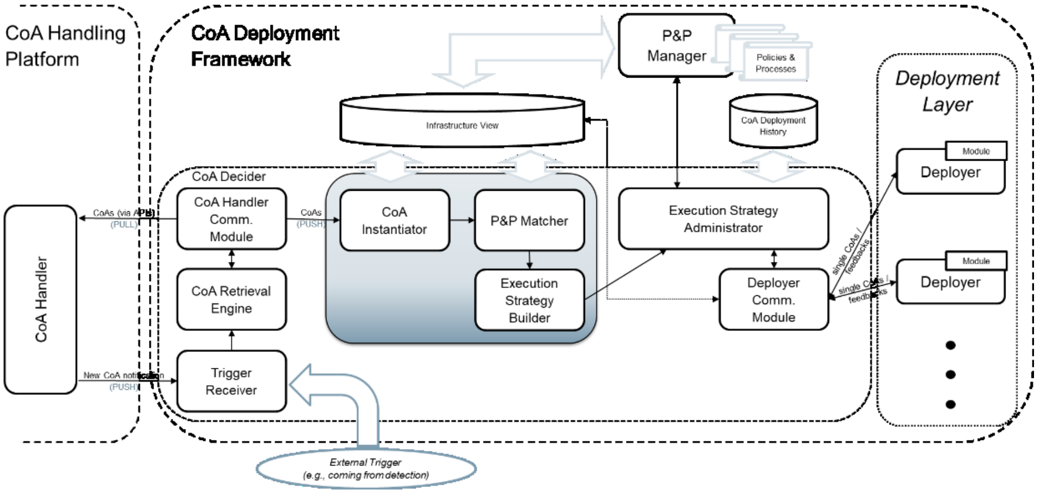


Figure 11: Overview of the "CoA Deployment Framework"

As shown in Figure 11, the “CoA Deployment Framework” consists of numerous software components. The architectural elements on the left correspond to the process of “course of actions” retrieval. When certain conditions arise (e.g., a cyberattack is detected by an intrusion detection system or an operator proactively asks for executing operations) the “CoA Deployment Framework” uses the available information (condensed under the name of “External Trigger”) to retrieve a proper “course of action” among the ones available in the “CoA Handling Platform”. If a suitable “course of action” exists, the process of instantiation begins. This process is the core of the overall approach as it transforms a set of generic technical information into the actual set that should be deployed given the requirements and constraints of the targeted infrastructures. The instantiation covers two important aspects. On the one hand, it modifies various technical parameters of the “course of actions” by replacing the actual information needed to the deployment. For example, wherever the “course of action” indicates the application of a given rule to a firewall, the instantiation process replaces the specific IPs of the firewalls in which such rule should be deployed. On the other hand, the instantiation process verifies that no single action included in the “course of actions” conflicts with incident response regulations, policies, or processes either generally applicable (e.g., GDPR) or internal to the company. For example, wherever a “course of action” might indicate to share data that might include persona information to an incident handler (e.g., sending hard drive image to a forensics analyst), the instantiation process adds a caveat (in the form of a preceding extra action) in which the permission of proceeding with the operation is explicit (e.g., by sending an email to a legal department and wait for approval). At the end of the instantiation process, the resulting “course of actions” complies with a target infrastructure as well as a company’s incident response process and is ready to be deployed. The actual execution of this last operation is implemented by the “Execution Strategy Administrator” in charge of communicating the actions to be executed to the “Deployment Layer”.

- Finally, the third building block focuses on the actual deployment of courses of action within the aforementioned environment. This approach foresees the use of simple software components called “Deployers” whose tasks are: translating actions sent by the “Execution Strategy Administrator” to a set of instructions understood by a specific device (e.g., a firewall, a proxy, etc.) and reporting back on the success/failure of operations.

The feasibility of the overall approach and a proof-of-concept implementation of the three building blocks has been shown already at the end of Y2. Over Y3, all building blocks have been improved and further tested in realistic scenarios. Especially important was the work performed on the "CoA Handling Platform" to improve the interoperability with standards such as CACAO and OpenC2. The results of the testing have been fed back to the corresponding standardization groups at OASIS to which Siemens belongs.

2.5 Outlook Y4

During Y4, we are going to complete the implementation related to the core components of the CONCORDIA Platform of Threat Intelligence as well as finalize a few services to implement the vision and reach the goals set up by the "T3.1/T3.2 Liaison". Furthermore, we are going to **promote the use of the CONCORDIA Platform** with the aim of increasing the quantity and quality of information exchange. On the one hand, we are going to support partners who did not take part in the platform's ramp-up phase in accessing and using T3.1's solutions. On the other hand, we are going to take advantage of new data structures to describe complex information (e.g., creating and importing ad-hoc taxonomies coming from the work performed in T4.1, T2.1, and T2.2).

The Security Metrics will be expanded to include data from the DDoS-CH and possibly further components of CONCORDIA's Platform for Threat Intelligence like the Incident Response Automation. We will improve the current dashboards and define new ones to **support a broader situational awareness**. This will include an investigation of dashboards that are limited to a certain subset of information like pilot-specific dashboards as well as dashboards that aggregate information over multiple components of the platform. Such aggregated views can in part be provided by component interactions like the automatic linkage of Incident Clearing House reports to malware information in MISP. We strive to research a cross-component dashboard matching information in the platform to threat groups which might be an interesting complement to the Threat Landscape view of WP4.

Moreover, we plan to improve upon the prototypic anomaly detection capabilities of the Security Metrics component to detect significant threats. A technical evaluation can, for example, be done by comparing our results with other public threat reports that detail severe attacks. Furthermore, we **plan to cooperate with SOC analysts** to improve the presentation of anomalies (e.g., in form of threat reports).

Finally, within the "T3.1/T3.2 Liaison", we are going to **enhance the "Code of Engagement"** starting by the feedback collected among the CONCORDIA partners as well as from external stakeholders. This document, together with the operational CONCORDIA Platform for Threat Intelligence, will eventually be the final deliverable envisioned within T3.1.

3. Piloting a DDoS Clearing House for Europe (T3.2)

3.1 Task objective

The objective of Task 3.2 is to **pilot** the concept of a DDoS Clearing House with European industry for Europe that enables groups of organizations to proactively and **collaboratively** protect European critical infrastructure against DDoS attacks.

The task's **two key deliverables** are a pilot in the Netherlands and in Italy and a DDoS Clearing House "cookbook" that enables other groups of organizations to set up and operate their own Clearing House.

3.2 Preamble

Last year we refined the architecture of the DDoS Clearing House components, dividing them in core- and supplementary components, and advanced their implementation. We developed a VM on which all the components of the Clearing House are pre-installed. We made initial preparations for the pilots in the Netherlands and Italy. We refer to D3.2 for the details.

We again summarize the DDoS Clearing House concept for completeness in the key achievements in Y3 section. This is background information which helps clarify our achievements and could also be found in the previous deliverable with minimal changes.

3.3 Status

T3.2 is **on track** toward carrying out our pilots in the Netherlands and Italy, which is the task's ultimate objective.

Our key achievements in Y3 are: (1) we developed and demonstrated a realistic and **distributed testbed** for the DDoS Clearing House, (2) we further improved the Clearing House components, which resulted in a **stable version** of the system, and (3) we finalized the technical preparations for the pilots.

The goal of the distributed testbed is to learn how the DDoS Clearing House operates in a realistic setting, without the members of an anti-DDoS coalition having to modify their production networks or sign data sharing agreements, which are processes that we found often take a considerable amount of time. Referring to the previous review, we would like to make clear that the DDoS Clearing House **does not use any blockchain technology**.

Our testbed operates at TRL6 ("Technology demonstrated in relevant environment") and precedes the actual pilots in the Netherlands and Italy, which will be at TRL7 ("System prototype demonstration in operational environment"). The transition to production (TRL 8-9) will take place outside CONCORDIA, such as in the Dutch anti-DDoS coalition.

In Y3, we also made progress towards the pilot in Italy. Three parties agreed to pilot the DDoS Clearing House: Telecom Italia's Security LAB, their internal SOC, and the university of Turin. More members may join their coalition in Y4.

As for outreach, we presented T3.2 and our work on the DDoS Clearing House 14 times, both outside of CONCORDIA, as well as within the project. We published 2 blogs and a demonstration video [DEMO21]. We also demonstrated the distributed testbed at the CONCORDIA Open Door event in October.

As a recognition of our work, **the EC selected the DDoS Clearing House for their Innovation Radar** in January of 2021, rating it as an explorative innovation with a high market potential [INRAD21].

Our work in Y3 follows up on our achievements in Y2. Last year, we incrementally improved the individual components of the Clearing House. In Y3, we used them to develop a stable version of the entire system, following the same iterative approach we used in Y2. We tested this stable version on the distributed testbed.

Looking forward, our focus in Y4 will be on carrying out the two pilots, further improving the Dissector and Converter modules, and delivering the DDoS Clearing House cookbook (see Outlook Y4).

We met online through our monthly T3.2 calls (12 in total) in which we discussed (preliminary) results, the status of the work, the division of work among the partners, and prepared presentations

3.4 DDoS Clearing House overview

Motivation: DDoS attacks reduce Europe's digital sovereignty
Europe and other regions around the globe have become increasingly dependent on online services, even more so after the Covid-19 pandemic [COVID]. However, these increasing dependencies also increase the impact of DDoS attacks, particularly as societies more and more connect their critical infrastructure to the Internet, such as energy grids [WODC19], water supply systems [Herzog11], cooperative vehicle ecosystems [Lima16], connected ambulances [ZDNET19], and 5G cellular access networks (Task 2.1).

DDoS attacks on these kinds of critical infrastructures carry the risk of **reducing Europe's digital sovereignty** (and that of digital societies elsewhere) because they disrupt societies. For example, the DDoS attacks on Estonia in 2007 took down all government websites, sites of political parties, as well as those of two major banks [Herzog11]. Similarly, the series of DDoS attacks in the Netherlands in 2018 caused service disruptions at three banks, the Dutch Tax Services, and at "DigiD" [NOS18], the identity systems for citizens to interact with government services. DDoS strikes may also affect the underlying Internet infrastructure, as illustrated by the attack on the DNS root in 2015 [Moura16], the IoT-powered DDoS attack on DNS operator Dyn in 2016 [Mirai17], and the DDoS attacks on several Dutch ISPs in September of 2020 [Tweakers20].

The problem: DDoS mitigation is crucial, but it is a soloistic activity today
Resilience to DDoS attacks is thus key for the digital sovereignty of societies such as Europe. The problem, however, is that organizations often focus on protecting the availability of their own services if a DDoS attack takes place (e.g., by redirecting the traffic through a scrubbing service), without trying to help other potential victims by

sharing the metadata of the attack with them, for instance in terms of its packet length, traffic distribution, and source IP addresses.

While this “soloistic” approach is logical from an individual organization’s business continuity perspective, it has two major drawbacks. First, it **reduces the capabilities of ecosystems (e.g., specific sectors) to quickly respond to a DDoS attack** because metadata about DDoS attacks is confined to the victim or the third-party DDoS mitigation providers they work with. As a result, potential victims will not be able to prepare for the attack and they will have to go through the same learning curve as the first victim. This unnecessarily increases the time it takes the second victim to mitigate the attack and might extend the service unavailability for their customers. It also increases pressure on their operations teams because they must handle attacks relatively unprepared while their services are starting to degrade, which increases the probability of human error and further extended outages. This process repeats itself for the next few victims, until operations teams can reactively share details about the attack through personal communications channels such as secure chat. At that point, however, the attacks can already have created significant disruptions, as we have seen in the Netherlands in January of 2018 [NOS18], for example.

The second drawback of a soloistic DDoS mitigation strategy is that it makes it **more difficult to learn from past attacks** and subsequently innovate anti-DDoS procedures and systems. The reason is that a post-mortem analysis of large DDoS attacks may require several datasets from several operators to fully understand what happened. For example, the analysis of the IoT-powered DDoS attack on DNS operator Dyn in 2016 involved 11 datasets (e.g., telnet honeypots, passive DNS traces, and DDoS traces) across 9 different organizations [Mirai17]. With organizations’ current soloistic mitigation strategy, it is difficult to get an overview of which organization has which datasets about the attack and then collaboratively analyze and learn from the data. This reduces the DDoS response and innovation capabilities of sectors and even entire societies, making them more susceptible to large service disruptions.

Our approach: anti-DDoS coalitions

The objective of our work is to address the above problems by **changing the model of handling DDoS attacks** from a soloistic activity to a collaborative one [DDoS18]. This enables critical service providers to (1) **increase their insight into DDoS attacks** from their own narrow view to an ecosystem-wide view, and (2) **increase their capabilities to handle DDoS attacks** because the new insights give them more grip on the requirements that they need to put on their DDoS mitigation facilities (their own or those of a contracted third party). As a result, a collaborative DDoS mitigation strategy **contributes to increased digital sovereignty**, not only at the level of sectors and society but at the level of individual organizations as well.

To change to a collaborative DDoS mitigation strategy, we introduce the notion of an **Anti-DDoS Coalition (ADC)**, which is a group of organizations that pledge to a common goal: to improve the resilience of the services that group members offer to their users by **fighting DDoS attacks on a cooperative basis**. The members of an ADC engage in **various activities** that increase their anti-DDoS capabilities and that help them attain their joint objective. These include large-scale DDoS drills to test members’ DDoS procedures and readiness, sharing DDoS expertise (“ISAC-style”), and the **sharing of metadata on**

specific DDoS attacks through a DDoS Clearing House (see below for details) [DDoSCH20].

The members of an ADC typically consist of public and private organizations that are potential DDoS victims (e.g., grid operators, financial institutions, and government agencies). For example, the Dutch ADC [DNADC] has a cross-sector membership (e.g., telecommunications, finance, and governments) and a national focus (the Netherlands). An alternative way to organize ADCs is based on a specific sector (e.g., financial services, e-health providers, or the energy sector), potentially across EU Member States. Another example of an ADC is an Information Sharing and Analysis Center (ISAC), but they typically focus on sharing expertise and do not share real-time DDoS metadata. ADCs can also have different governance models, ranging from membership organizations with a board and bylaws to lose and more informal collaborations like MANRS [MANRS].

In addition to potential victims, the membership of an ADC can also involve DDoS mitigation providers that are willing to share the metadata of the DDoS attacks they handle or that provide shared DDoS mitigation services for the members of the ADC [DDoSCH20]. An example is NBIP, a not-for-profit scrubbing provider from the Netherlands, which is a member of the Dutch national ADC.

Organizations may be part of multiple ADCs at the same time. For example, a pan-European bank could share their DDoS metadata with national cross-sector ADCs in the different Member States where they have offices as well as wit the pan-European banking ADC. These coalitions will typically have different objectives, such as protecting the Netherlands' critical infrastructure against DDoS attacks versus protecting European banks against DDoS attacks.

Our key technical enabler: the DDoS Clearing House

An important building block of an ADC is a **DDoS Clearing House**, a shared system that enables participating organizations to automatically exchange metadata about DDoS attacks (e.g., traffic patterns, source IP addresses, and packet lengths) in the form of so-called **"DDoS fingerprints"**. A Clearing House thus provides an **extra layer of security information** on top of the DDoS mitigation services that the members of an ADC need to have in place (e.g., scrubbing and blackholing services) and does not replace them.

The principle behind the Clearing House is that **to be forewarned is to be forearmed**. Sharing DDoS fingerprints with other members warns them that new attacks may be underway. Figure 12 illustrates this for an example ADC. Organization 1 gets hit by a DDoS attack, generates a fingerprint that describes the attack and shares it with the other members of the ADC. The operations teams of the other coalition members use the fingerprint to derive traffic filtering rules and install them in their network equipment in case the attack comes their way next. As a result, they will be able to mitigate the attack when it comes their way, for instance through the filtering rules dropping the DDoS traffic.

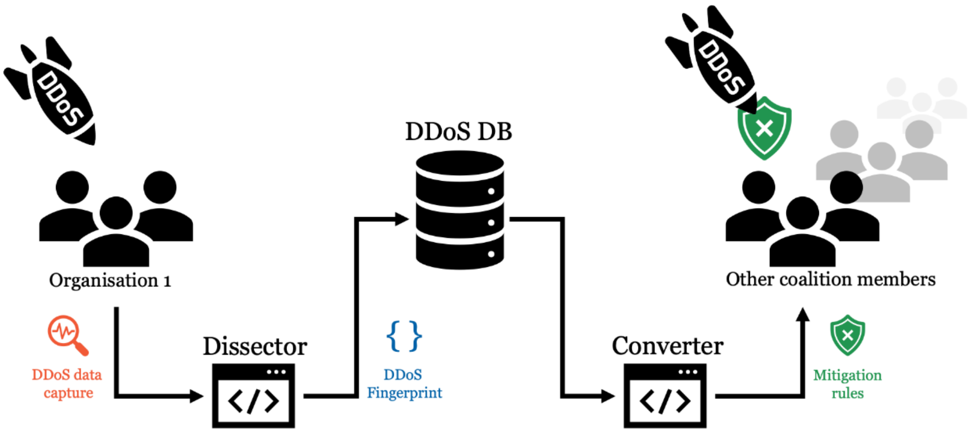
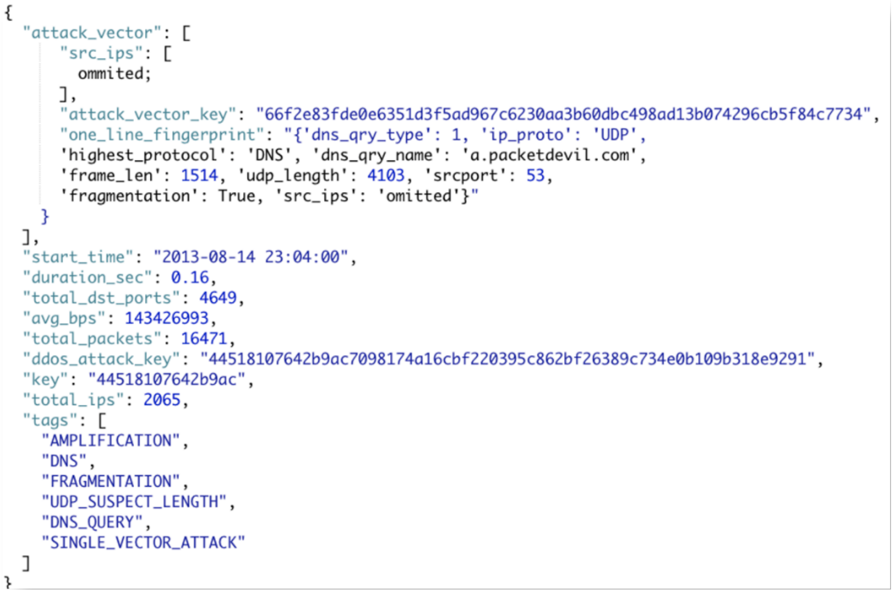


Figure 12: Example of an ADC and their DDoS Clearing House

The advantage of the Clearing House is that the fingerprints help its members to derive packet filtering rules more quickly for DDoS attacks that haven't hit them yet, which is work that usually takes place under intense pressure. For example, if the other coalition members in Figure 12 were to be the next target of the DDoS attack without having the fingerprint generated by Organization 1, then they would have to inspect the incoming DDoS traffic, write a packet filtering rule for the different types of equipment in their network, and push it into their network while, at the same time, the availability of their services might start degrading. Having Organization 1's fingerprint beforehand gives them more time to implement rules, which increases the probability that they will be able to effectively mitigate the attack.

Figure 13 shows an example of the DDoS fingerprint of an amplification attack using the Domain Name System (DNS). The fingerprint for instance lists the set of source IP addresses from which the NTP traffic originated (line "src_ips"), the number of source addresses (line "total_src_ips"), the protocol that was used (line "service"), and the duration (line "duration_sec").



```
{
  "attack_vector": [
      "src_ips": [
        ommited;
      ],
      "attack_vector_key": "66f2e83fde0e6351d3f5ad967c6230aa3b60dbc498ad13b074296cb5f84c7734",
      "one_line_fingerprint": "{'dns_qry_type': 1, 'ip_proto': 'UDP',
      'highest_protocol': 'DNS', 'dns_qry_name': 'a.packetdevil.com',
      'frame_len': 1514, 'udp_length': 4103, 'srcport': 53,
      'fragmentation': True, 'src_ips': 'omitted'}"
    }
  ],
  "start_time": "2013-08-14 23:04:00",
  "duration_sec": 0.16,
  "total_dst_ports": 4649,
  "avg_bps": 143426993,
  "total_packets": 16471,
  "ddos_attack_key": "44518107642b9ac7098174a16cbf220395c862bf26389c734e0b109b318e9291",
  "key": "44518107642b9ac",
  "total_ips": 2065,
  "tags": [
    "AMPLIFICATION",
    "DNS",
    "FRAGMENTATION",
    "UDP_SUSPECT_LENGTH",
    "DNS_QUERY",
    "SINGLE_VECTOR_ATTACK"
  ]
}
```

Figure 13: Example of a DDoS fingerprint

Clearing House architecture and key components

The architecture of the DDoS Clearing House consists of two types of components: **core components**, which enable operations teams to generate, store, distribute, and use fingerprints based on actual or simulated DDoS attack traffic; and **supplementary components**, which enrich and visualize fingerprints and make them available through the CONCORDIA Threat Intelligence Platform.

Figure 14 provides an overview of these components, which we will discuss in more detail in the next sections. The logos in Figure 14 indicate which T3.2 partners are responsible for which components.

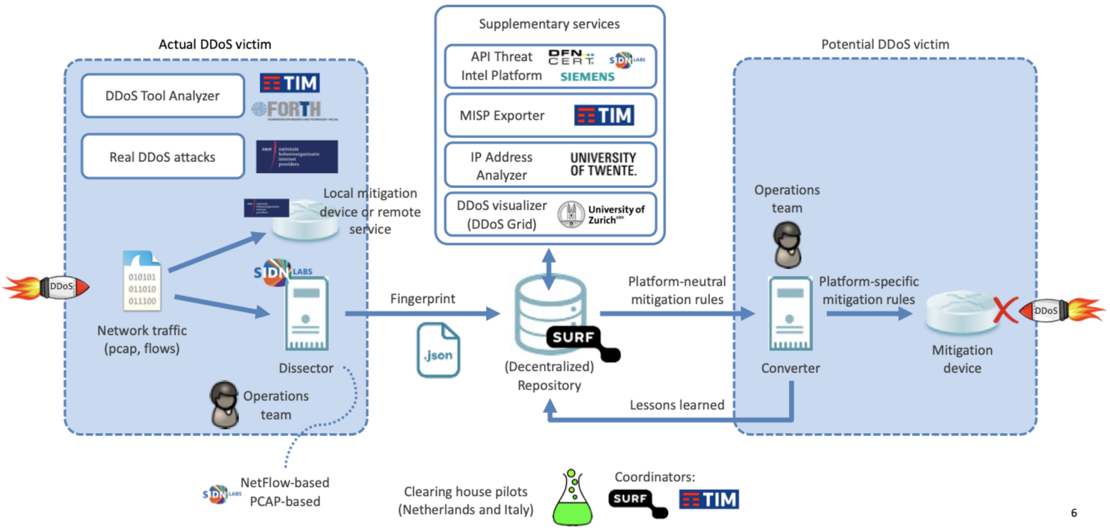


Figure 14: Clearing House components and data flow

The arrows in Figure 14 illustrate how a fingerprint typically flows through the system, from its creation at the member that gets hit by a DDoS attack (left) to its use by a potential victim (right). Each member of an ADC runs all the Clearing House's components, either in a "containerized" environment using Docker (our preferred method) or alternatively through the DDoS Clearing House-in-a-box VM. For simplicity, Figure 14 only shows one actual victim and one potential victim.

Table 2: Clearing house components (core, owner**)** provides an overview of the function of each of the Clearing House components (core components in *italics*), an indication of their maturity level, and the T3.2 experts working on them (owners underlined). SIDN and TIM organize the pilots in the Netherlands and in Italy, respectively.

Table 2: Clearing house components (*core*, owner)

Name	Function	Maturity	Partners
Dissector	Generate DDoS fingerprints based on PCAP files and flow data	High	SIDN
DDoS-DB	Insert, update, search, and retrieve DDoS fingerprints. Synchronize fingerprints between DDoS-DB instances.	High	SURF, SIDN
Converter	Generate mitigation rules based on DDoS fingerprints + export to MISP platform	Medium	TI, SIDN, SAG
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High	UZH
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack by querying multiple databases.	Medium	UT
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks. Integrated into the Clearing House testbed in Y3 (see Section 3.5).	Medium	FORTH
MISP Exporter	Export DDoS Fingerprints to the MISP platform. Integrated into the Converter in Y3 (Section 3.6).	Medium	TI, SAG
Distributed Testbed	Tests the cycle of the Clearing House in a representative, distributed setting (TRL6)	Medium	SIDN, SURF

We will discuss the testbed (last row of Table 2: Clearing house components (core, owner**)**) in Key achievement #2 and our progress for the individual Clearing House components (column Maturity) in Key achievement #3.

Progress beyond the state of the art

While the concept of collaborative DDoS defense has been around for a long time [DDOS13] [BloSS19] [Meng15] [Conrads19], **it has not yet been widely adopted**. Instead, service providers currently mitigate DDoS attacks single-handedly, focusing on protecting their own infrastructures (soloistic approach). Some do participate in group protection services such as NBIP-NaWas to share equipment and expertise, and to spread the cost.

The lack of deployment also means that potential DDoS victims have a limited insight into other mechanisms required to implement a cooperative anti-DDoS strategy. Examples include software that can easily be deployed in operational environments, software auditing, anti-DDoS drills, operational costs, and organizational and legal constructs. The DDoS Clearing House that we will pilot in CONCORDIA will advance the state of the art by developing and evaluating the mechanisms needed for these different perspectives *combined*, and not only from a technical perspective.

Relation to other CONCORDIA tasks

Task 3.2 is closely related to Task 3.1 (Building a Threat Intelligence for Europe) and we worked with them to develop a high-level design of the CONCORDIA Threat Intelligence Platform in Y2 of the project.

Other related tasks are T3.3 (Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Training), T4.2 (Legal aspects), T1.2 (Network-Centric Security), and T2.1 (Telecom Sector: Threat Intelligence for the Telco Sector).

3.5 Key achievements in Y3

In this section we describe the concrete innovations this task has made in the field, our four key achievements of Y3, and our dissemination results.

Key achievement #1: Refined innovations

In Y3, we refined and further concretized T3.2’s key innovations, which are:

1. We bridge the multidisciplinary gap from designing and developing the DDoS Clearing House to deploying it, which is more than technology (although individual components may be innovative as well and/or may result in new challenges)
2. We provide a multidisciplinary open-source design (technology, legal, organizational, experiences, lessons learned) that we share through the DDoS Clearing House cookbook so that other anti-DDoS coalitions can set up their own Clearing House and the organization around it and can further improve it, in Europe and beyond.
3. Our open-source design is based on our experience of running two pilots with the DDoS Clearing House, one in the Netherlands and one in Italy. By carrying out pilots in two different Member States we are also able to consider possible cultural differences (e.g., legal, organizational).
4. The DDoS Clearing House can operate across heterogeneous networks, which is important to accommodate different members of an Anti-DDoS Coalition. Some components, such as the Dissector, do not even require Internet access to process DDoS attacks. This means that processing can be done locally by each institution.
5. We provide a rich set of services with the Clearing House, such as the DDoS Grid and interfacing with MISP (upload fingerprints, download Snort rules).

The EC underscored these innovations by selecting the DDoS Clearing House for their Innovation Radar.

Key achievement #2: developed a DDoS Clearing House testbed

Our first key achievement for Y3 is the development and operation of a distributed testbed for the DDoS Clearing House [Hout21]. We developed it because we learned that **starting up a pilot in an established ADC such as in the Netherlands is a difficult job**. This is because it requires the ADC members to connect the Clearing House to their production networks and because setting up the required data sharing agreements is a time-consuming endeavor. The testbed enables us to test and demonstrate the DDoS Clearing House as it would be deployed in production, without having to wait for these slower processes to complete.

Our testbed creates a **realistic environment to test the DDoS Clearing House**. It consists of three components: a *virtual* anti-DDoS coalition (vCoalition) of two member organizations, the Clearing House components distributed across the vCoalition’s members, and a remote, cloud-hosted traffic generator. Figure 15 shows that we distributed all components across the Internet, instead of virtualizing them in a single network.

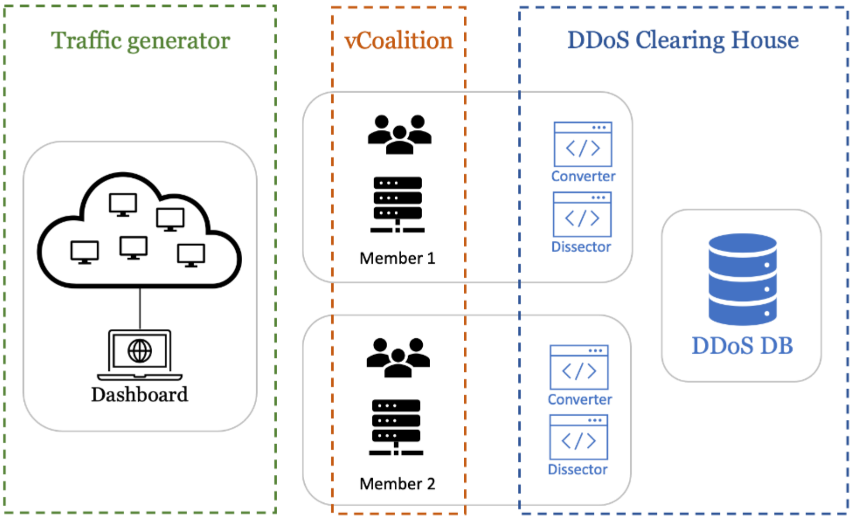
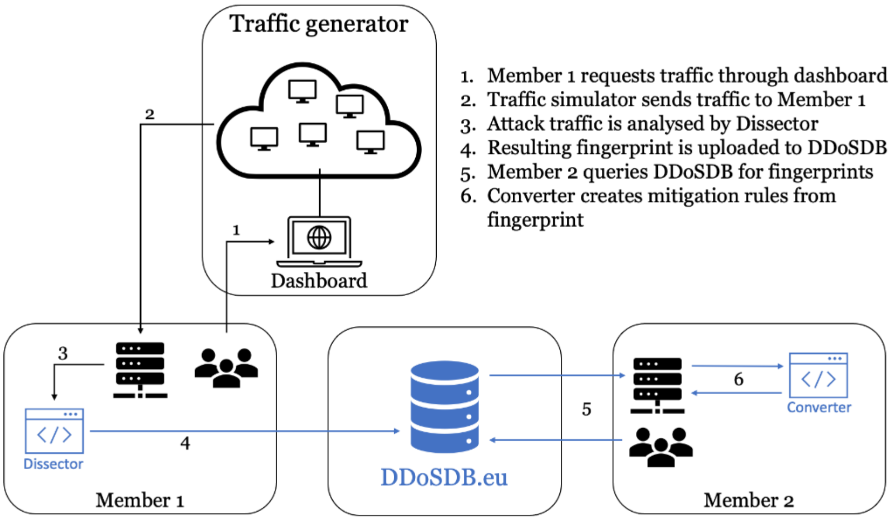


Figure 15: DDoS Clearing House testbed components

The vCoalition consists of two T3.2 partners that run their own dedicated research network, *outside* of critical production infrastructure. In our testbed, the vCoalition comprises SIDN and SURF, which both have such networks and can easily connect these networks to the Clearing House.

Figure 16 and Figure 17 show that the Traffic Generator transmits test traffic that emulates DDoS attacks. The generator consists of five attack servers, hosted throughout the world on a cloud hosting platform. The partners in the vCoalition can instruct the Traffic Generator to send them a particular type of DDoS attack sample through an online dashboard (interface). The Traffic Generator can only send test traffic to the requesting partner and is not of the same caliber as a real DDoS attack; it is meant only to test the cycle of the DDoS Clearing House with various types of DDoS attacks.



1. Member 1 requests traffic through dashboard
2. Traffic simulator sends traffic to Member 1
3. Attack traffic is analysed by Dissector
4. Resulting fingerprint is uploaded to DDoSDB
5. Member 2 queries DDoSDB for fingerprints
6. Converter creates mitigation rules from fingerprint

Figure 16: DDoS Clearing House testbed flowchart, part 1

The partners in the vCoalition know in advance that the IP addresses that the Traffic Generator uses are those of the five machines that transmit the test traffic, which means that these addresses do not constitute personally identifiable information (PII), which would normally be the case for DDoS attacks that take place "in the wild". Our legal experts confirmed that this enables us to freely share any generated DDoS fingerprints without data sharing agreements.

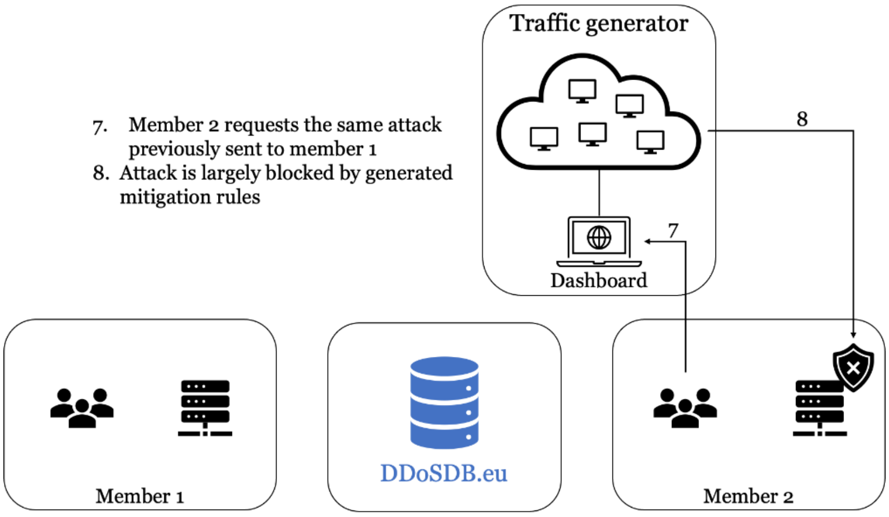

Traffic generator
7. Member 2 requests the same attack previously sent to member 1
8. Attack is largely blocked by generated mitigation rules
8
7
Dashboard
Member 1
DDoSDB.eu
Member 2

Figure 17: DDoS Clearing House testbed flowchart, part 2

Our testbed allows us to temporarily skip typically time-consuming processes such as setting up data sharing agreements and obtaining traffic traces from production systems, which helps to advance the system towards a pilot (TRL7) and eventually to a production version (TRL 8-9). The latter will be an activity for actual ADCs, such as the ADC in the Netherlands.

We elaborate on the implementation of our testbed in a blog [Hout21] and shot a video [DEMO21] to demonstrate how we used the testbed to test the Clearing House in a close-to-production environment.

The DDoS Clearing House testbed, as well as all Clearing House components are publicly accessible on our github page[1].

Key achievement #3: further improved Clearing House components

We have improved the Clearing House components in Y3 to a stable state, as indicated by the column Maturity in Table 2. In comparison to Table 2 in D3.2 (Y2), all Clearing House components now have a maturity level of medium or high. As a result, the technical system can be used in pilots in ADCs and in the distributed testbed.

Improved core components

The DDoS Clearing House's core components are responsible for generating, storing, and using fingerprints.

Dissector (SIDN). Generates fingerprints based on DDoS network traffic traces.
In Y3, we improved the Dissector by implementing algorithms to support multi-vector attacks [Ceron21]. These attacks combine different attack strategies to hit a target with more complex traffic. We generate a fingerprint for each attack vector and combine them

[1] https://github.com/ddos-clearing-house

into one fingerprint that can be shared through DDoS-DB. We also implemented strategies to fingerprint "DDoS Carpet Bombing" attacks, which target a range of IP addresses or subnets.

We further improved the usability of the Dissector by allowing multiple input files to build a single DDoS attack fingerprint. We advanced our flow-based dissector to extract more meta-data fields. We increased the stability of the dissector by rewriting the code and fixing (possible) bugs, as well as provided better error handling.

We made a containerized version of the Dissector using Docker. This enables organizations to quickly deploy the Dissector without needing to install all the required dependencies. Instead, they can simply use Docker to build an *image* of the Dissector, which includes all dependencies. This also increases the stability of the Dissector because it is executed inside the Docker container, making it indifferent to varying software versions and even varying operating systems in which the Dissector may be deployed.

Lastly, we examined the possibility of using machine learning algorithms in the Dissector, for example to infer the type of DDoS attack in a traffic capture file. We will continue this exploration in Y4 when we obtain more traces of DDoS traffic with which we can train machine learning models.

DDoS-DB (SURF, SIDN). Stores fingerprints, enables Dissectors, Converters, and supplementary services to manage DDoS fingerprints in DDoS-DB (e.g., insert, retrieve, update). DDoS-DB also allows operations teams to interactively search and edit fingerprints in DDoS-DB.

In Y3, we improved DDoS-DB by introducing the ability to get fingerprint information through an API. This API can be used by supplementary services to retrieve fingerprints and is also used for synchronizing fingerprints between multiple instances of DDoS-DB, for example a central instance shared by all members of an ADC and a local instance at a specific member organization. Operations teams use the web interface to indicate the fingerprints that can be shared between the DDoS-DB instances. We made it possible to automatically synchronize multiple instances of DDoS-DB with push and pull methods, ensuring automatic distribution across an ADC if several members use local instances of DDoS-DB; even when behind a firewall.

Similar to the Dissector, we created a *containerized* version of DDoS-DB, allowing for easy one-button deployment without the need to install dependencies and with the benefits of running in a standardized container environment. For production use, we added Let's Encrypt certificates with automatic update on top of the Docker deployment, simplifying operation even further.

We completely overhauled the look and feel of the DDoS-DB, making it more professional and intuitive to operations teams. The changes in Y3 resulted in a stable version of DDoS-DB which will only require limited additional work in the future.

(Multi-)Converter (TI, SIDN, SAG). Generates mitigation rules based on DDoS fingerprints.

In Y3, we improved the Converters that generate iptables rules and SNORT rules from a DDoS fingerprint. We use a simple version of the iptables Converter in the Clearing House testbed we developed this year (see Section 3.5). We also integrated the MISP Exporter module into the Converter, thus creating a “multi-converter”, which calls Converters to generate specific types of mitigation rules (e.g., iptables).

The Multi-Converter also uses the MISP exporter to insert fingerprint data in appropriate MISP objects/attributes. We (re-)evaluated all DDoS fingerprint fields and mapped them to new MISP attributes or objects. We introduced the use of the DDoS MISP object for the generation of mitigation rules, which can now contain multiple IP source addresses, multiple destination ports and multiple source ports. This permits a better (finer-grained) mapping of the fingerprint data to the snort rules generated from this object.

Moreover, we have proposed and implemented in the Multi-Converter an extended mapping of the fingerprint data to MISP attributes, or directly to snort rules (stored as snort network attributes in MISP), particularly in those cases where the exact attribute needed was not found in MISP. This permits us to create tailored snort rules from fingerprint data which were not previously taken into consideration, such as DNS query name, HTTP request, ICMP code and type, etc. This module is ready for implementation in the DDoS Clearing House, but testing is still ongoing.

Improved supplementary services

The Clearing House’s supplementary services aim to enrich fingerprints and make the system intuitive to use for operations teams. Together, they further enhance the added value of the core components.

DDoS Tool Analyzer (FORTH). The DDoS Tool Analyzer creates fingerprints of the DDoS traffic generated by tools frequently used by attackers to carry out DDoS attacks. These tools include hping3 [HPING], nmap [NMAP] (mostly used for scanning purposes though), ddos simulator [DDOSIM], and others.

In Y3, we integrated this component into the Traffic Generator of the testbed (see Section 3.5). The testbed uses hping3 to customize and send Internet packets to a target in the *virtual* anti-DDoS coalition. We apply the different DDoS simulation tools from this component in the further development of the testbed. Because we use the DDoS tools on the testbed, we can now create fingerprints of the traffic generated by the testbed instead of using the tools separately.

Before its integration in the testbed infrastructure, we also experimented with other DDoS tools, including [HULK], Pyloris, RUDY, and DAVOCET (this is work in progress and we will check if and how they can fit in the testbed).

We employed Elasticsearch in combination with a packet analysis extension called Packetbeat [PACKETBEAT], to visualize incoming traffic on a target machine. This is also used in the testbed to visualize the traffic sent from the traffic generator module.

DDoS Grid (UZH). The DDoS Grid provides a dashboard for the visualization of DDoS fingerprints based on PCAP files or DDoS fingerprints.

In Y3 we researched how to automatically classify and visualize DDoS traffic. We integrated a machine learning module into the DDOS Grid, using Random Forest and K-Nearest Neighbor algorithms, which automate different steps of a post-mortem DDoS analysis becoming critical when analyzing large datasets as those involving 5G and IoT scenarios. An experimental evaluation of the model was conducted based on a dataset from DARPA[1] including two Neptune (TCP-SYN Flood) and one Smurf (ICMP Flood) attack, which were correctly classified in the post-mortem analysis (cf. Figure 18).

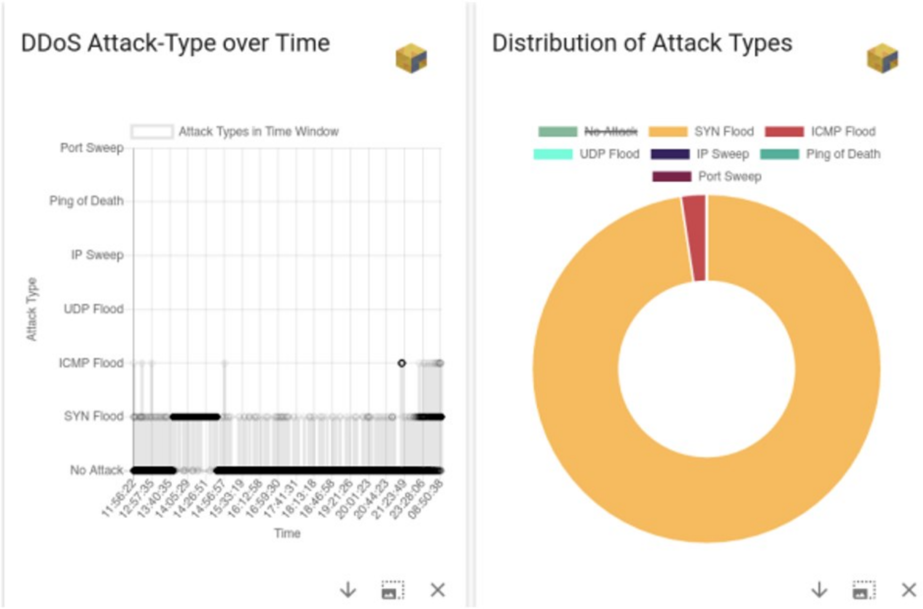


Figure 18: Visualizations, representing the DARPA PCAP file, showing an over-time analysis and the total distribution of attack types

Further, we implemented a new tab in the DDoS Grid to visualize the economic impact of an attack. The added tab allows different stakeholders to (optionally) share economic information and gain insights from analysis of the cyberattack information and economic impacts of attack. Models in the economic tab include the Return on Security Investment (ROSI) and quantitative risk metrics such as Net Present Value (NPV).

We recorded short demo videos of these improvements, which can be found online: Economic Tab[2], ML Classifier[3]. The overall maturity status of the DDoS Grid is high.

IP Address Analyzer (UT). Uses active measurement and IP intelligence datasets provided by third parties to analyze the source IP addresses in a fingerprint and adds these details to the fingerprint. Examples are the network capacity of attacking machines and the networks where they reside. The metadata that the Address Analyzer provides gives network operators and researchers a better understanding of the similarities and differences between various attacks and attacking hosts.

[1] https://archive.ll.mit.edu/ideval/data/2000/LLS_DDOS_2.0.2.html
[2] https://youtu.be/AJErwUZGhYQ
[3] https://youtu.be/WFFGp916qQg

In Y3, we improved the performance of the IP Address Analyzer to allow the analysis on a large set of IP addresses, which is common for DDoS traffic. The component is running in a stable version and ready to be used in combination with other components of the DDoS Clearing House.

We also added a world map plot to show the geolocation of public IP addresses in a DDoS fingerprint, to get a visual insight of where the DDoS traffic is coming from. Lastly, we added MeasurementLab lookup support (network speed measurements) to further extend the functionality of the IP analyzer component

Key achievement #4: completed technical preparations for the pilots

In Y3, we matured the DDoS Clearing House software to a stable state, which means that it is ready to be piloted in an ADC, in particular in the Netherlands or Italy.

Virtual pilot (SIDN, SURF). With our new distributed testbed for the DDoS Clearing House (see Section 3.5), we effectively piloted the Clearing House with simulated DDoS traffic. This indicates the Clearing House can go full cycle (from attack to mitigation) and that it is ready for a pilot (and perhaps even a production) environment. The blog and demo video on the testbed also highlight the added value of the Clearing House, which might motivate partners in the Netherlands, Italy and elsewhere to connect to the system for a pilot.

The Netherlands (SIDN, SURF, UT). SURF, SIDN, and the UT continued their active contribution to the Dutch ADC, which currently consists of 16 critical service providers across the sectors of the Netherlands (e.g., banks, telcos, and governments).

In Y3, SIDN wrote a document for members of the Dutch ADC on the technical requirements for production networks to fingerprint DDoS attacks using the Dissector and to upload these fingerprints to DDoS-DB (see Appendix section 9).

Also, SIDN, SURF, and the UT actively participated in the Clearing House Working Group (WG) of the Dutch ADC. One of SIDN's legal experts joined the Dutch ADC's Legal WG and contributed to their legal framework (e.g., the consortium agreement) and the Code of Engagement being developed in T4.2. SIDN also contributed to the Dutch AD''s Communications WG and the new WG "Architecture and Society".

The Dutch ADC made the following overall progress:

- They finalized and approved a consortium agreement, which will be signed by the members of the Dutch ADC. The consortium agreement also acts as "bottom up" input for Task 4.2 of CONCORDIA.
- They filed an additional funding request with the Dutch government for starting up production. The requested funds will be used to hire a Product Manager for the DDoS Clearing House and to pay for the costs of bringing the DDoS Clearing House software to production level (TRL8-9) and to pay for the hosting of DDoS-DB.
- A new coalition member joined the ADC: the Digital Trust Center; an organization founded by the Dutch Ministry of Economic Affairs that provides (cybersecurity) information and support to Dutch companies. Two members left the coalition for financial reasons, but there is another interested party on the horizon.

Currently, we are working on setting up the pilot with three members of the Dutch ADC: NBIP, one of the partners that provides DDoS scrubbing services, University of Twente, and KPN, a major ISP in the Netherlands. We are optimistic that the containerization of the Clearing House components and the testbed will make it easier to carry out the pilot, but at the same time operations teams need to have the time and leeway to actually connect their production networks to the Clearing House. The testbed demonstrator may speed up this process by helping senior management of members to appreciate the added value of the Clearing House.

Italy (TI). In Y3, we have made progress in the pilot that will be run in Italy. We have established an ADC with three partners: TIM's Security LAB, TIM's internal Security Operation Center (SOC), and the University of Turin. TIM's departments are dedicated to the protection of the Telecom Italia corporate infrastructure.

The pilot in Italy was delayed previously because of COVID-19 and non-core activities at TIM being put on hold. Currently, there is an informal agreement to run a pilot with the Clearing House starting from lab environments, mainly because legal and organizational action points have been not yet fully addressed.

At the present time each of the three partners has its own network infrastructures, security tools and its own set of the CONCORDIA anti-DDoS tools already up and running. Regular calls have been scheduled to discuss the status, results, and next steps.

The pilot in Italy will focus on creating DDoS fingerprints and sharing these via MISP by using a dedicated MISP instance potentially interconnected to the CONCORDIA H2020 MISP.

Dissemination results

Month	Event
Dec	T. van den Hout, "Demonstrating the DDoS Clearing House distributed testbed", La Fabrique Défense conference
Oct	T. van den Hout, "Demonstrating the DDoS Clearing House distributed testbed", CONCORDIA Open Door 2021
Oct	T. van den Hout, R. Poortinga-van Wijnen, "Demonstrating the DDoS Clearing House", demonstration video: https://youtu.be/UwRB74kabn8
Oct	C. Hesselman, T. van den Hout, "DDoS Clearing House for Europe (Task 3.2) – Status Update GA7", 7th CONCORDIA General Assembly
Sep	M. Tsantekidis, C. Papachristos, participation at the CyberHOT Summer School, Chania 2021
Sep	C. Hesselman, "Developing and Evaluating a DDoS Clearing House for Europe", Euritas Summit
Jul	C. Hesselman, "DDoS Clearing House for Europe", NBIP@20
Jul	T. van den Hout, "DDoS Clearing House Operational simulation", SIDN Labs presentation session
Jun	C. Hesselman, "DDoS Clearing House for Europe", ICANN71 vTechDay
May	C. Hesselman, "DDoS Clearing House for Europe", Online meetup @ ABNAMRO Bank
Mar	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2)", 6th CONCORDIA General Assembly

Feb	C. Hesselman, J. Ceron, "DDoS Clearing House Update", Plenary meeting of the Dutch anti-DDoS Coalition
Feb	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2)", 3rd CONCORDIA review
Jan	R. Ruiter, C. Hesselman, "No More DDoS – Anti-DDoS Coalition", Inter-ISAC meeting NL
Jan	C. Hesselman, "SIDN Labs activities" (including a discussion on the DDoS Clearing House) - NGI talks (Next Generation Internet)

and

Table **4** show our dissemination results for Y3 in the form of presentations (including a demo video) and blogs, respectively.

Table 3**:** Task 3.2 presentations in Y3 (2021)

Month	Event
Dec	T. van den Hout, "Demonstrating the DDoS Clearing House distributed testbed", La Fabrique Défense conference
Oct	T. van den Hout, "Demonstrating the DDoS Clearing House distributed testbed", CONCORDIA Open Door 2021
Oct	T. van den Hout, R. Poortinga-van Wijnen, "Demonstrating the DDoS Clearing House", demonstration video: https://youtu.be/UwRB74kabn8
Oct	C. Hesselman, T. van den Hout, "DDoS Clearing House for Europe (Task 3.2) – Status Update GA7", 7th CONCORDIA General Assembly
Sep	M. Tsantekidis, C. Papachristos, participation at the CyberHOT Summer School, Chania 2021
Sep	C. Hesselman, "Developing and Evaluating a DDoS Clearing House for Europe", Euritas Summit
Jul	C. Hesselman, "DDoS Clearing House for Europe", NBIP@20
Jul	T. van den Hout, "DDoS Clearing House Operational simulation", SIDN Labs presentation session
Jun	C. Hesselman, "DDoS Clearing House for Europe", ICANN71 vTechDay
May	C. Hesselman, "DDoS Clearing House for Europe", Online meetup @ ABNAMRO Bank
Mar	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2)", 6th CONCORDIA General Assembly
Feb	C. Hesselman, J. Ceron, "DDoS Clearing House Update", Plenary meeting of the Dutch anti-DDoS Coalition
Feb	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2)", 3rd CONCORDIA review
Jan	R. Ruiter, C. Hesselman, "No More DDoS – Anti-DDoS Coalition", Inter-ISAC meeting NL
Jan	C. Hesselman, "SIDN Labs activities" (including a discussion on the DDoS Clearing House) - NGI talks (Next Generation Internet)

Table 4: Task 3.2 blogs in Y3 (2021)

Month	Event
Oct	T. van den Hout, R. Poortinga-van Wijnen, C. Hesselman, C. Papachristos, K. Vink, "Developing and running a testbed for the DDoS Clearing House", https://www.concordia-h2020.eu/blog-post/developing-and-running-a-testbed-for-the-ddos-clearing-house/ (reposted on the CONCORDIA site and the site of the Dutch ADC)
Apr	J. Ceron, P. van Stam, G. Schaapman, C. Hesselman, "New DDoS classifiers for the DDoS Clearing House", https://www.concordia-h2020.eu/blog-post/new-ddos-classifiers-for-the-ddos-clearing-house/ (reposted on the CONCORDIA site and the site of the Dutch ADC)

Key lessons learned

We identified three key lessons learned based on our work in Y3.

Our first lesson learned is that piloting a new collaborative system such as the DDoS Clearing House is a process with a **long lead time**. The main causes are that ADC members are understandably careful to make changes in their production systems to connect to the Clearing House and that the legal and organizational aspects can take a long time as well, as we already learned last year.

We have also learned to **take "baby steps"** in setting up the pilots. In particular, we learned that our testbed is a valuable intermediate step towards a real pilot: it enabled us to fully test the system we built in a realistic environment (TRL6) and to demonstrate how it works, which might further motivate the partners in the Dutch ADC to join the pilot (TRL7). We were able to develop the testbed because we designed it so that we could temporarily skip the establishment of data sharing agreements and did not need to change production networks**.**

Finally, we learned that the simulated production environment that the testbed provides is **very useful to quickly test new additions** in a realistic setting, which aligns with T3.2's iterative development strategy. It for instance allowed us to quickly identify problems in the technical systems and quickly abandon ideas that likely would not work in a production setting. This will also be valuable to further increase the maturity of the DDoS Clearing House to TRL8-9 post-CONCORDIA.

3.6 Outlook Y4

In Y4, the final year of CONCORDIA, T3.2 will tackle four challenges: (1) running a pilot in the Netherlands with the DDoS Clearing House for the Dutch anti-DDoS coalition, (2) running a pilot for the three-party ADC in Italy, (3) further maturing the Dissector and the Converter, and (4) publishing the cookbook. We will also continue our collaboration with other tasks in CONCORDIA, specifically T3.1 on the Threat Intelligence Platform, and T4.2 on the legal constructs.

Pilot in the Netherlands. To carry out the pilot in the Netherlands, the members of the Dutch ADC will need to connect their networks to the Clearing House. While this is a challenge from an operational perspective, we are optimistic that we'll be able to pilot the DDoS Clearing House in Y4. This is because (1) operations teams need to put minimal effort in connecting to the Clearing House because we containerized its components in Y3 and (2) because we were able to fully test the system in a realistic environment in Y3 through our distributed testbed (TRL6). In addition, the product manager that the Dutch ADC is attempting to fund will be a motivational factor for partners to invest organizational effort in running a pilot. However, operations teams do need to have the time and leeway to connect their production networks to the Clearing House.

Pilot in Italy. In 2022, the ADC in Italy (two departments in the Telecom Italia Group and the University of Turin) will start to share DDoS fingerprints of real attacks targeted at the partners' infrastructures, primarily through MISP. The partners' legal departments will be involved in the pilot to discuss privacy regulations of using real DDoS traffic and the subsequent sharing with other partners. The Dutch pilot agreements and documentation will form the basis of the agreements in Italy. The Dissector and Converter modules of the Clearing House will be used to analyze past real DDoS attacks target at TI or academic infrastructures in Italy. Lastly, we will investigate the possible extension of the Italian ADC for this pilot.

Further maturing the Clearing House's Dissector and Converter. In Y4, we will be focusing strongly on improving the Dissector and Converter modules. We will update the Dissector to analyze and fingerprint new types of DDoS attacks, make the Dissector more robust, and make it more broadly applicable to additional types of traffic capture files, such as Parquet. We will also advance the generation of mitigation rule generation by Converters, using both the fingerprints from DDoS-DB, as well as the new MISP objects.

We will also further improve the distributed testbed, for instance so that we can test the Clearing House "full circle" with more intricate types of DDoS attacks. We also plan to connect additional T3.2 partners to the testbed, potentially with a lightweight waiver agreement.

Publishing the cookbook. Our final objective in Y4 will be to aggregate our previous documents and lessons learned into the DDoS Clearing House cookbook. It will help organizations in Europe and elsewhere to set up their own Anti-DDoS Coalitions, or join existing ones, making use of the DDoS Clearing House software. We aim to publish the report in the form of a paper, for instance in Springer's Journal of Internet Services and Applications (JSAC).

Continue inter-task collaboration. As before, we will continue working with other CONCORDIA tasks, specifically with:

- T3.1 (Building a Threat Intelligence for Europe): to refine the CONCORDIA Treat Intelligence Platform and its interaction with the DDoS Clearing House.
- T3.3 (Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Training): to integrate our distributed testbed as Cyber range in CONCORDIA.
- T4.2 (Legal aspects): to develop a "code of engagement" document for organizations to join the DDoS Clearing House as it continues to evolve.

References are in Chapter 7

4. Developing CONCORDIA's ecosystem (T3.3)

4.1 Task objective

The objective of T3.3 is to establish the CONCORDIA cybersecurity ecosystem with virtual labs, services and training activities. *Virtual Lab* activity aims to develop an ecosystem that would support validations and demonstrations of CONCORDIA's results on large IT infrastructures and in smaller cybersecurity labs. *Services* activity aims to create a curated portfolio of public and proprietary tools and available cybersecurity labs to create a cutting-edge advantage for the partners to speed up research and development of cybersecurity systems. *Training* activity aims to develop and continuously evolve cyber range trainings to achieve better automated and custom-tailored trainings that correspond to the evolving cyber threat landscape.

4.2 Preamble

The focus in year 2 was on Cyber Training (inventory of Cyber Ranges, virtual labs and Trainings) and is available online[1]

MUNI provided an open-source cyber range platform, so all consortium partners can use it to develop and run content for cybersecurity education. MUNI also delivered a network topology description format and the first prototype of an open format for sharing the content (details can be found in Deliverable D3.2).

The first steps of scenario exchange in Cyber Ranges were done as well as the cooperation with other H2020 projects.

We summarize again labs and cyber ranges in section 4.3 below as these are ongoing activities.

4.3 Status

Task 3.3 is on track towards its goal. This year the Training site was updated and increased with special selection criteria and organizer information.

The work in Y3 is built on the results of Y1 and Y2 described in Delivery D3.2.. We focused on collecting virtual labs, the open-source KYPO Cyber Range platform and new Services and Tools.

In the dissemination sector, we implemented a **Blog Post Sep 2021: CONCORDIA's Cybersecurity Ecosystem: Virtual Lab, Services and Training - Cyber Range Open Format Exchange**[2] and published **The Current State of The Art and Future of European Cyber Range Ecosystem**[3]**:** created by the Cyber Range Focus Group CONCORDIA, ECHO and SPARTA

[1] https://www.concordia-h2020.eu/map-courses-cyber-professionals

[2] https://www.concordia-h2020.eu/blog-post/concordias-cyber-security-ecosystem-virtual-lab-services-and-training/

[3] https://ieeexplore.ieee.org/document/9527931

4.4 Key achievements Y3

This chapter is structured as in the project Description of Work (DoW): Virtual Labs, Services and Training.

4.4.1 Virtual Lab

As CONCORDIA takes a holistic and scalable approach to cybersecurity, our vision is to provide a common portal via the CONCORDIA website as entry point for Cyber Range platforms, (virtual) labs, and services. All these services are bringing added value to CONCORDIA stakeholders.

The CONCORDIA ecosystem concept on virtual labs goes along with three main guidelines:

I. A virtual platform: the CONCORDIA Platform will consist of a collection of solutions running on heterogeneous technologies and providing different services.
II. Compatible models and structures: services provided by the platform will take advantage of each other, mutually exchanging information and jointly supporting possible new features.
III. Uniform engagements rules: data access and usage policies will be aligned and integrated as much as possible so to guarantee straightforward and trustworthy executions of services.

We updated the list of labs including guidelines, terms of usage, and further information in year 3. This activity is ongoing to improve the offer.
In addition, a new "Flying Lab" was integrated and activities on remote access of several (virtual) labs have been finalized.

Our final goal is to have a common portal via the CONCORDIA website including the common Threat Intelligence platform and the DDoS Clearing House.

One of the goals of the Virtual Lab is to grant access to cybersecurity labs to partners and possibly also to certification bodies. This goal is very tightly connected to the Services and Training activities where several potential labs and solutions were mapped.

In addition, we created a dynamic list which includes available Labs and Cyber Ranges (CONCORDIA-public/private/commercial, pilots, other). Detailed information is given for interfaces, policies, and conditions. Furthermore, the willingness to cooperate and share trainings` data and content for scenario exchange is essential for the continued success of CONCORDIA.

The listed (virtual) labs are in scope of cyber-security experimentation and research, machine learning, big data, secure data hosting, special malware detection or 5G cellular IoT security features. As an example for virtual labs in operation, the **High-Security Laboratory (HSL**) is designed to host decisive research activities in order to make networks, internet exchanges and associated telecommunications equipment safer. It allows to collect and store data while ensuring their confidentiality and integrity, both logically and physically, while offering a safe environment for researchers to work. The technology behind: Around 95 servers, organized in per-project clusters and isolated zones. Usage is free for nonprofit usage (NDA and/or acknowledgement required).

Another example is represented by a prototype 5G cellular IoT Lab. The access to services can be granted to collaborating organizations upon agreement. This lab is an initiative from Telenor & OsloMet, which focuses on accelerating the development of a secure 5G mobile network capable of accommodating the next wave of communication, namely the communication between billion of Internet of Things (IoT) devices. Improvements are ongoing.

The **Dynamic Malware Lab** is planning for shared data and services as follows:
In accordance with the lab's objectives, both data and services are made available to partners. Some of the offerings will be made completely freely accessible, while others (especially services) will only be made available to a limited group of users due to resource limitations and the potential for misuse. The Virtual Dynamic Malware Lab was put into operation in its basic configuration in 2021 and a test run with external participants (as part of teaching) was carried out in the summer of 2021. Another test run with remote collaborating partners, which also involves the expansion of the offered features and sample configurations, is currently underway. Here, Bachelor students implement a research botnet based on known botnets and can study its propagation and containment as well as take-down in different network topologies from different angles in the Dynamic Malware Lab. Until the beginning of 2022, some internal adjustments to the backend are still planned. These adjustments address the automated generation of emulated network environments as well as the integration of further hypervisor solutions in order to support a broader spectrum of system architectures, particularly in the area of IoT networks and embedded devices. Furthermore, web-based control and monitoring of experiments for users as well as user administration are to be improved in 2022. The goal is to make the Lab infrastructure access for the cooperation partners easier and quicker as well as reducing the administrative overhead for setting up access and instructing users.
Furthermore, the publication of reference data (which are generated in the Lab) is planned for the coming year. Here PCAP and Netflow recordings of the executed malware from all relevant links of the emulated network topology as well as the corresponding playbook descriptions and executables will be archived and made available. This data should be freely accessible (where possible and appropriate). However, especially the publication of the playbooks and configuration files for reproduction or extension of the experiments bears the risk to give unintentionally misusable information (like access data) to unauthorized users of the infrastructure. Therefore, access to these data is only granted upon request within the infrastructure.

The **Open Source Analytics Lab (OSA)** at RI CODE is used to crawl, process and analyze freely available data from various sources on the Internet. Furthermore, the OSA Lab will explore and investigate new approaches to the interaction with databases and datasets. For this purpose, the OSA Lab is equipped with appropriate hardware. A media system with projector and 6 large-format screens allows the presentation of processed data, for example in the form of dashboards, statistics and reports. Three workstations are available for search, analysis and processing.
Additional hardware, such as XR devices allow the implementation of elements of multimodal interaction. The focus of research in 2021 was in the area of speech recognition and processing. Among other things, a testbed was built to compare different speech recognition systems. The testbed consists of a server running different open source SREs, which are accessible via an API from different clients. Currently the open-source solutions Mozilla DeepSpeech and Alpha Cephei Vosk are installed and can be used for experiments. Furthermore, the API supports requests to commercial systems, for example Microsoft

Windows Speech Recognition. The recognition results of different systems can be compared with each other.

As part of a bachelor thesis, a study was conducted to investigate the suitability of systems for various tasks in the field of speech processing. For this purpose, a benchmark was developed which currently contains four different experiments representing increasing complexity of utterances. The goal of the study was to find out which systems are suitable for multimodal interaction with sophisticated data processing frameworks.

To find out the most appropriate system for a specific task, we will conduct further experiments that consider not only robustness of detection, but also resource efficiency and latency. In the next step, the most promising systems will be installed within a productive environment and made available to the community in the medium term. From this, we hope to obtain additional data to improve the underlying models and increase the robustness of the detection.

Another area of research in 2021 was gaze-tracking based human computer interaction (HCI). Here, further insights were gained into how gaze-tracking can be used to design context-aware interfaces for data analysis. In the medium term, we plan to explore different approaches for a context-aware interface that combines the input modalities of speech and gaze. A prototype that allows interaction with structured georeferenced datasets displayed on a 3D map already exists. Since multimodal interaction requires specific hardware, this prototype cannot be made available remotely to the community at this time.

The **5G & IoT Lab** is a joint initiative of the research center CODE, the Technical University of Munich (TUM) and the Central Office for Information Technology in the Security Sector (ZITiS) to research the security and performance of the mobile communications standard 5G. The aim is to investigate cybersecurity in mMTC scenarios in the field of 5G. Among other applications, this laboratory environment can be used to investigate the detection of anomalies in the 5G core infrastructure or to investigate network slicing, and with this the application of Software Defined Networking (SDN) in 5G core networks.

The focus of CODE is on the 5G application scenario "Massive Machine Type Communication" (mMTC). The infrastructure of the 5G part is based on the open-source software OpenAirInterface (OAI) and is dislocated at the three partners (FI CODE, TUM and ZITiS). The "Internet of Things (IoT)" area of the central laboratory was designed as an extension to explore the mMTC scenario. This maps various hardware interfaces and protocols using market-available "low-cost" IoT systems, which include the following: 3G, 4G, 5G; Bluetooth, Bluetooth Low Energy (BLE); DigiMesh; IEEE 802.15.4; LoRa, LoRaWAN; NFC; SigFox; WiFi; ZigBee.

In conjunction with the 5G interface of the OAI interface, an mMTC scenario can thus be generated in combination with the two laboratory components.

The "5G & IoT Lab" is based on market-available "low-cost" systems and open-source software. The core of the 5G part is the OpenAirInterface software, which maps both the core network and the base stations. Currently, the core network is located within the TUM laboratory and the "evolved Node Basestations" (eNodeBs, eNBs) of CODE and ZITiS communicate "tunneled" with the core network via the S1-C/U and NG-C/U interfaces, respectively. The tunnel is provided by Open VPN servers. The core network enables the communication between the various user equipment’s (UEs) which are connected to the various "next generation node bases" (gNBs) or eNBs.

In the next step this lab infrastructure will be connected to the CODE cyber range to enable the training of attack and defence scenarios for the protection of 5G networks and IoT devices.

Motivation to share data and infrastructure in and beyond consortium is ongoing. Currently, the list of these labs is internally published and planned for the public at a later stage.

4.4.2 Services

The map of courses and training

To provide a portfolio of tools and services to CONCORDIA and the wider community, a map with an overview of courses and trainings or professionals has been published and maintained[1]. Any information of value is thus in one place and can easily be found.

CTF Best Practice Guide

We started with a best practice guide for CTFs last year We recommend activities for participants as well as for the organizers of CTF events. This work describes an ongoing activity to improve the process.

We published a list of tools after internal quality review. In our Cybersecurity Tools list[2] we recommend nearly 50 tools, including type and terms of use. In the future, special selected tools can be added to CONCORDIA's virtual labs.

Special Tools Development

The discovery of evasion vulnerabilities over the Suricata intrusion detection system was done in collaboration with the CatenaCyber company[3]. We have provided access to the cyber-range platform to this SME for the experiments, and a talk regarding these vulnerabilities was recently given by students at the OSIF SURICON conference in October 2021.

4.4.3 Training

Cyber range platforms, CR-based trainings, and related tools are the main focus of the training activity. Discussions on technical topics such as exchange of scenarios, traffic composition, automatic execution of attack scenarios and network simulation/emulation are ongoing to optimize project results.

Currently, five operational Cyber Ranges from the Commercial and Academic sectors are available in CONCORDIA for public information and experience sharing (Figure 19).

[1] https://www.concordia-h2020.eu/map-courses-cyber-professionals/

[2] https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/

[3] https://catenacyber.fr

Cyber Ranges

Cyber Ranges provide a multipurpose virtual environment in which organisations can test critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their strategic information, services, and assets.

Check our solutions!

Figure 19: Cyber Ranges for public use in Concordia

As T3.3 has focused on researching the possibility of interchanging testing and training content - rather than creating a tight integration (federation) of cyber ranges - (with e.g. base virtual images, network topologies, SW configurations, and scenario descriptions) between cyber range platforms in year 3, the result of sharing content is shown as below.

We are working with 4 Cyber Ranges on the Exchange of Scenarios: Masaryk University (MUNI-KYPO), Uni BW (CODE-ICE&T), University Lorraine (UL- HNS) and University Milan UMIL (Cyber Range from Threat Arrest Project)
Having different concepts and technologies, we are providing below a rough overview of these cyber ranges:

MUNI (KYPO)

KYPO CRP won Innovation Radar prize.[1]
The virtual environment for hands-on cybersecurity education from Masaryk University, KYPO Cyber Range Platform, won the 7th edition of the European Commission's Innovation Radar competition. The expert jury announced it as the winner of the Disruptive Technologies category on 21 October. The category is intended for high-tech innovations that have the potential to significantly impact their area.

The KYPO scenario is divided into two independent parts. This approach provides a better separation of technical and educational parts. It also supports the creation of "building blocks" and their exchange among scenarios.
The first part is Sandbox Definition and Sandbox Provisioning (see Figure 20 and Figure 21 below), describing technical infrastructure (sandbox), networking, virtual machines, and the content of the machines. We follow infrastructure as a code approach in all parts.

1. **Topology Definition**: The file with the sandbox structure definition (hosts, routers, networks, etc.). It uses our simple open format (YAML), which is possible to convert to a HEAT Template.
2. **Sandbox Provisioning**: It is used to customize Topology Instances, e.g., set up an environment, create users, install packages, etc. Sandbox Provisioning must specify

[1] https://www.concordia-h2020.eu/news/press-release-kypo-cyber-range-platform-is-the-european-commissions-innovation-radar-prize-winner/

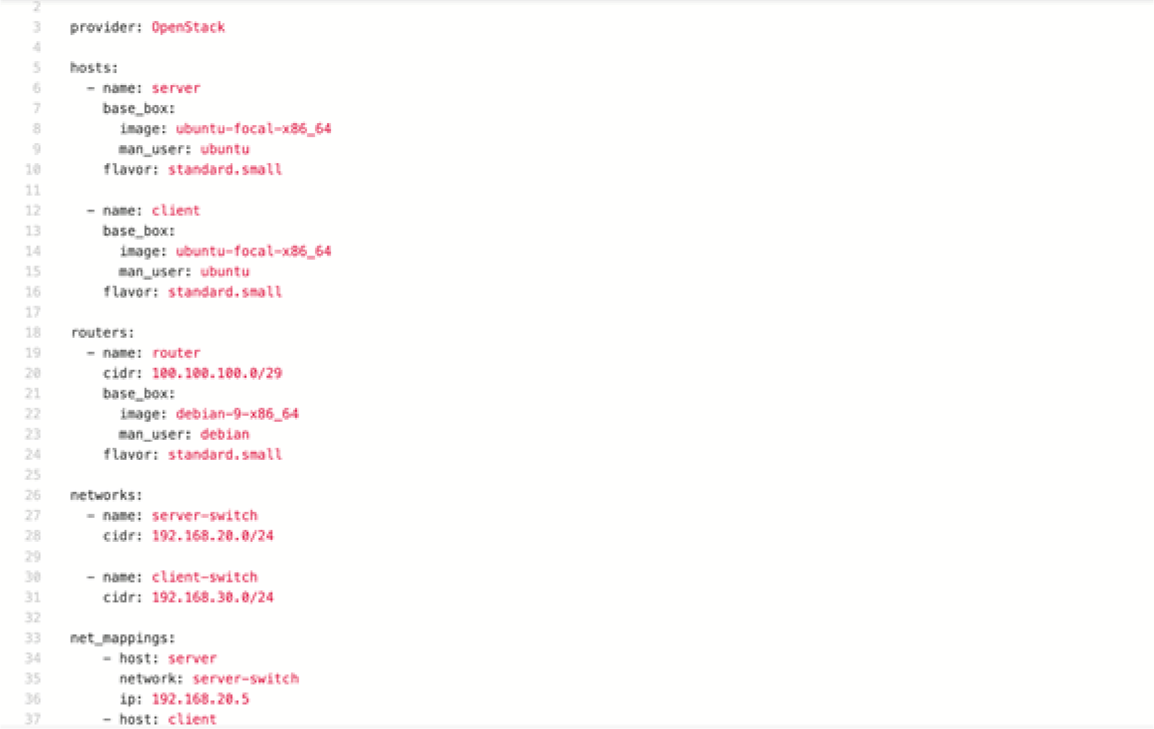
how to connect to instances, e.g., user name and SSH key. The Ansible tool is used to perform these actions. We use our virtual machines (build by Packer), but standard OpenStack images can also be used.

The second one is the Training definition. Definition includes information about the title, notes for instructors, learning outcomes, and levels. Currently, three types of levels are available

1. **Info Level**: Contains information for the trainee (welcome message or important information about the following levels).
2. **Game Level**: In this level, the user has to solve a predefined assignment. By solving the assignment, the trainee acquires a secret flag, and after submitting the flag, they can continue to the next level of the training.
3. **Assessment Level**: It can be either a test or a questionnaire, and it serves to test users' knowledge or gets feedback from users. The assessment can contain one of the following types of question:
    - **Multiple choice question (MCQ)**: Trainees are asked to select one or multiple answers from the choices offered as a list.
    - **Extended matching item (EMI)**: Trainees are asked to pair items from row and column that are semantically related.
    - **Freeform question (FFQ)**: Trainees are asked to type the answer to the submit field.

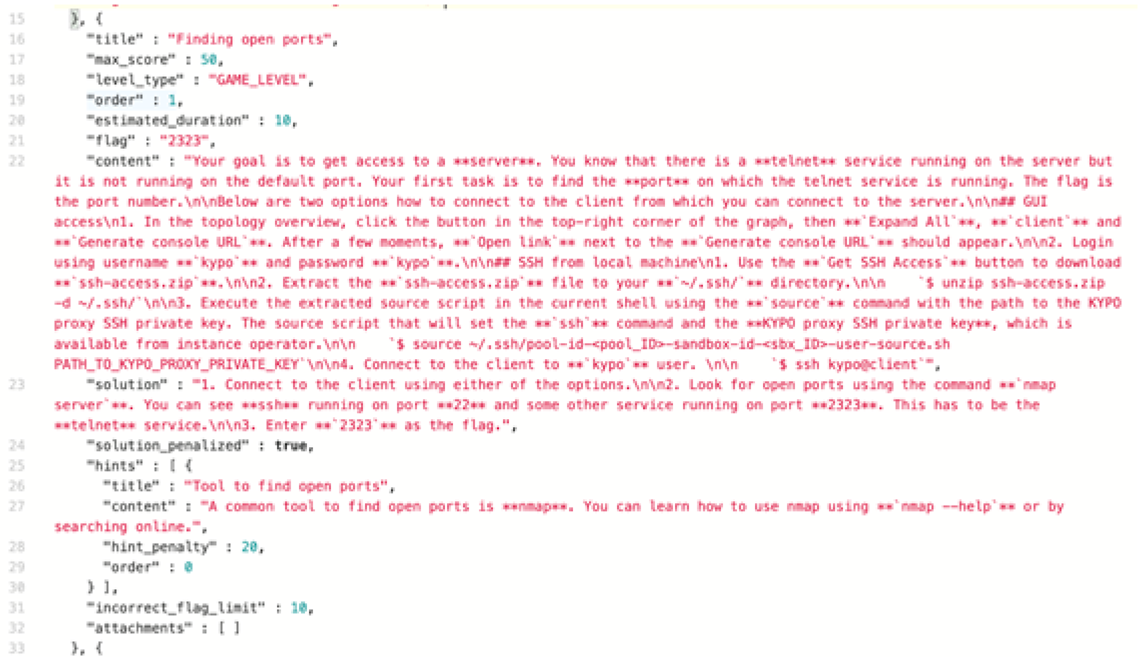
CODE (ICE&T)

VMWare vRealize Orchestrator is used to deploy internally defined environments. It is planned to implement some sort of import functionality based on the YAML format presented by MUNI (see Figure 20 and Figure 21 below).



```yaml

provider: OpenStack

hosts:
  - name: server
    base_box:
      image: ubuntu-focal-x86_64
      man_user: ubuntu
    flavor: standard.small

  - name: client
    base_box:
      image: ubuntu-focal-x86_64
      man_user: ubuntu
    flavor: standard.small

routers:
  - name: router
    cidr: 100.100.100.0/29
    base_box:
      image: debian-9-x86_64
      man_user: debian
    flavor: standard.small

networks:
  - name: server-switch
    cidr: 192.168.20.0/24

  - name: client-switch
    cidr: 192.168.30.0/24

net_mappings:
    - host: server
      network: server-switch
      ip: 192.168.20.5
    - host: client
```

Figure 20: Screenshot of a released topology description format



```
  }, {
    "title" : "Finding open ports",
    "max_score" : 50,
    "level_type" : "GAME_LEVEL",
    "order" : 1,
    "estimated_duration" : 10,
    "flag" : "2323",
    "content" : "Your goal is to get access to a **server**. You know that there is a **telnet** service running on the server but
it is not running on the default port. Your first task is to find the **port** on which the telnet service is running. The flag is
the port number.\n\nBelow are two options how to connect to the client from which you can connect to the server.\n\n## GUI
access\n1. In the topology overview, click the button in the top-right corner of the graph, then **`Expand All`**, **`client`** and
**`Generate console URL`**. After a few moments, **`Open link`** next to the **`Generate console URL`** should appear.\n\n2. Login
using username **`kypo`** and password **`kypo`**.\n\n## SSH from local machine\n1. Use the **`Get SSH Access`** button to download
**`ssh-access.zip`**.\n\n2. Extract the **`ssh-access.zip`** file to your **`~/.ssh/`** directory.\n\n    `$ unzip ssh-access.zip
-d ~/.ssh/`\n\n3. Execute the extracted source script in the current shell using the **`source`** command with the path to the KYPO
proxy SSH private key. The source script that will set the **`ssh`** command and the **KYPO proxy SSH private key**, which is
available from instance operator.\n\n    `$ source ~/.ssh/pool-id-<pool_ID>-sandbox-id-<sbx_ID>-user-source.sh
PATH_TO_KYPO_PROXY_PRIVATE_KEY`\n\n4. Connect to the client to **`kypo`** user. \n\n    `$ ssh kypo@client`",
    "solution" : "1. Connect to the client using either of the options.\n\n2. Look for open ports using the command **`nmap
server`**. You can see **ssh** running on port **22** and some other service running on port **2323**. This has to be the
**telnet** service.\n\n3. Enter **`2323`** as the flag.",
    "solution_penalized" : true,
    "hints" : [ {
      "title" : "Tool to find open ports",
      "content" : "A common tool to find open ports is **nmap**. You can learn how to use nmap using **`nmap --help`** or by
searching online.",
      "hint_penalty" : 20,
      "order" : 0
    } ],
    "incorrect_flag_limit" : 10,
    "attachments" : [ ]
  }, {
```

Figure 21: Screenshot of a prototype of training description format

In order to deploy such topologies either ISO images or OVA/OVFs of the targeted systems would be needed. Besides vRealize Orchestrator some other tool (maybe Ansible) is needed for the automated network configurations inside the VMs or additional steps such as Microsoft AD settings (DNS, etc).

The ICE&T does not support assessment levels as such but maybe the available moodle server could be used to map the different levels and question types.

As CODE cyber range as a commercial CR currently does not provide an import/export format, multiple future steps and implementations are necessary. The VMWare's REST APIs (vSphere and vRealize) could be used to get VM and network information. The ICE&T cyber range uses Microsoft System Center Orchestrator to run several activities during a training.

UL (HNS)

The HNS (Hybrid Network Simulation) cyber-range platform provides an xml-based import/export format for exchanging topologies amongst HNS platforms, based on dedicated archives.

An HNS archive includes the different virtual machines (in the qcow2 format) stored into a separate directory (possibly compressed in tar.gz), complemented by a description of the physical properties (given by the hnsEntryConfig.xml file of a virtual machine, and corresponding to an example of such definition. There is no description of the internal modules/ packages/ networking configurations of the virtual machine (the full virtual machine is exported and is given inside the archive), only the physical properties are described. The archive also includes a topology definition referring to these entities and complemented by topology links. The HNS cyber-range platform does not support training definitions (such as info levels, game levels nor assessment levels introduced by KYPO).

We are considering the integration with respect to two aspects: the **building of topologies**, and the **configuration of virtual machines** from the KYPO open format. We are already capable to build network topologies using the open format and the HNS proprietary interface, through the development of a dedicated driver; the next step is to support the configuration of virtual machines using Ansible definitions that are used in the open format.

UMIL (Cyber Range from Threat Arrest Project)
From a methodological point of view, the threat-arrest cyber range implements a model-based approach based on the Cyber Threat and Training Preparation (CTTP) models. The models, that are at the core of the training scenarios implementation, are built upon the analysis undertaken in the following steps: 1) analysis of a pilot system, 2) tailoring a programme to the organization's needs and creating a virtual twin of the actual system, 3) training and user feedback, and 4) post-training auditing and security level evaluation.
Phase 1: considers hardware and software components, with an automated analysis of known vulnerabilities, system logs, with a semi-automated analysis consisting of automatic statistical analysis and manual examination by experts, and personnel interviews, discussing behavioral aspects.
Phase 2: tailors a training programme to the organization needs. It correlates the program with professional specification/certification standard programmes.
Phase 3: implements basic training activities. It is composed of teaching (lectures, tutorials, awareness videos, other teaching material) and evaluation (exercises, capstone projects, on-line tests) that will be proposed to the trainees. Then, advanced training is provided based on serious games, and hybrid cyber ranges (emulated and/or simulated environments). Automated trainee assessment is implemented based on evaluation reports, event captors, simulated attacks, fabricated logs, and post-training evaluation of the target systems where the trainees are supposed to operate and exploit the lessons learnt.
Phase 4 is composed of course evaluation and users' feedback. Continuous operational auditing is also implemented.

From a technological point of view, THREAT-ARREST cyber range builds on OpenStack IaaS, over which the platform tools run and strictly cooperate. The emulated environments are based on HEAT templates. In particular, the platform is composed by the following tools:

- Training Tool (TT), that provides the basic user interface, trainee assessment, scenario deploying, and act as orchestrator of the whole training process;
- Emulation Tool (ET), triggered by the TT, creates and makes available the emulated environments via a common web browser. The ET takes in input the relevant CTTP model and compiles it in HEAT YAML Templates;
- Simulation Tool (ST), based on the Jasima simulation framework, simulates attacks, user interaction, and sensors data flows in order to recreate realistic working environments. The ST is deployed by the ET, and configured by the TT when requested by the CTTP models;
- Gamification Tool (GT), that provides the infrastructure to supply the trainee with serious games (based on the online card game Protect) and interactive questionnaires to train user on the most common social engineering attacks;
- Data Fabrication Platform (DFP), that can be trigger by the TT and configured based on the CTTP models to produce customized system logs, to be injected inside the emulated environments;
- Assurance Tool (AT), that provides the trainers with facilities to create and manage the CTTP models, and mechanism for the pre- and post-evaluation of vulnerabilities inside the target systems. The results of the evaluation will be exploited to evaluate

the trainees and the training activities basing on the improvement of the target system overall vulnerability level.

Inter-platform communication among the tools are guaranteed via the RabbitMQ message broker.

Metamodeling of the emulated environment: OpenStack[1] resource types can be a common base to describe the physical aspects of the cyber ranges., while the general aspects of the training scenario can be generically described with the means of simple descriptive fields. In particular, the proposed metamodel can support the modeling of

- the VMs included in the scenario, in terms of image, memory, disk, vCPUs, and network interface;
- possible script to be launched with the VM instancing;
- description of the network in terms of CIDR and common gateway, as requested by OpenStack;
- possible routers connecting the networks;
- general description of the training scenario, in terms of title, description, and difficulty level (to be agreed on a common scale).

The exchange language should not be limited to XML, but also JSON can be a good candidate notation. The proposed metamodel is general enough to allow all the different cyber ranges to describes their virtual lab. Since an automatic translation could be out of the scope of this collaboration, the proposed exchange format gives all the building blocks that can be used by the trainers to describe their scenarios and, when needed, create new scenario (manually) basing on the imported description.

Cyber Range Focus Group Cooperation

We continue in cooperation with the other pilots (ECHO, SPARTA, CyberSec4Europe) and H2020 projects (THREAT-ARREST) in the area of cyber range platforms and cyber range based trainings. Furthermore, T3.3 participates in CCN's Cyber Range Focus Group and leads one of the activities in the group. As the result of talks inside, Cyber Range Focus Group T3.3 organized CCN Webinar on Cyber Ranges to show different approaches to solve cyber range topics through the four pilots and foster cooperation between the pilots.

In cooperation with partners from ECHO and SPARTA, MUNI submitted an article[2], The Current State of The Art and Future of European Cyber Range Ecosystem, in IEEE International Conference on Cybersecurity and Resilience (CSR). The article covers the state of the art and describes a possible development of European cyber ranges.

The following events were held with CONCORDIA's participation

CODE - CTF and CTF qualification–	26-27.11. 2021
CODE's Jeopardy-style CTF involved multiple categories of challenges. The teams had to go through an online qualifying CTF. https://www.unibw.de/code/events/ctf-2021/view	
UL – 3 rd Security Management Course	22-26. 11. 2021
The UL course provided an overview of methods and tools related to security management in an integrated manner, the different	

[1] https://docs.openstack.org/heat/latest/template_guide/openstack.html

[2] https://ieeexplore.ieee.org/xpl/conhome/9527731/proceeding

practical exercises being performed over the cyber range platform. http://telecomnancy.univ-lorraine.fr/fr/security-management	
Capture the Flag event on the TELECOM Nancy Cyber-security platform - Done with strict sanitary restrictions	26.-27.1. 2021
UL Cybersecurity Hackathon Day - Done with strict sanitary restrictions	26. 5. 2021

Table 5. Task T3.3 Training events in Y3

CODE - CTF and CTF qualification–	26-27.11. 2021
CODE's Jeopardy-style CTF involved multiple categories of challenges. The teams had to go through an online qualifying CTF. https://www.unibw.de/code/events/ctf-2021/view	
UL – 3 rd Security Management Course	22-26. 11. 2021
The UL course provided an overview of methods and tools related to security management in an integrated manner, the different practical exercises being performed over the cyber range platform. http://telecomnancy.univ-lorraine.fr/fr/security-management	
Capture the Flag event on the TELECOM Nancy Cyber-security platform - Done with strict sanitary restrictions	26.-27.1. 2021
UL Cybersecurity Hackathon Day - Done with strict sanitary restrictions	26. 5. 2021

4.5 Outlook Y4

Our plans for T3.3 in Y4 are:

Virtual Lab

- Collaborate with Task 3.1 and Task 3.2 for common platform access
- Get more information about features and terms of use in the context of existing cybersecurity labs and improve remote access for public use
- Motivation (ongoing) to share infrastructure (inside and beyond consortium) and strengthen cooperation to increase added value

Services

In year 4, we plan to create best practice guides for the organization of cyber trainings such as capture the flag (CTF) or cyber range events. We want to increase the number of tools, evaluate and give added value. The plan is to provide a more fine-grained mechanism of filtering and search in the available CONCORDIA items.

Training

- UL/Telecom Nancy is planning to organize a third edition of the **Security Management** course week for the Fall 2022, as well as to organize a cybersecurity **hackathon day** centered on the cyber-security of industrial systems, mixing student teams with industrial participants, and based on the best practice guide established by the ANSSI cyber-security agency.
- T3.3 will promote a community around KYPO Cyber Range Platform (was released 11/20) and build a content ecosystem around the platform (as described above). All content will be described in the open format, MUNI will also encourage and increase the number of organizations inside and outside the consortium to use the open format in their cyber ranges and be a leading example in developing cyber range content. The open format for sharing training content for cyber ranges is fully developed and successfully tested inside the consortium by the end of the project.

5. Establishing a European education ecosystem for cybersecurity (T3.4)

5.1 Task objective

This task contributes to the development of a European Education Ecosystem for Cybersecurity through a number of targeted actions addressing mainly the cybersecurity industry and its professionals (e.g. technicians, mid-level management, executives) and teachers.

5.2 Preamble

The work of the task T3.4 in Y3 builds on the outcomes of the Y1 and Y2. The map of courses and trainings for cybersecurity professionals launched in Y1 was updated in Y2 and revamped in Y3 in terms of content and appearance. Based on the Methodology for developing and deploying courses for cybersecurity professionals delivered in Y2, the task created and ran a course targeting the Cybersecurity Consultant role profile. The analysis of the different certification schemes which was subject of a specific report in Y2 and the pilot certification exam ran in conjunction with the course targeting the consultant role profile built the basis for a skills certification scheme developed in Y3. The survey developed under Teach-the-Teachers activity end of Y2, was deployed in Y3 and complemented with interviews. Finally, as part of building the education ecosystem action, the cross-pilots Education group setup in Y2, continued working together by addressing specific challenges selected by the group in collaboration with ENISA and ECSO.

5.3 Status

The Task 3.4 is progressing as planned. The map of courses for professionals was revamped, and two instances of the course addressing the cybersecurity consultant role profile plus the associated Skills Certification Scheme were deployed. Under the Teach-the-Teachers activity we continued collecting feedback from stakeholders via survey and interviews. The collaboration with the other three pilots within the Cybersecurity Competence Network (CCN) - Education focus group[1] continued while focusing on specific priorities, thus advancing the development of the European Education Ecosystem for Cybersecurity. The task contributed further to the CONCORDIA Roadmap by revising and updating the chapter linked to Education.

5.4 Key achievements Y3

In the Year 3 (2021), under Task T3.4 the effort was allocated to the following actions:

- *Action 1.* Pooling, assessing and disseminating existing courses
- *Action 3.* Develop courses for cybersecurity professionals;
- *Action 4.* Develop a framework for a CONCORDIA certificate to be attached to the courses produced by the consortium
- *Action 5.* Teach-the-Teachers
- *Action 6.* Contribute to building a European Education Ecosystem for Cybersecurity.

[1] Cybersecurity Competence Network (CCN) Education formed of representatives of the 4 pilot projects (CONCORDIA, SPARTA, ECHO CYBERSEC4EUROPE) working on Education related tasks.

Figure 22. depicts the 6 actions of the Task 3.4 where the green colour illustrates the progress we made under the different task actions from the beginning of the project (totally green means completed such as Action 2, and white means to be done).

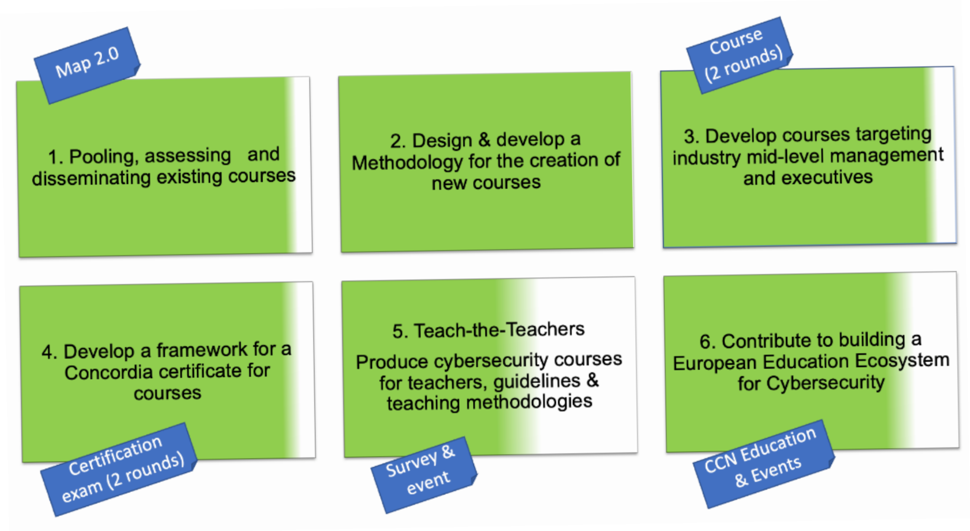

Map 2.0
1. Pooling, assessing and disseminating existing courses
2. Design & develop a Methodology for the creation of new courses
Course (2 rounds)
3. Develop courses targeting industry mid-level management and executives
4. Develop a framework for a Concordia certificate for courses
Certification exam (2 rounds)
5. Teach-the-Teachers
Produce cybersecurity courses for teachers, guidelines & teaching methodologies
Survey & event
6. Contribute to building a European Education Ecosystem for Cybersecurity
CCN Education & Events

Figure 22: Structure of the Task T3.4 actions and progress from the beginning of the project

5.4.1 Updating the CONCORDIA map on courses for cybersecurity professionals

In Y3 we have revamped the courses map. This new version of the map brings improvements both on functionalities and on the content. From the functionality's viewpoint, with support of FORTH partner we have created individual accounts to all course owners to allow them full access to their content. This way they are able to update/delete the existing content and provide new content if the case. After the technical implementation of the changes, in mid-September the old content was automatically uploaded on the platform and the old course providers were invited to simply check and update it. In support of their work, we have created a user manual[1.] The map 2.0 was subject of a communication campaign during the European Cybersecurity Month in October to attract new course providers.

Content-wise the new version of the courses map[2] is organized under 3 tabs:

- The first tab displays the different filters available for the end users to more easily identify the content based on their needs;
- the second tab is mainly addressed to course providers and offers details on the purpose of the map, the link and explanations on the way to submit content for the map;
- the third tab is providing quick links to the ENISA database of university related courses and to Education related news and reports Besides, the information collected regarding the courses was extended by adding to the form 3 new fields: (1) Institution Type (university / private organization / public organization / PPP); (2) Proficiency Level (beginner / intermediate / advanced); (3) Fee (free/charges applies)

[1] https://www.concordia-h2020.eu/wp-content/uploads/2021/08/RegisteryourCourse.pdf

[2] https://www.concordia-h2020.eu/map-courses-cyber-professionals/.

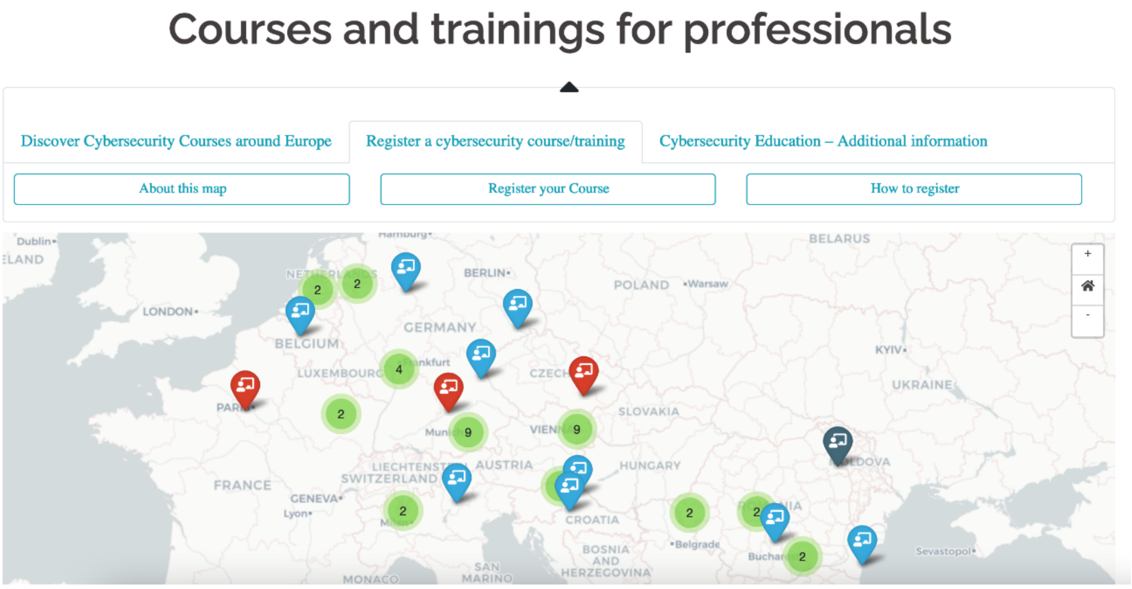


Figure 23: CONCORDIA map 2.0 (view from the second tab)

5.4.2 Deploying the course for Cybersecurity Consultant role profile

Following the development of the course targeting the Cybersecurity Consultant role profile in Y2, in Y3 we ran two instances of the course: the pilot in the first semester of the year, and an open session of the course in the second half of the year.

The course deployment model

Since the role of the Cybersecurity Consultant has been identified as intermediate in level, the course is directed to professionals already active in cybersecurity or individuals having already some basic knowledge in cybersecurity.

Considering the targeted profile, the course content addresses three main learning objectives (LO):
LO1: Threats – Get updated on the existing and emerging cybersecurity threats, the assets possible to be impacted, and the latest models of attacks.
LO2: Technology – Become knowledgeable about specific technological threats, learn how to anticipate and prevent them, while developing proactive management skills.
LO3: Economics – Get an understanding of the economics behind cybersecurity activities within your organization. Learn about risk management and information security to protect the corporate reputation and preserve customer loyalty.

The course is organized in two modules: an online module and a face-to-face/live webinar module, as illustrated below:

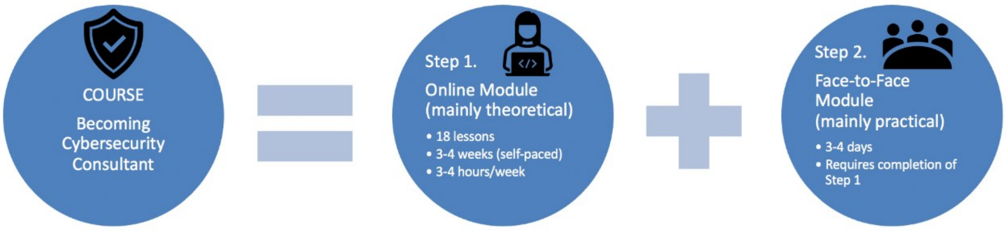

COURSE
Becoming Cybersecurity Consultant
Step 1.
Online Module (mainly theoretical)
• 18 lessons
• 3-4 weeks (self-paced)
• 3-4 hours/week
Step 2.
Face-to-Face Module (mainly practical)
• 3-4 days
• Requires completion of Step 1

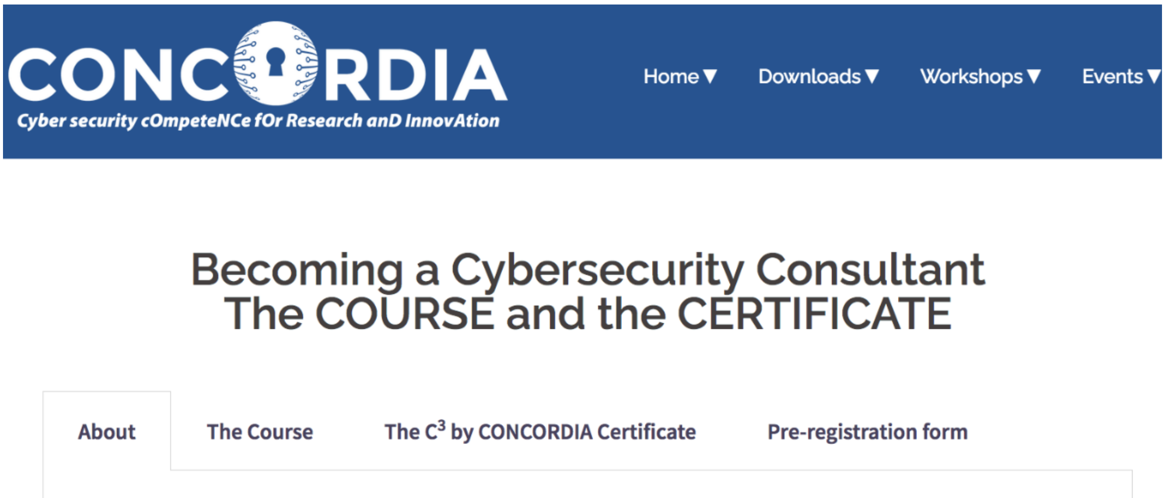
Figure 24: Structure of the CONCORDIA course

The online content is hosted under the COURSERA platform, and currently contains a total of 19 lessons (see Figure 29 for the last version of the structure) deployed over 59 videos and 22 quizzes, covering about 12 hours of study (quizzes not included). The content (lessons and quizzes) is structured and automatically proposed to be taken over a period of 4 weeks with reminders set accordingly and sent automatically to the participants by the platform. Yet, the learners can follow the lessons and take the quizzes at their own pace since all the content is fully accessible to the registered learners from the beginning of the period until the very last day.

The Face-to-Face/webinar part of the course is designed to build on the theoretical concepts covered in the online part by bringing into the discussion of the group different case studies while also involving the participants in hands-on exercises. The agenda of the webinar is organized over 3 half days, 3 hours a day (see Figure 30 for the last version of the agenda). The exercises vary in style, from simulations on specialized platforms such as Moon Cloud[1] and KYPO CRP[2] to paper based and were time bound. In order to keep the participants fully engaged and motivated, we invite them to share their individual results via private channels on Slack[3] with the lecturer. The solutions are afterwards discussed with the whole group.

The access to the webinar is given only to the participants who successfully finished the online module (listened to all videos and passed all the quizzes). This will ensure a similar level of understanding of the topics targeted by the course, thus a smooth flow of the exercises and associated discussions.

The information on the course, its target audience, the deployment model and the associated Certification scheme are presented on the project website[4].


CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion
Home ▼
Downloads ▼
Workshops ▼
Events ▼

Becoming a Cybersecurity Consultant
The COURSE and the CERTIFICATE

About
The Course
The C^3 by CONCORDIA Certificate
Pre-registration form

Figure 25: Tabbed structure of the webpage presenting the course and the certificate

[1] https://www.moon-cloud.eu/en/
[2] https://crp.kypo.muni.cz/
[3] https://slack.com/
[4] https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/

The Pilot course

In order to test and validate the content of the course, we have invited each project partner to delegate 2 representatives to attend the course and provide feedback. As a courtesy, we also extended the invitation to the external participants who took part in the webinar in June 2020 (see the workshop page[1]) and contributed to the definition of the Cybersecurity Consultant role profile.

The online module was open in private mode between January 21 – March 8 and was followed by the webinar on May 11-12-13. Due to the COVID-19 restrictions, the face-to-face module of the pilot course was organized as a live webinar.

From the 150 people invited, 48 of them decided to enroll in the online part of the course and 29 participants managed to finish the module. The rest of the participants did not manage to score 80% or higher in the quizzes, criteria set as a condition to advance from one module to another. We then proceeded to invite all the 29 successful learners to register for the second part of the course but only 12 of them finally managed to accommodate their agenda to the live event. The participants' funnel is depicted below.

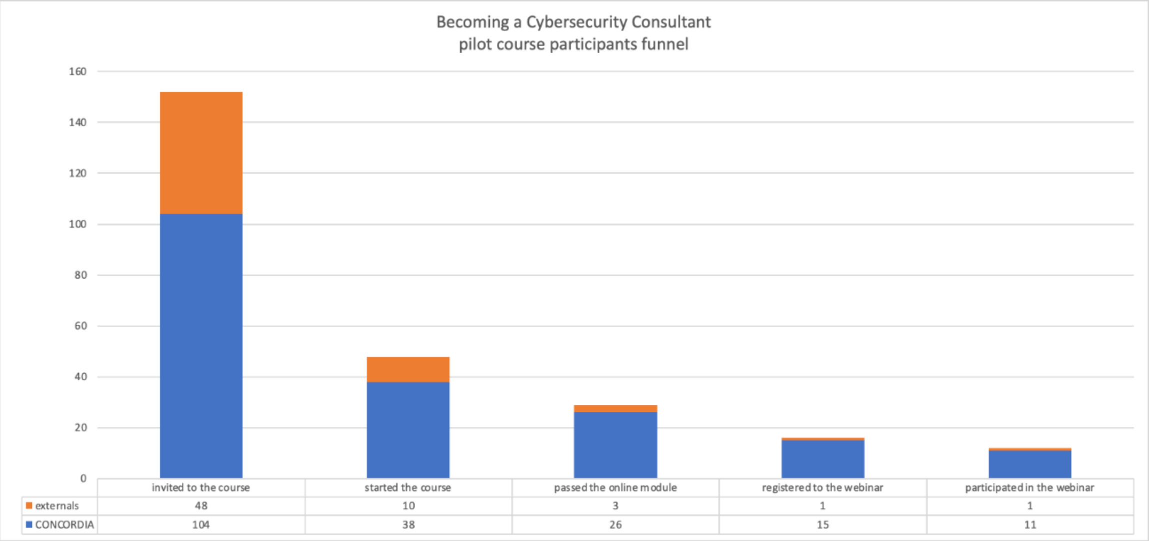


Figure 26: Pilot course - the participants' funnel

Out of the 12 participants to the webinar, 4 were coming from the industry, 5 represented universities or research organizations and 3 were coming from other types of professional cyber-related entities.

Gender wise, only 10% of the participants starting the pilot-course and finishing the online module were female. The absolute values of the participants in the pilot course from gender perspective are presented in the figure below.

[1] https://www.concordia-h2020.eu/workshops/workshop-education-2020/

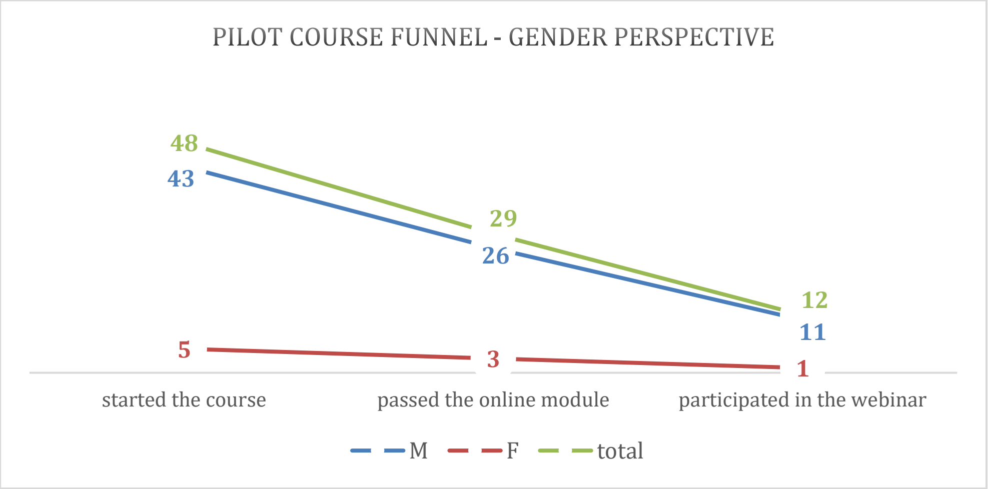


Figure 26b: Pilot course participants' funnel: gender perspective

Following the closure of the pilot course we have compiled a Report[1] including details on this pilot in terms of structure, its deployment and the feedback collected from the participants following each of the course modules. The feedback received from the participants was overall positive and very positive. We took on board some of their suggestions, between them (1) adding new videos on the online module (e.g., description of the targeted role profile, risk management) and (2) offering more space for hands on exercises during the webinar, and we moved toward organizing the first open-to-the-market course.

The first open-to-the-market instance of the course

The first open course was scheduled to start in October, during the European Cybersecurity Month. In view of reaching out to as many potential participants as possible, we have opened a pre-registration form already in mid-June. The pre-registration was promoted via the CONCORDIA newsletter and the European Commission specific Cybersecurity newsletter, and on social media. By end of September, we have received pre-registrations from 71 individuals from 17 European countries, more than half of them representing Corporates, SME/startups and freelancers.

The online module ran on the Coursera platform in the second half of October, and it was taken by 45 participants. Out of this group 23 of them managed to finish all the lessons and pass all the quizzes and were invited to attend the webinar. Finally, only 15 of them attended in full the 3 half-days webinar.

[1] https://www.concordia-h2020.eu/wp-content/uploads/2021/07/Pilot_Course_BCSC_Report_Final.pdf

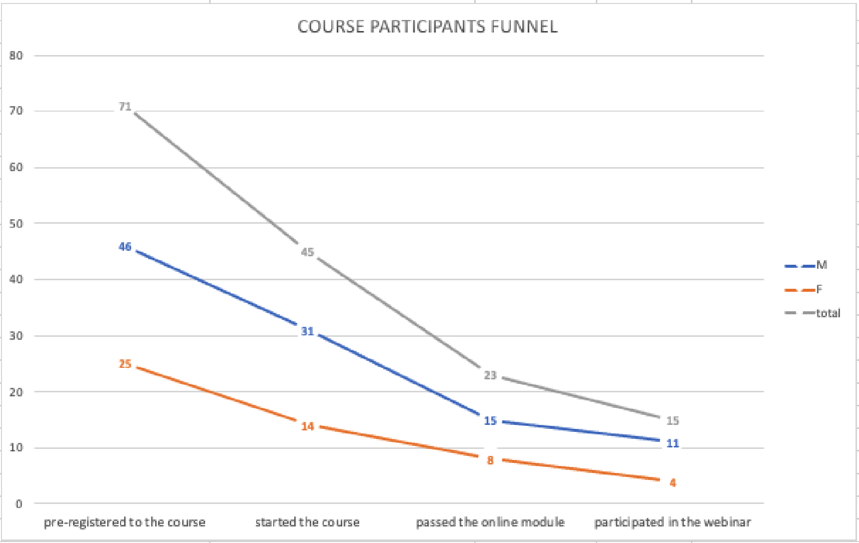
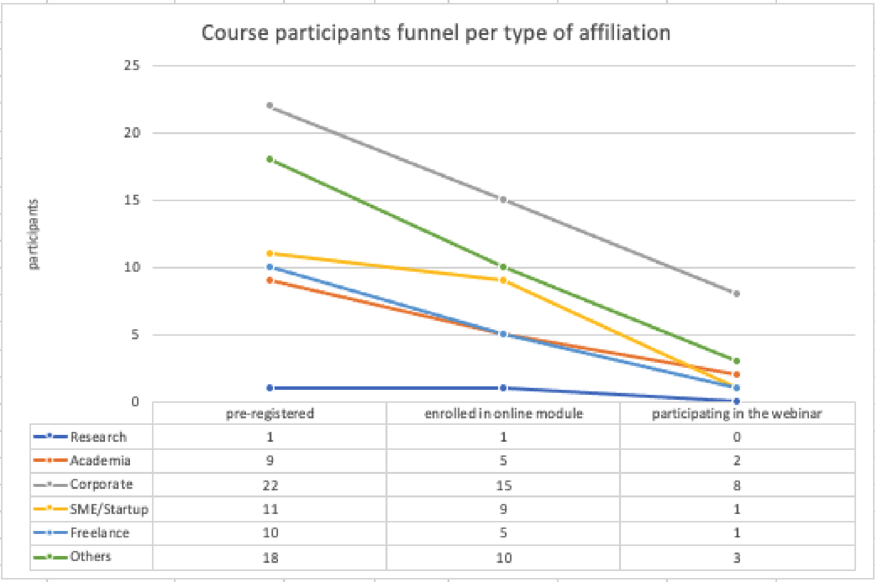


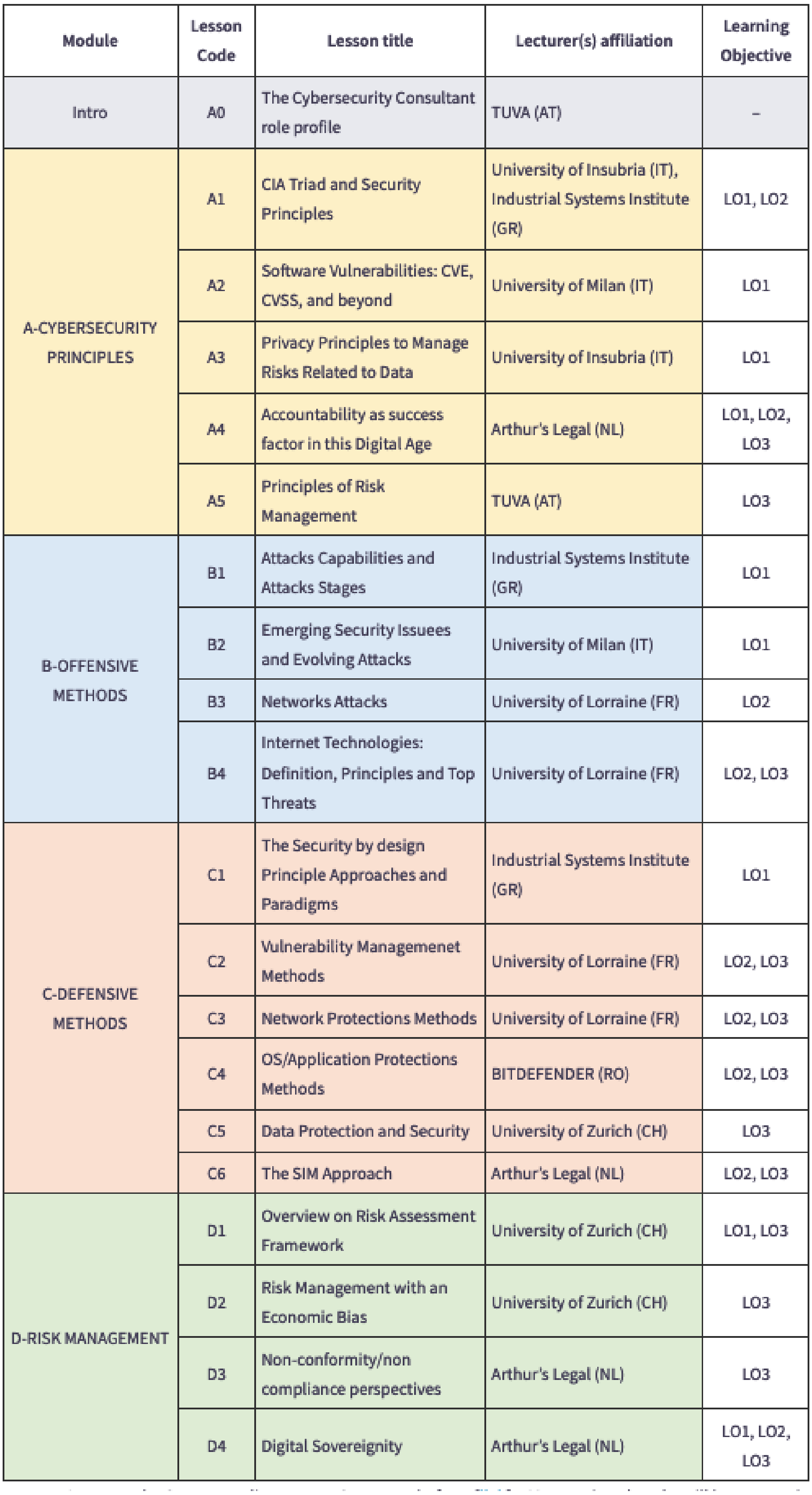
Figure 27: Course participants funnel, gender perspective



	pre-registered	enrolled in online module	participating in the webinar
Research	1	1	0
Academia	9	5	2
Corporate	22	15	8
SME/Startup	11	9	1
Freelance	10	5	1
Others	18	10	3

Figure 28: Course participants funnel, per type of organization

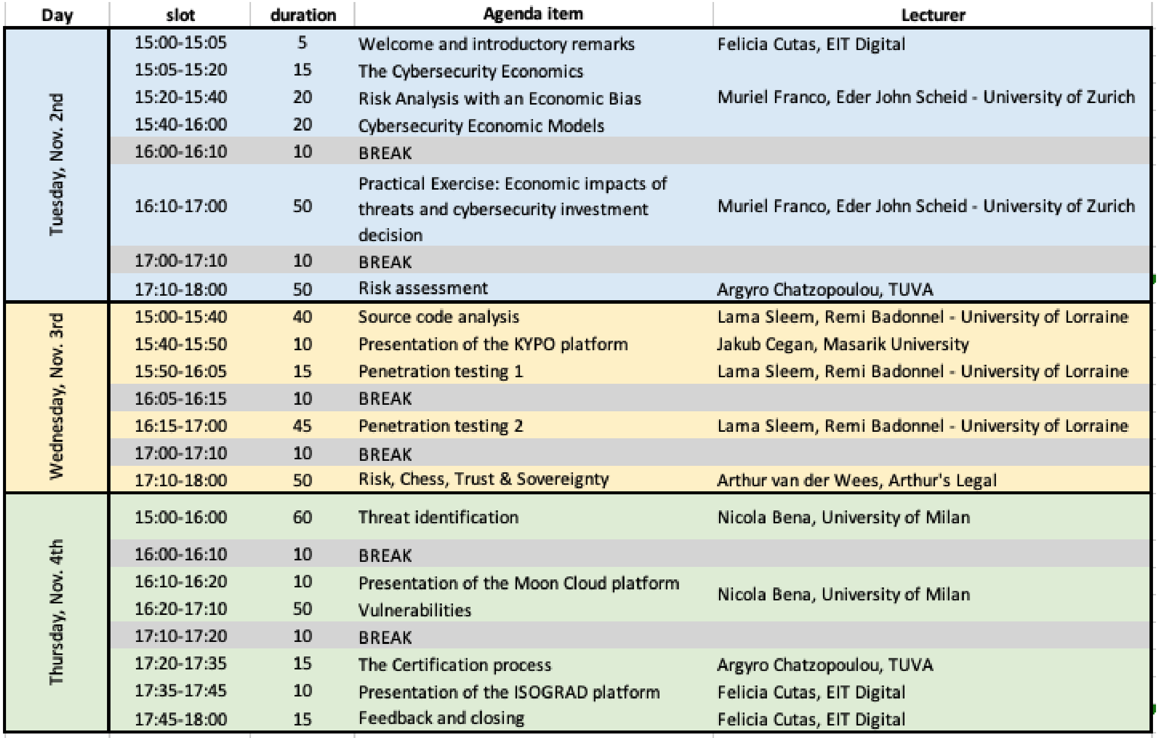
An overview of the online content presenting the title of the lessons, the organizations covering the specific content and the link between the lessons and the specific learning objectives is depicted below:



Module	Lesson Code	Lesson title	Lecturer(s) affiliation	Learning Objective
Intro	A0	The Cybersecurity Consultant role profile	TUVA (AT)	–
A-CYBERSECURITY PRINCIPLES	A1	CIA Triad and Security Principles	University of Insubria (IT), Industrial Systems Institute (GR)	LO1, LO2
	A2	Software Vulnerabilities: CVE, CVSS, and beyond	University of Milan (IT)	LO1
	A3	Privacy Principles to Manage Risks Related to Data	University of Insubria (IT)	LO1
	A4	Accountability as success factor in this Digital Age	Arthur's Legal (NL)	LO1, LO2, LO3
	A5	Principles of Risk Management	TUVA (AT)	LO3
B-OFFENSIVE METHODS	B1	Attacks Capabilities and Attacks Stages	Industrial Systems Institute (GR)	LO1
	B2	Emerging Security Issuees and Evolving Attacks	University of Milan (IT)	LO1
	B3	Networks Attacks	University of Lorraine (FR)	LO2
	B4	Internet Technologies: Definition, Principles and Top Threats	University of Lorraine (FR)	LO2, LO3
C-DEFENSIVE METHODS	C1	The Security by design Principle Approaches and Paradigms	Industrial Systems Institute (GR)	LO1
	C2	Vulnerability Managemenet Methods	University of Lorraine (FR)	LO2, LO3
	C3	Network Protections Methods	University of Lorraine (FR)	LO2, LO3
	C4	OS/Application Protections Methods	BITDEFENDER (RO)	LO2, LO3
	C5	Data Protection and Security	University of Zurich (CH)	LO3
	C6	The SIM Approach	Arthur's Legal (NL)	LO2, LO3
D-RISK MANAGEMENT	D1	Overview on Risk Assessment Framework	University of Zurich (CH)	LO1, LO3
	D2	Risk Management with an Economic Bias	University of Zurich (CH)	LO3
	D3	Non-conformity/non compliance perspectives	Arthur's Legal (NL)	LO3
	D4	Digital Sovereignity	Arthur's Legal (NL)	LO1, LO2, LO3

Figure 29: Structure of the course online content

The webinar was deployed on 2-3-4 November from 15:00-18:00 CET based on the following agenda:



Day	slot	duration	Agenda item	Lecturer
Tuesday, Nov. 2nd	15:00-15:05	5	Welcome and introductory remarks	Felicia Cutas, EIT Digital
	15:05-15:20	15	The Cybersecurity Economics	Muriel Franco, Eder John Scheid - University of Zurich
	15:20-15:40	20	Risk Analysis with an Economic Bias	
	15:40-16:00	20	Cybersecurity Economic Models	
	16:00-16:10	10	BREAK	
	16:10-17:00	50	Practical Exercise: Economic impacts of threats and cybersecurity investment decision	Muriel Franco, Eder John Scheid - University of Zurich
	17:00-17:10	10	BREAK	
	17:10-18:00	50	Risk assessment	Argyro Chatzopoulou, TUVA
Wednesday, Nov. 3rd	15:00-15:40	40	Source code analysis	Lama Sleem, Remi Badonnel - University of Lorraine
	15:40-15:50	10	Presentation of the KYPO platform	Jakub Cegan, Masarik University
	15:50-16:05	15	Penetration testing 1	Lama Sleem, Remi Badonnel - University of Lorraine
	16:05-16:15	10	BREAK	
	16:15-17:00	45	Penetration testing 2	Lama Sleem, Remi Badonnel - University of Lorraine
	17:00-17:10	10	BREAK	
	17:10-18:00	50	Risk, Chess, Trust & Sovereignty	Arthur van der Wees, Arthur's Legal
Thursday, Nov. 4th	15:00-16:00	60	Threat identification	Nicola Bena, University of Milan
	16:00-16:10	10	BREAK	
	16:10-16:20	10	Presentation of the Moon Cloud platform	Nicola Bena, University of Milan
	16:20-17:10	50	Vulnerabilities	
	17:10-17:20	10	BREAK	
	17:20-17:35	15	The Certification process	Argyro Chatzopoulou, TUVA
	17:35-17:45	10	Presentation of the ISOGRAD platform	Felicia Cutas, EIT Digital
	17:45-18:00	15	Feedback and closing	Felicia Cutas, EIT Digital

Figure 30: Agenda of the webinar

The activity was coordinated by EIT Digital and received substantial support in all its phases, from design to implementation, from CONCORDIA academic and industry partners: University of Milan, University of Loraine, University of Zurich, The Industrial System Institute Greece, University of Insubria BITDEFENDER, Arthur’s Legal. Since the pilot course was developed and deployed in conjunction to the pilot Cybersecurity Skills Certification scheme, the process required a close collaboration with TÜV Trust IT GmbH, member of the TÜV Austria Group.

5.4.3 Towards a Cybersecurity Skills Certification Scheme

This activity was deployed in strong collaboration with task T5.3 - Certification.

In Year 3 (2021) Task 3.4 ran two instances of the skills certification exam for the Cybersecurity Consultant role profile – C^3 by CONCORDIA. The activity was deployed in conjunction with the course “Becoming a Cybersecurity Consultant”.

The model

The Certification exam is structured in two steps: a theoretical exam to test the knowledge acquired during the online part of the course, and a practical exam to test the skills and abilities developed during the live webinar part of the course.

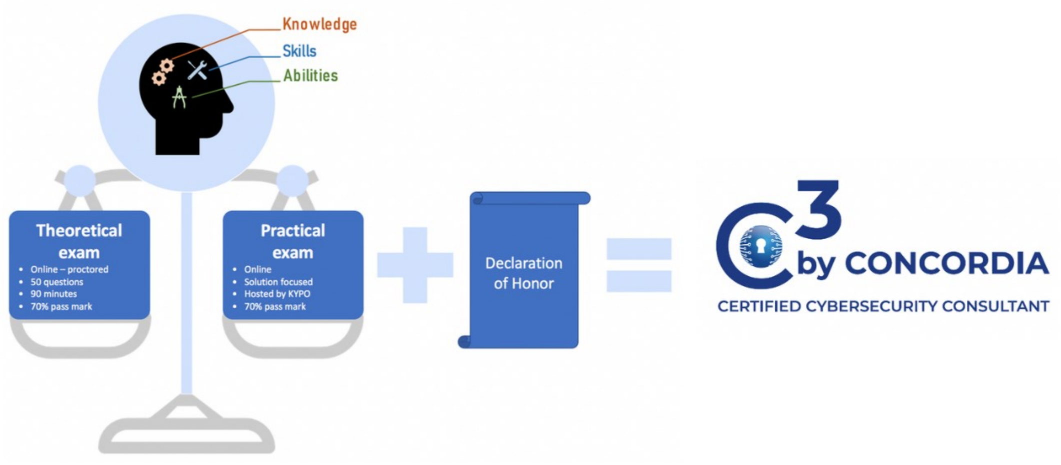


Figure 31: The elements of the C^3 by CONCORDIA certification

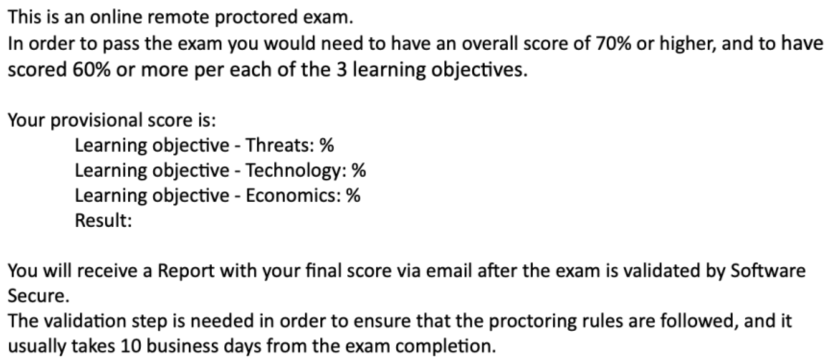
The theoretical exam is running under ISOGRAD – a specialized platform for deploying AI assisted proctored examinations. The candidates are invited via email to participate in the theoretical part of the exam, within a specific timeframe of about 10 working days. Each participant has the opportunity to select the desired timeslot to undertake the exam, based on her/his preference. Clear instructions on setting up their accounts and using the platform are given to the participants upfront via a manual.

The participants sitting in this exam have 90 minutes to answer a set of 50 multiple choices questions. The questions are selected from a databank of 170 questions by applying a specific algorithm which considers

- the category of the questions (e.g. the learning objectives used in the Course: Threats, Technology, Economics) by ensuring that all learning objectives will be equally covered
- the level of difficulty by applying the formula: 30% Low - 50% Medium- 20% High level of difficulty

In order for a participant to pass the exam they should reach an overall score of at least 70%, with a minimum 60% success rate per each of the three learning objectives. Each question is awarded one mark. No negative marking is applicable.

An analysis of the result is displayed to the candidate after the completion of the test (see Figure 32. below), but a specific text was crafted to inform them that this would not be the final results as the review and quality review is pending.



This is an online remote proctored exam.
In order to pass the exam you would need to have an overall score of 70% or higher, and to have scored 60% or more per each of the 3 learning objectives.

Your provisional score is:
Learning objective - Threats: %
Learning objective - Technology: %
Learning objective - Economics: %
Result:

You will receive a Report with your final score via email after the exam is validated by Software Secure.
The validation step is needed in order to ensure that the proctoring rules are followed, and it usually takes 10 business days from the exam completion.

Figure 32: Example of message received at the end of the theoretical exam

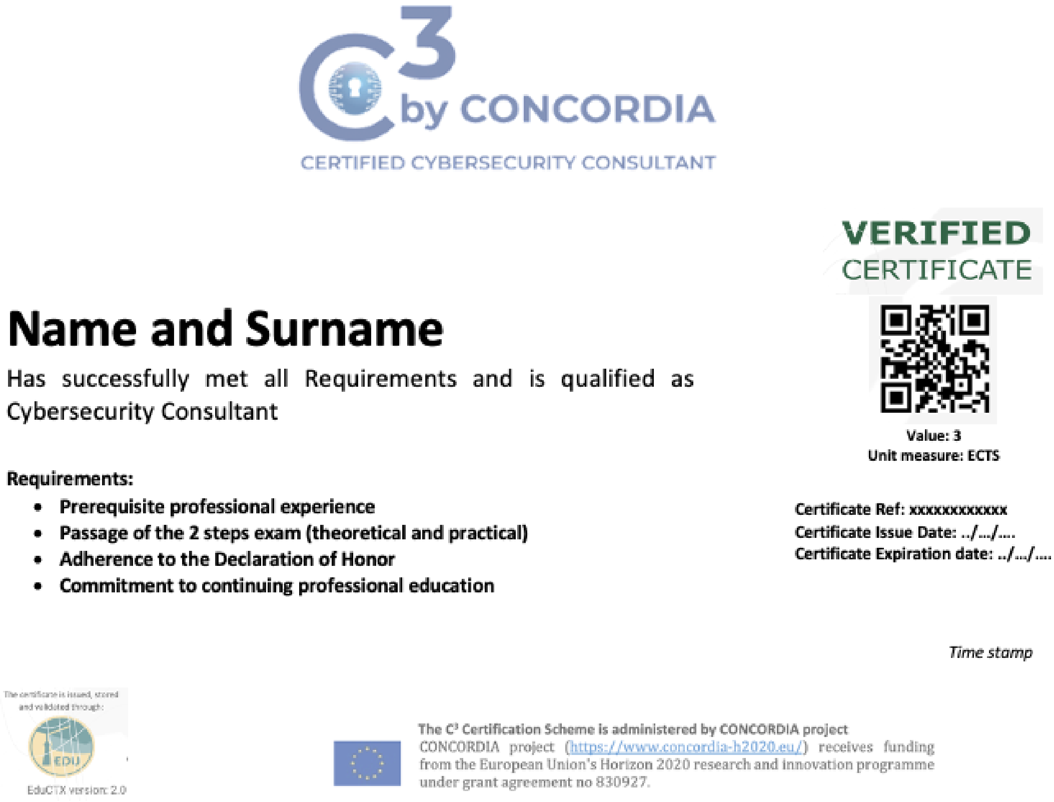
The practical exam consists of solving a specific scenario implemented through two different platforms: KYPO - Kypo Cyber Range (CRP)[1] and Moon Cloud[2]

The implemented scenario aimed to assess and validate skills and abilities of the participants within the following domains: Risk assessment; Threat identification; Vulnerabilities; Source code analysis; Penetration testing.

With respect to the scoring, KYPO CRP uses a level-based approach combining hands-on exercises with tests (single/multiple choice). Tests are evaluated with no negative points. The hands-on exercise allows 5 attempts for the correct answer. After that the solution is displayed and the trainee gets 0 points for the exercise.

The details linked to the setting up of the platforms and on the deployment of the pilot exams were captured in the Pilot Skills Certification report which is included as annex in the Deliverable D5.4.

After the exams are completed and the results are announced, the participants successfully passing both exams are receiving a certificate. The C^3 by CONCORDIA certificate is issued under the blockchain based platform EduCTX[3], developed and managed by University of Maribor. The certificate contains, between others, information regarding the date of issuing and expiration, the conditions of validity and security elements for easy identification.



C3 by CONCORDIA

CERTIFIED CYBERSECURITY CONSULTANT

VERIFIED CERTIFICATE

Name and Surname

Has successfully met all Requirements and is qualified as Cybersecurity Consultant

Requirements:

- **Prerequisite professional experience**
- **Passage of the 2 steps exam (theoretical and practical)**
- **Adherence to the Declaration of Honor**
- **Commitment to continuing professional education**

Value: 3
Unit measure: ECTS

Certificate Ref: xxxxxxxxxxxx
Certificate Issue Date: ../…/….
Certificate Expiration date: ../…/….

Time stamp

The certificate is issued, stored and validated through:

EduCTX version: 2.0

The C^3 Certification Scheme is administered by CONCORDIA project
CONCORDIA project (https://www.concordia-h2020.eu/) receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

Figure 33: Draft template C3 by CONCORDIA Certificate

[1] https://docs.crp.kypo.muni.cz/

[2] https://www.moon-cloud.eu/en/

[3] https://eductx.org/

The pilot Certification exam

An application for the C^3 by CONCORDIA certification exam was created and dispatched on the 25th of May 2021 to all participants of the Cybersecurity Consultant course which successfully attended both the online and live webinar modules of the course. The received applications were reviewed by the project team in relation to the certification scheme acceptance criteria. An acceptance email was sent to the relevant participants, providing information on the timeline of the examination.

The period that the exam could be undertaken through the ISOGRAD platform was June 1st – June 14th, 2021. The number of candidates that passed the theoretical exam after the quality review were eight (8). The average score for people that passed the theoretical exam was 79.5% and of those that failed 70.5% (this is above the 70% required overall threshold, but the requirement that an above 60% grade should be achieved in each of the sections was not met).

The period that the exam could be undertaken through the Moon Cloud and KYPO Cyber Range platform was June 1st – June 14th, 2021. The number of participants in the practical exams was 6. All the participants passed the practical exams. The average score for people that passed the practical exam was 90%.

The first open-to-market Certification exam

The first open-to-the-market Certification exam was launched on November 5th by sharing with the participants to the course the link to the registration form. For this instance of the Certification exam, T3.4 developed a specific form under the EU Survey platform. The exams were deployed based on the following schedule:

- The theoretical exam was scheduled for the period November 16th – November 29th
- The practical exam was scheduled for the period December 12th – December 17th.

At the time of closing this deliverable the Certification process was under deployment thus the results will be reported in the subsequent deliverable (D3.4).

The activity on Certification was coordinated by EIT Digital and TÜV Trust IT GmbH, member of the TÜV Austria Group, and received support from University of Milan, University of Loraine, University of Zurich, The Industrial System Institute Greece, University of Insubria, BITDEFENDER, Arthur's Legal, Masaryk University, University of Maribor.

The feedback received from the participants to the Certification exams helped finalizing the C^3 by CONCORDIA Certification Scheme[1] developed under task T5.3. The document describes the model proposed to setup and run the certification exam thus detailing the following elements:

[1] https://www.concordia-h2020.eu/wp-content/uploads/2021/11/Concordia_Certification_SchemeC3_v1.pdf

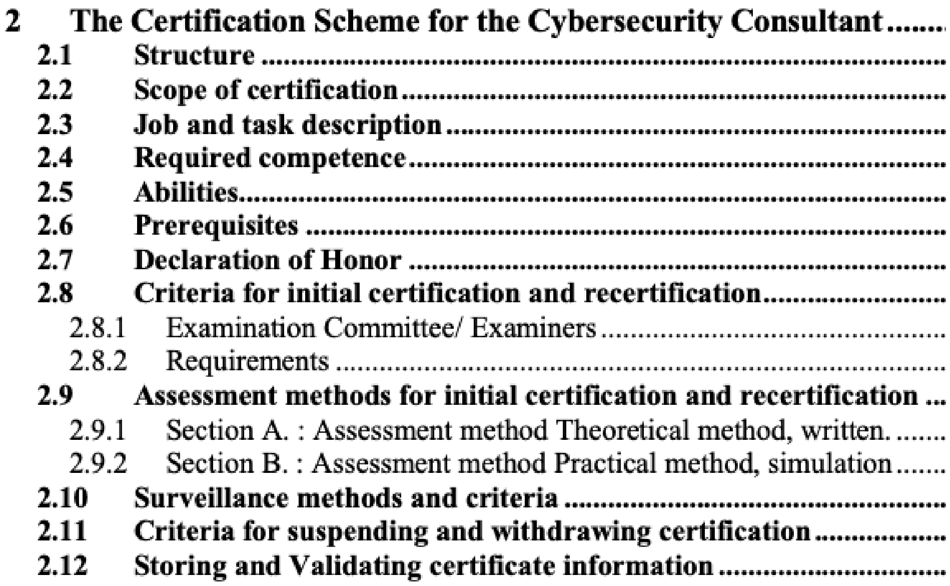


Figure 34: CONCORDIA Skills Certification Scheme - excerpt from the List of Contents

5.3.4. Teach-the-Teachers

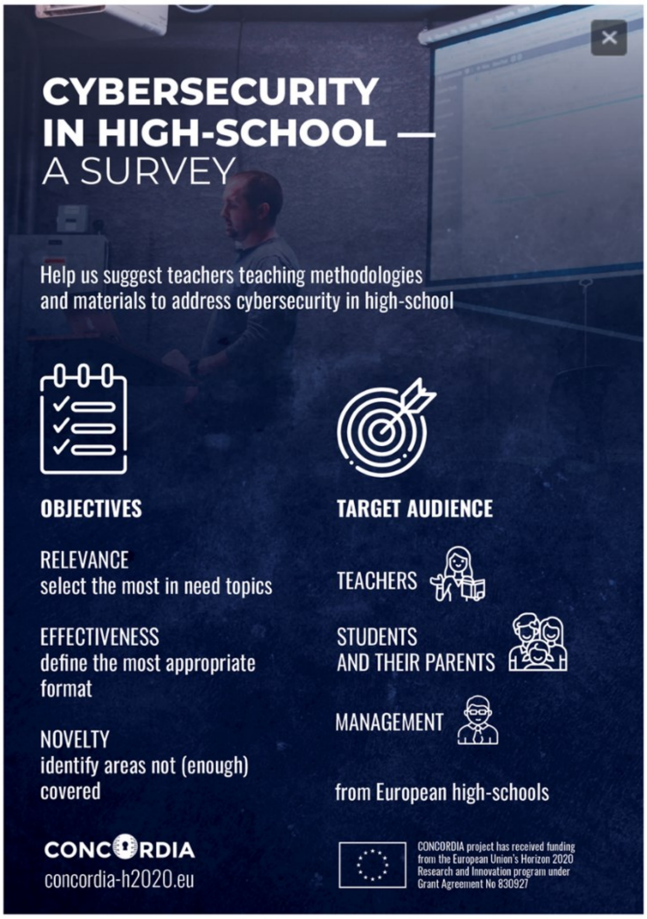
Under this action T3.4 aims at developing a set of tools and a specific methodology for the use of teachers when teaching cybersecurity and cybersafety to their high-school students.

In order to identify the current needs in terms of content and delivery methodologies fit for high-school level, we decided on applying a funnel approach by starting with collecting structured data via an EU wide survey followed by interviews with a small group of people. The identified needs are then further validated in a live event before moving to the next step in the process, the design of the materials. By the end of the project, we aim at piloting the content created.

End of year 2020 Task 3.4 launched a survey linked to the Teach-the-Teaches activity which aimed at collecting information from a pool of stakeholders on the type of content and delivery methodologies fit for high-school level. Concretely, the survey has the following objectives:

- RELEVANCE: To select the most in need topics to be covered in the materials.
- EFFECTIVENESS: To define the most appropriate format for the materials to be developed.
- NOVELTY: To identify areas not covered (enough) by existing programs.

The main target audience of the survey is composed of teachers, students and their parents, and the management of the high-schools within Europe.



CYBERSECURITY IN HIGH-SCHOOL — A SURVEY

Help us suggest teachers teaching methodologies and materials to address cybersecurity in high-school

OBJECTIVES

RELEVANCE
select the most in need topics

EFFECTIVENESS
define the most appropriate format

NOVELTY
identify areas not (enough) covered

TARGET AUDIENCE

TEACHERS

STUDENTS AND THEIR PARENTS

MANAGEMENT

from European high-schools

CONCORDIA
concordia-h2020.eu

CONCORDIA project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927

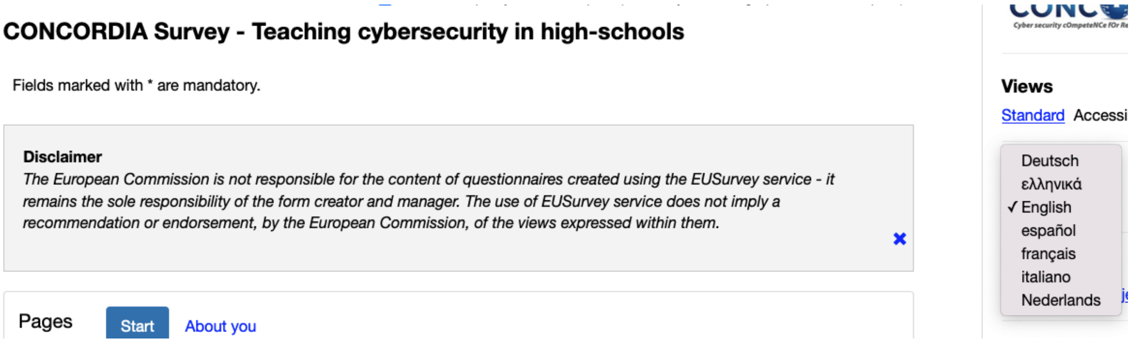
Figure 35. Visual used to promote the survey on social media channels

Since the audience of the survey is diverse, the questions have been customized accordingly per audience type. The question regarding the audience is the first one and this affects the rest of the questions accordingly.

Independent of the audience, the elements covered by the survey are:

- Demographics (anonymized)
- Digital Services used by high-school students in general
- Digital Services used by high-school students in the school environment
- Devices used by high-school students in general
- Devices used by high-school students in the school environment
- Degree of confidence of high-school students' specific online activities
- Degree of awareness of high-school students' regarding online risks
- Incidents experienced by high students related to online risks
- Possible subjects that could be discussed within a relevant cybersecurity course for high school students
- Type of methods/instruments to be used while teaching cybersecurity at high-school level
- Cybersecurity subjects of courses already existing

The CONCORDIA Survey - Teaching cybersecurity in high-schools[1] was built on the EU survey platform in English and launched online in December 2020. Starting January 2021, it was translated and made available in six additional languages such as German, Spanish, French, Italian, Greek, Dutch, and continued to be disseminated on social media.



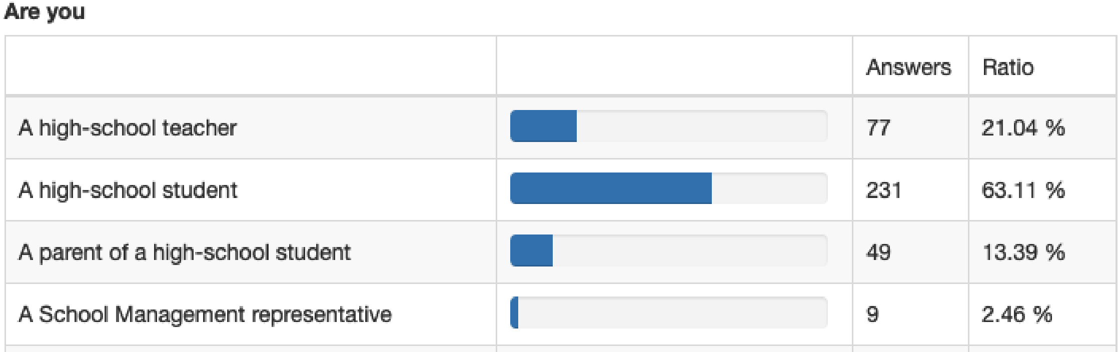
CONCORDIA Survey - Teaching cybersecurity in high-schools

Fields marked with * are mandatory.

Disclaimer
The European Commission is not responsible for the content of questionnaires created using the EUSurvey service - it remains the sole responsibility of the form creator and manager. The use of EUSurvey service does not imply a recommendation or endorsement, by the European Commission, of the views expressed within them.

Figure 36: Print-screen of the survey, displaying the available languages

Until November 2021 we have collected input from 366 participants, out of which more than half were high-school students.



Are you

		Answers	Ratio
A high-school teacher		77	21.04 %
A high-school student		231	63.11 %
A parent of a high-school student		49	13.39 %
A School Management representative		9	2.46 %

Figure 37: Distribution of contributors to the survey per categories

The current contributors are coming from 10 EU member states, in their vast majority representing Romania (46%), Slovenia (24%), Greece (13%), Cyprus (12%). The promotion of the survey was done via mainly two channels: social media and CONCORDIA network. The posts on social media did not benefit from a paid campaign; the country-based results reflect the connections different project partners have within national ecosystems, which helped disseminating the information locally.

After collecting initial input via the survey, we ran a series of 10 interviews with teachers and parents accepting to help us further in the process. The objective of the interviews was to refine the conclusions of the survey and get more in-depth feedback.

The analysis of the answers collected via the survey and the interviews was structured under a specific report[2] and made public in December 2021.
The main findings of the analysis are:

[1] https://ec.europa.eu/eusurvey/runner/6e30ed0b-3888-eff4-e85f-0d7c92f178db

[2] https://www.concordia-h2020.eu/wp-content/uploads/2021/12/TEACHING-CYBERSECURITY-IN-HIGH-SCHOOL-survey_report.pdf

- Students feel more confident in most of the online activities, but their parents and teachers are more concerned about their level of confidence. Here, we needed to measure if students do not only feel confident but also are confident in taking online actions in a secure and safe way. To do so we asked the students a number of questions to assess their cybersecurity skills, the analysis of those questions is presented later in this report under the "Responses per country analysis".
- Students also seem to be more confident in being aware of, being able to detect, avoid and handle the risks than their parents and teachers believe they are. Teachers look to be more concerned than the parents. And handling the risks seems to be the statement that also students mention they feel less confident about. These results show cybersecurity courses need to focus also on risk coping techniques to teach students not only to be aware of the risks but also to be prepared to respond to those risks properly.
- The results of our study show that many high-school students have experienced an online risk, proving that actions need to be taken to educate and support students in topics related to cybersecurity. Additionally, it seems that students do not share their risks' experiences with their parents, and teachers. It could be seen as a sign that they do not trust them or talk about such topics with them but maybe with their friends or other adults. By including cybersecurity as a part of high-school courses or as a mandatory topic to be discussed in high-school environment, a collaboration between students, teachers and parents might be built in handling the online risks.
- Even if cybersecurity is taught in high schools (based on teachers' responses), students and parents seem to be mostly unaware of it. More effort is needed to promote and to establish cybersecurity courses in high schools.
- In identifying the 'hot' cybersecurity topics that are more important to discuss during a course with high-school students, the three groups of participants agreed on the topics of 'Being safe in online social media', 'Recognizing Fake Accounts', 'Ensuring Privacy'. The selection of these topics is in line with the very high percentage (93%) of participants mentioning that they use social media applications, but it is opposed to the level of confidence students mention they feel in those activities. More specifically the students replied to be 'confident' (on average) in being safe in online social media platforms and recognizing fake online content and 'neutral confident' in ensuring their privacy.
- The cybersecurity courses need to be built with more interactive and gamified instruments that will engage the students to participate in, be more interested and pay attention to learn.

Since the answers to the survey came mainly from 4 countries, T3.4 looked also into identifying potential differences in perception between the same categories of target audience located in different countries. The analysis flags sometimes significant differences in perceptions within the same target category but based in different countries. These findings will be considered when drafting the methodology for the use of the high-school teachers.

On more general terms, the interviews reveal that there is a high interest about cybersecurity among teachers, parents, and students, however, there seems to be a gap between the education and the cybersecurity experts' community. This gap affects the communication between these two groups and consequently the ability to design and apply context-specific solutions. The participants to the interview describe large diversities between cybersecurity education across institutes (current state of play), but they all seem to agree on the necessary steps that must be done onwards (future strategy). Indicative example is that all participants concur towards the need for interactive courses on cybersecurity. Another aspect that has been identified in this analysis, has to do with the lack of coordinated actions and initiatives across EU to support schools and students. Currently, cybersecurity education is either provided as an additional topic inside computer science courses or through independent activities organized by external providers and agencies (e.g., Munich police was mentioned by one participant to the interview). Furthermore, the lack of central coordination and well-defined protocols and strategies also affects the ability to identify and respond to incidents.

T3.4 intends to keep the survey open in Y4 and promote it further, in an attempt to collect input from stakeholders located in other EU countries. The initial findings subject of the above-mentioned report will be further refined with the new input.

As a subsequent step to the survey and interview phases, in order to validate the findings and test the interest of the teachers and students to some existing solutions within the consortium in view of developing them further, we started organizing a webinar. Since almost half of the contributions to the survey came from Romania, T3.4 decided to answer positively to the invitation coming from the ADeSE NGO to contribute to the one-week event Cybershare Academy for Schools[1] in December 2021. The event brought together 14 teachers and 93 high-school students coming from 11 schools from Romania and Croatia. It was co-organized with tasks T3.3 and T4.5 and included presentations of the survey results, workshops for beginners and advanced students, a Capture-the-Flag challenge ran under KYPO cyber-range platform, and a panel on girls-in-cyber. The presentation of the event and the top 3 winning schools make the subject of a specific newsitem[2] on the CONCORDIA website.

The overall activity was coordinated by EIT Digital and received support from CONCORDIA partners: Cyprus University of Technology, TÜV Trust IT GmbH, Research Institute CODE, University of Maribor, Institute Jozef Stefan, University of Zagreb, University of Patras, University of Lorraine, University of Insubria.

5.3.5. Building the Ecosystem

Coordinating the CCN Education cross-pilots group

In Y3, the collaboration initiated by T3.4 beginning of the year 2020 with the other 3 pilot projects ECHO, SPARTA and CyberSec4Europe under the Cybersecurity Competence Network CCN-Education focus group[3] continued. Starting 2021 the European organization ECSO was also actively involved in the group work.

[1] https://www.concordia-h2020.eu/news/cybershare-academy-for-schools/

[2] https://www.concordia-h2020.eu/news/cybershare-academy-for-school-2021/

[3] https://cybercompetencenetwork.eu/focus-groups/education-focus-group/

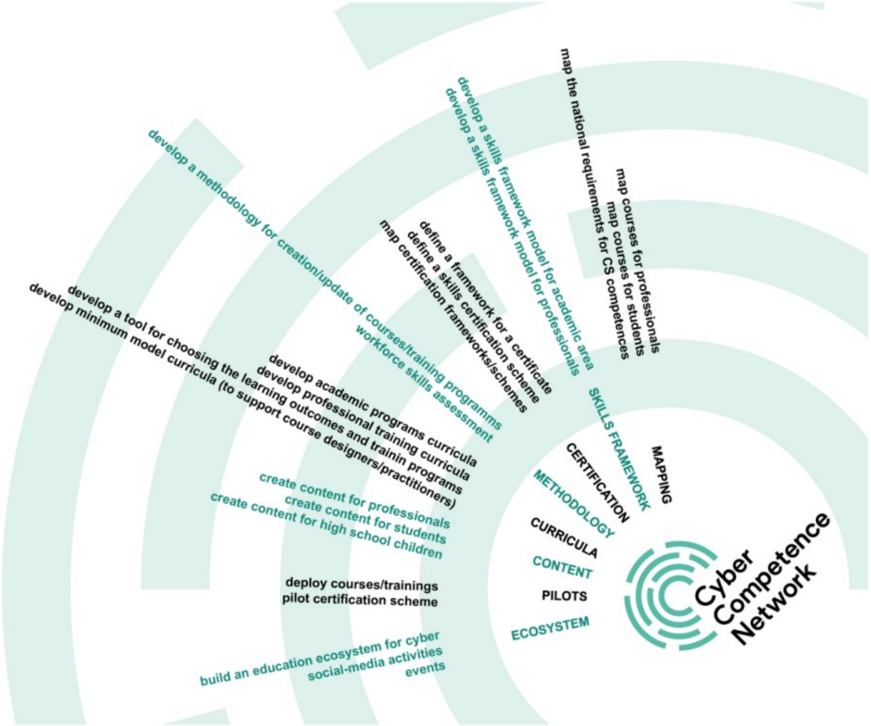
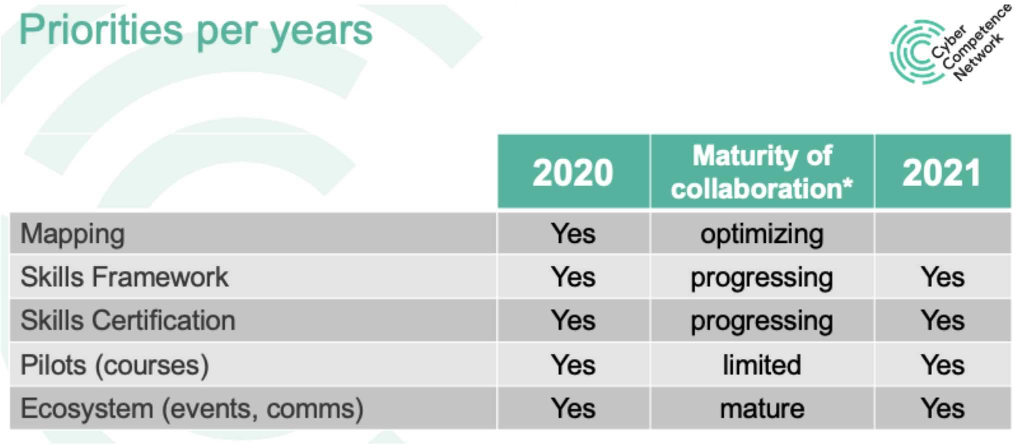

map the national requirements for CS competences
map courses for professionals
map courses for students
develop a skills framework model for academic area
develop a skills framework model for professionals
define a framework for a certificate
define a skills certification scheme
map certification frameworks/schemes
develop a methodology for creation/update of courses/training programms
workforce skills assessment
develop academic programs curricula
develop professional training curricula
develop a tool for choosing the learning outcomes and trainin programs
develop minimum model curricula (to support course designers/practitioners)
create content for professionals
create content for students
create content for high school children
deploy courses/trainings
pilot certification scheme
build an education ecosystem for cyber
social-media activities
events
MAPPING
SKILLS FRAMEWORK
CERTIFICATION
METHODOLOGY
CURRICULA
CONTENT
PILOTS
ECOSYSTEM
Cyber Competence Network

Figure 38: Summary of all Education related topics addressed by the 4 the pilots

Following an analysis of the individual projects' priorities, the group determined the themes of prime concern for this year. In view of taking this decision, we have attached to each of the topics a maturity of collaboration level using the scale: undefined / limited/ progressing / mature / optimizing. The main topics for collaboration in 2021 were selected from the categories 'progressing' and 'mature' while those under the heading 'optimizing' were used for communication purposes.


Priorities per years

	2020	Maturity of collaboration*	2021
Mapping	Yes	optimizing	
Skills Framework	Yes	progressing	Yes
Skills Certification	Yes	progressing	Yes
Pilots (courses)	Yes	limited	Yes
Ecosystem (events, comms)	Yes	mature	Yes

Figure 39: Assessment of the maturity of collaboration per strands &priorities for 2021

In concrete terms the CCN Education group:

(1) finalized the transfer of the database of courses collected by SPARTA and CS4EU to the ENISA database CyberHEAD while also cross linking with the CONCORDIA map of courses. The results were communicated via a newsitem on the CCN website[1].

(2) exchanged with ENISA in support of validating the skills framework and the 10 role profiles identified by the ENISA specific working group

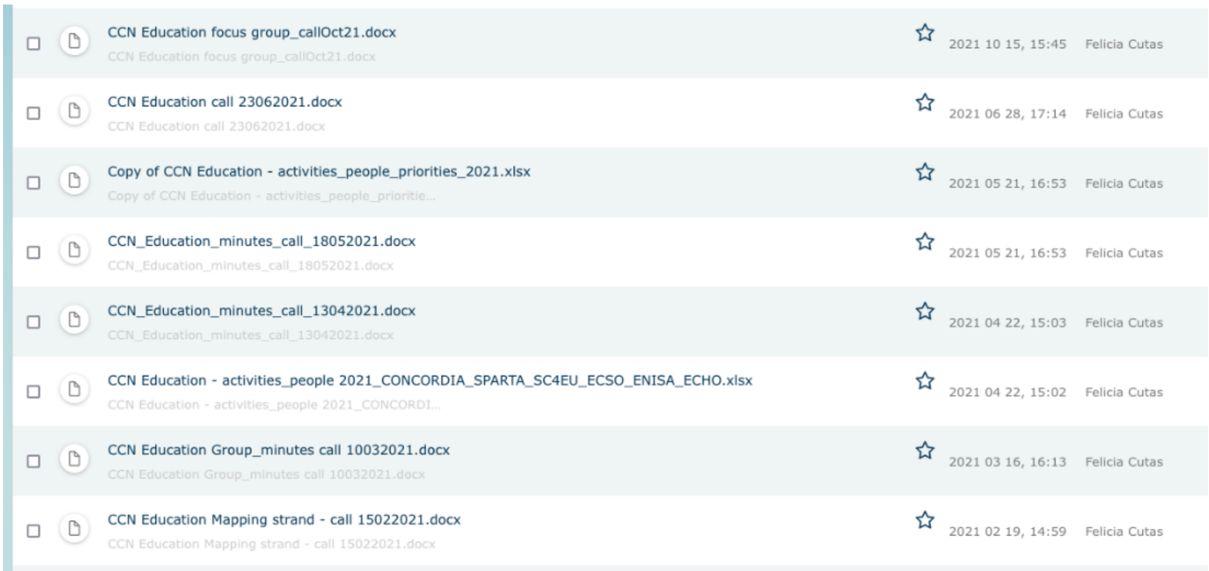
(3) supported individual efforts in running pilots such as CONCORDIA course and ECSO – ECHO corporate HR survey by promoting the initiatives in specific networks

(3) continued the collaboration on Certification strand between CONCORDIA and CS4EU on a joint project for certifying the MOOC platforms

(4) continued building the cybersecurity education related ecosystem: in the year 2021 CCN-Education went public by participating in a panel during the ARES conference – ETACS 2021[2] led by SPARTA. The discussions built on current issues and trends in cybersecurity training and education.

(5) provided feedback to the Education specific chapter of the ENISA draft Proposal for the future ECCC

The minutes of the periodic meetings were documented on the EC platform CIRCABC.



□	CCN Education focus group_callOct21.docx CCN Education focus group_callOct21.docx	☆	2021 10 15, 15:45	Felicia Cutas
□	CCN Education call 23062021.docx CCN Education call 23062021.docx	☆	2021 06 28, 17:14	Felicia Cutas
□	Copy of CCN Education - activities_people_priorities_2021.xlsx Copy of CCN Education - activities_people_prioritie...	☆	2021 05 21, 16:53	Felicia Cutas
□	CCN_Education_minutes_call_18052021.docx CCN_Education_minutes_call_18052021.docx	☆	2021 05 21, 16:53	Felicia Cutas
□	CCN_Education_minutes_call_13042021.docx CCN_Education_minutes_call_13042021.docx	☆	2021 04 22, 15:03	Felicia Cutas
□	CCN Education - activities_people 2021_CONCORDIA_SPARTA_SC4EU_ECSO_ENISA_ECHO.xlsx CCN Education - activities_people 2021_CONCORDI...	☆	2021 04 22, 15:02	Felicia Cutas
□	CCN Education Group_minutes call 10032021.docx CCN Education Group_minutes call 10032021.docx	☆	2021 03 16, 16:13	Felicia Cutas
□	CCN Education Mapping strand - call 15022021.docx CCN Education Mapping strand - call 15022021.docx	☆	2021 02 19, 14:59	Felicia Cutas

Figure 40: Excerpt from the Cybersecurity Education library on CIRCABC

Communicating with the Ecosystem

In Y3 the communication with the ecosystem was limited to online means due to the restrictions imposed by the COVID crisis.

[1] https://cybercompetencenetwork.eu/ccn-projects-contributed-to-the-enisa-cyberhead-portal-which-helps-students-to-choose-cybersecurity-programs/

[2] https://www.ares-conference.eu/conference-2021/detailed-program/

We have continued creating newsitems and reports to inform the followers about the progress on the different Education related activities and made them public under the dedicated section News and Reports on Education[1].

For the needs of the CONCORDIA course and certification for Cybersecurity Consultant[2], the respective webpages were compiled and the content was presented as a package on the project's website.

The different activities ran under the task such as the Teach-the-Teachers survey, the Cybersecurity Consultant course, the map – were subject to specific social media communication campaigns built and ran with support of Task 5.2 Communication. These activities were further promoted in the CONCORDIA stakeholders' newsletters built and disseminated by the Task 4.6 Stakeholders and were presented during the CONCORDIA open door 2021 event in virtual booths.

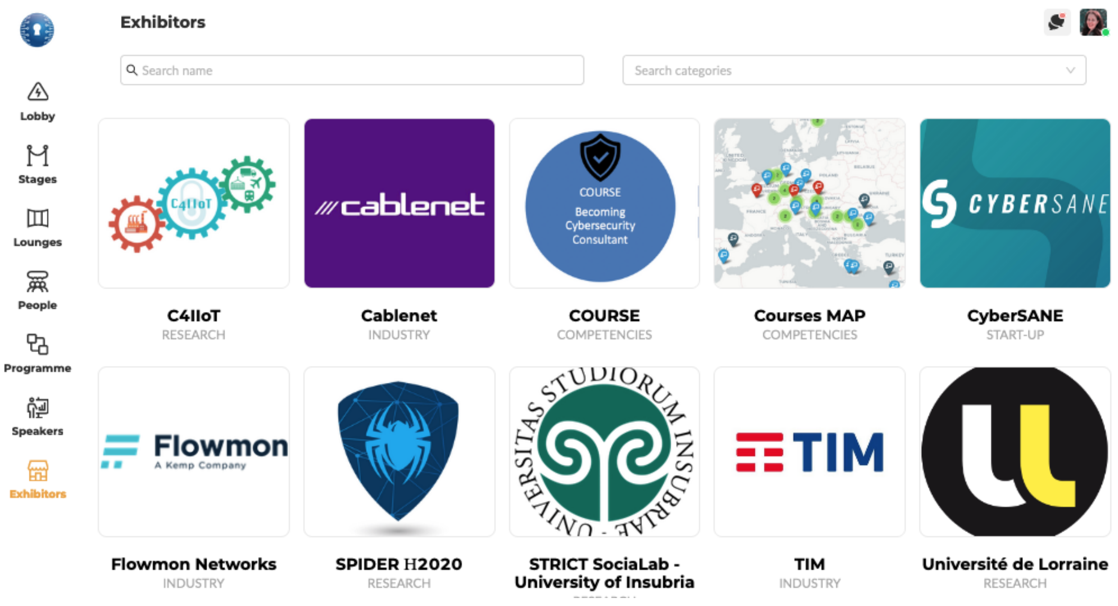


Figure 41: Content of the virtual exhibition room during COD2021

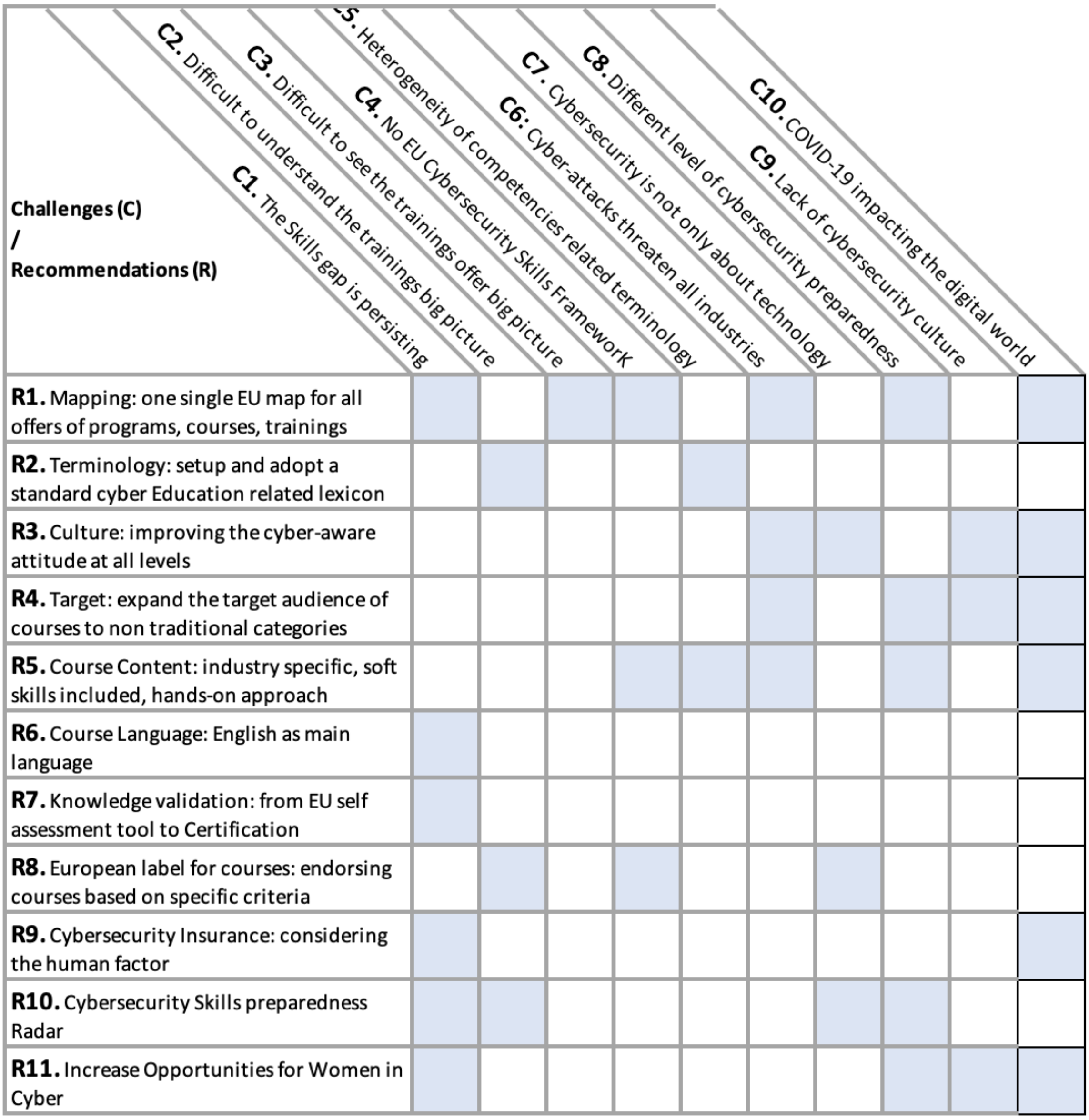
The Roadmap for Education and Skills

Finally, T3.4 contributed to the CONCORDIA roadmap by leading the chapter on Education. The CONCORDIA roadmap for Education and Skills aims at covering two main areas: Education for Cybersecurity Professionals and Cybersecurity Education in high-school. It will thus complement the efforts of the other pilot projects (SPARTA and ECHO) which are looking into the cybersecurity education at university level.

The challenges and recommendations mentioned in the roadmap for Education and Skills[3] are based on our findings when assessing CONCORDIA's courses portfolio, which were further revised in Y3. The recommendations aim at answering but also complementing

[1] https://www.concordia-h2020.eu/concordia-news-and-reports-on-education/
[2] https://www.concordia-h2020.eu/workshops/workshop-education-2020/
[3] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

some of the actions put forward by the European Commission in the Digital Education Action Plan (2021-2027).

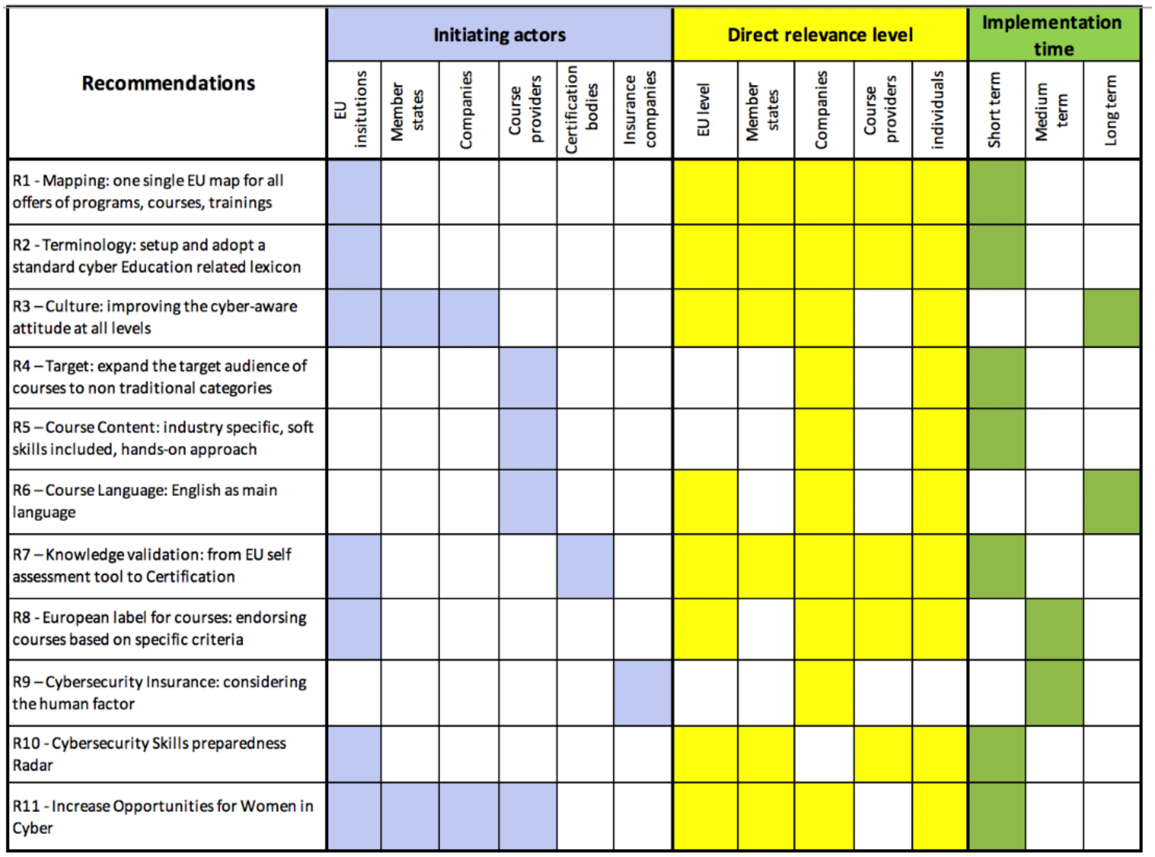


Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings big picture	C3. Difficult to see the trainings offer big picture	C4. No EU Cybersecurity Skills FrameworK	5. Heterogeneity of competencies related terminology	C6: Cyber-attacks threaten all industries	C7. Cybersecurity is not only about technology	C8. Different level of cybersecurity preparedness	C9. Lack of cybersecurity culture	C10. COVID-19 impacting the digital world
R1. Mapping: one single EU map for all offers of programs, courses, trainings	■		■	■		■		■		■
R2. Terminology: setup and adopt a standard cyber Education related lexicon		■			■					
R3. Culture: improving the cyber-aware attitude at all levels						■	■		■	■
R4. Target: expand the target audience of courses to non traditional categories						■		■	■	■
R5. Course Content: industry specific, soft skills included, hands-on approach				■	■	■		■		■
R6. Course Language: English as main language	■									
R7. Knowledge validation: from EU self assessment tool to Certification	■									
R8. European label for courses: endorsing courses based on specific criteria		■		■			■			
R9. Cybersecurity Insurance: considering the human factor	■									■
R10. Cybersecurity Skills preparedness Radar	■	■					■	■		
R11. Increase Opportunities for Women in Cyber	■							■	■	■

Figure 42: Mapping the Education related Challenges to the proposed Recommendations

The roadmap for Education and Skills along with the other chapter-roadmaps is currently the subject of a communication campaign. The Education is currently addressing only the cybersecurity professionals' segment.

In view of easing the interaction of the reader with the content, the T3.4 structured the content under a set of 10 main challenges and 11 main recommendations to address the identified challenges. An overview of the recommendations from their suggested initiators and the actors impacted is illustrated below. The figure also includes the proposed timeline for implementation of the recommendations.



Recommendations	Initiating actors						Direct relevance level					Implementation time		
	EU insitutions	Member states	Companies	Course providers	Certification bodies	Insurance companies	EU level	Member states	Companies	Course providers	individuals	Short term	Medium term	Long term
R1 - Mapping: one single EU map for all offers of programs, courses, trainings	🟦						🟨	🟨	🟨	🟨	🟨	🟩		
R2 - Terminology: setup and adopt a standard cyber Education related lexicon	🟦						🟨	🟨	🟨	🟨	🟨	🟩		
R3 – Culture: improving the cyber-aware attitude at all levels	🟦	🟦	🟦				🟨	🟨	🟨		🟨			🟩
R4 – Target: expand the target audience of courses to non traditional categories				🟦					🟨		🟨	🟩		
R5 – Course Content: industry specific, soft skills included, hands-on approach				🟦					🟨		🟨	🟩		
R6 – Course Language: English as main language				🟦			🟨		🟨		🟨			🟩
R7 – Knowledge validation: from EU self assessment tool to Certification	🟦				🟦		🟨	🟨	🟨	🟨	🟨	🟩		
R8 - European label for courses: endorsing courses based on specific criteria	🟦						🟨		🟨	🟨	🟨		🟩	
R9 – Cybersecurity Insurance: considering the human factor						🟦			🟨				🟩	
R10 - Cybersecurity Skills preparedness Radar	🟦						🟨	🟨		🟨	🟨	🟩		
R11 - Increase Opportunities for Women in Cyber	🟦	🟦	🟦	🟦			🟨	🟨	🟨		🟨	🟩		

Figure 43: Mapping of the Actors to be involved and those impacted by the proposed Recommendations

5.5 Outlook Y4

In Year 4 (2022) we will continue updating the courses map by (a) collecting the 2022 related dates for the already displayed courses and trainings, (b) adding new fields in the courses form related to the new role profiles and cybersecurity skills framework to be published by ENISA, and by (c) making available new content based on the submissions of the different European course providers and will promote them within the European cybersecurity ecosystem.

The feedback collected following the first public course will be used to further refine the content and Task 3.4 will re-run the course. Task 3.4 will continue running the C^3 by CONCORDIA Skills Certification for Cybersecurity Consultant in direct link to the deployment of the course targeting this profile.

The activities linked to the Teach-the-Teachers Action will continue to be implemented by continuing engaging with some stakeholders via interviews and events, and by developing and piloting specific methodology and associated materials for the teachers to use in their work of addressing cybersecurity-related matters with the high-school students.

The collaboration on CCN Education inter-pilots' group will continue on priorities set together with the members of the group, ENISA representative and ECSO representative.

The knowledge gained when developing the different activities under the T3.4 task, the interaction with the ecosystem representatives in different events and when collaborating with the other pilot projects set the basis for building the governance model for the education ecosystem to be delivered by the end of the project.

6. Conclusions and next steps

As a community building and sustainability activity, WP3 has fully met its objectives for Year 3 and proactively explored enhancements beyond the baseline activities as defined in the DoA. All WP3 activities are currently on track and all tasks have outlined their Y4 work. We are summarizing below the results achieved in Y3 and the way forward planned for Y4:

- T3.1 – After organizing the basic structure of the CONCORDIA Platform for Threat Intelligence and developing its core components, in year 3 we shifted the focus on the operationalization perspective developing key use cases (e.g., how is the CONCORDIA Platform for Threat Intelligence going to be used?) and drafting the “Code of Engagement”, namely a set of rules and guidelines driving the use of the CONCORDIA Platform for Threat Intelligence as well as its future developments. We plan to complete the work on the platform in year 4 by ensuring that all CONCORDIA partners can smoothly integrate T3.1 solutions with their own security toolchains and easily align their internal processes related to threat intelligence to the principles of the “Code of Engagement”.
- T3.2 - In Y3, Task 2 further developed the DDoS Clearing House components to achieve a stable version. We also developed a testbed for the Clearing House with which we can test the technical components. Lastly, we finished the technical preparations for the pilots in the Netherlands and Italy. In year 4 we plan to execute the two pilots, publish a “cookbook” with the lessons learned, and further mature the Clearing House components.
- T3.3 - In Year 3 we focused on collecting and updating virtual labs and started the exchange of scenarios between different Cyber Ranges based on the open-source KYPO Cyber Range platform exchange formats. In year 4 the open format for sharing training content for cyber ranges should be fully developed and successfully tested. The work on improving the virtual labs and related services (tool selection and use cases) will continue in Y4.
- T3.4 – In Y3, Task 3.4 launched the Courses map 2.0, ran two instances of the course “Becoming a Cybersecurity Consultant” and the associated C^3 by CONCORDIA certification exams. The work on the activity Teach-the-Teachers continued by collecting input via survey and interviews on the needs of high-school teachers and students in terms of content and format of materials to be used when teaching cybersecurity in school. The interaction with the Education ecosystem continued by participating in events, promoting content on social media and interacting with the CCN Education cross-pilot group. In Y4 we will (1) include new fields in the Courses map to align it to the ENISA skills framework, (2) further improve the content of the course and run additional 2 sessions followed by certification exams, (3) develop materials in support of high-school teachers addressing the challenges identified in Y3, and (4) propose guidelines and governance models for the European Education Ecosystem in Cybersecurity.

7. References

[Hout21] T. van den Hout, R. Poortinga-van Wijnen, C. Hesselman, C. Papachristos, K. Vink, "Developing and running a testbed for the DDoS Clearing House", blog, Oct 2021, https://www.sidnlabs.nl/en/news-and-blogs/developing-and-running-a-testbed-for-the-ddos-clearing-house

[Ceron21] J. Ceron, P. van Stam, G. Schaapman, and C. Hesselman, "New DDoS classifiers for the DDoS Clearing House", blog, April 2021, https://www.sidnlabs.nl/en/news-and-blogs/new-ddos-classifiers-for-the-ddos-clearing-house

[INRAD21] Innovation Radar, Secure Networks & Computing Innovation, "Distributed Denial of Service (DDOS) Clearing House", January 2021, https://www.innoradar.eu/innovation/37921

[DEMO21] "Demonstrating the DDoS Clearing House", video, Oct 2021, https://www.youtube.com/watch?v=UwRB74kabn8

[DOTS18] R. Dobbins, D. Migault, S. Fouant, R. Moskowitz, N. Teague, L. Xia, and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", Internet Draft, draft-ietf-dots-use-cases-16, July 2018, https://www.ietf.org/id/draft-ietf-dots-use-cases-16.txt

[Meng15] Meng, Y. Liu, J. Zhang, A. Pokluda, R. Boutaba, "Collaborative Security: A Survey and Taxonomy", ACM Computing Surveys, Vol. 48, Issue 1, September 2015, http://www.ntu.edu.sg/home/yangliu/csur.pdf

[Mirai17] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet", 26th USENIX Security Symposium, 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[DDOS13] Saman Taghavi Zargar, James Joshi en David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, Vol. 15, Issue 4, 4de kwartaal 2013

[BloSS19] Bruno Rodrigues and Burkhard Stiller, "Cooperative Signaling of DDoS Attacks in a Blockchain-based Network", SIGCOMM Posters and Demos '19: Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos August 2019, https://doi.org/10.1145/3342280.3342300

[D3.1] M. Caselli, C. Hesselman, R. Gloger, F. Cutas, and A. Pasic (editors), "Deliverable D3.1: 1st year report on community building and sustainability", December 2019

[HPING] https://tools.kali.org/information-gathering/hping3

[NMAP] https://nmap.org/

[DDOSIM] https://sourceforge.net/projects/ddosim/

[WODC19] J.M. Ceron, J.J. Chromik, J.J. Cardoso de Santanna, A. Pras, "Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands", Tech Report, University of Twente, June 2019

[ZDNET19] "This 5G ambulance could be the future of emergency healthcare", Nov 2019, https://www.zdnet.com/article/inside-the-5g-ambulance-that-could-let-doctors-treat-you-miles-from-the-hospital/

[DNADC] Homepage of the Dutch National Anti-DDoS Coalition, https://www.nomoreddos.org/en/

[DDoS18] C. Hesselman, J. van der Ham, R. van Rijswijk, J. Santanna, and A. Pras, "A Proactive and Collaborative DDoS Mitigation Strategy for the Dutch Critical Infrastructure", April 2018, https://www.sidnlabs.nl/en/news-and-blogs/a-proactive-and-collaborative-ddos-mitigation-strategy-for-the-dutch-critical-infrastructure

[DDoSCH20] C. Hesselman, R. Poortinga-van Wijnen, G. Schaapman, and R. Ruiter, "Increasing the Netherlands' DDoS resilience together", https://www.concordia-h2020.eu/blog-post/increasing-the-netherlands-ddos-resilience-together/

[eSilva19] K. e Silva, "Mitigating botnets: Regulatory solutions for industry intervention in large-scale cybercrime", Ph.D. thesis, Tilburg University, Dec 2019

[Conrads19] J. Conrads, "DDoS Attack Fingerprint Extraction Tool: Making a Flow-based Approach as Precise as a Packet-based", M.Sc. Thesis, University of Twente, Aug 2019

[CTIP20] M. Caselli, J. Ceron, C. Keil, J. Kohlrausch, and C. Hesselman, "Work in Progress: the CONCORDIA Platform for Threat Intelligence", https://www.concordia-h2020.eu/blog-post/a-concordia-platform-for-threat-intelligence/

[MANRS] [MANRS] Mutually Agreed Norms for Routing Security, https://www.manrs.org/ [Accessed: May 20, 2020]

[Keijzer20] Secretary of State Monica Keijzer, "Answers to questions by MP Weverling on DDoS attacks on Internet service providers" (in Dutch), Netherlands House of Parliament, October 2020, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D42266&did=2020D42266

[Hesselman20] C. Hesselman, M. Kaeo, L. Chapin, kc claffy, M. Seiden, D. McPherson, D. Piscitello, A. McConachie, T. April, J. Latour, and R. Rasmussen, "The DNS in IoT: Opportunities, Risks, and Challenges", IEEE Internet Computing, Vol. 24, No. 4, July-Aug 2020

[Tweakers20] "Large-scale ddos attacks on Dutch providers take place again", Tweakers, Sep 2020, https://tweakers.net/nieuws/171644/opnieuw-vinden-grootschalige-ddos-aanvallen-op-nederlandse-providers-plaats.html

[NOS18] "After banks now also Tax and Customs Administration and DigiD victim of DDoS attacks" (in Dutch), January 2018, https://nos.nl/artikel/2214339-na-banken-nu-ook-belastingdienst-en-digid-slachtoffer-ddos-aanvallen.html

[COVID] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld, and G. Smaragdakis, "The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic", ACM Internet Measurement Conference (IMC2020), Oct 2020

[Lima16] A. Lima, F. Rocha, M. Völp, P. Esteves-Veríssimo, "Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems", 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Oct 2016, Pages 59–70, https://doi.org/10.1145/2994487.2994489

8. Appendix T3.1: CONCORDIA Platform for Threat Intelligence Scope

As announced since the beginning of the project, "Threat Intelligence" is a topic of paramount importance within CONCORDIA. This aspect is not just present among the initial objectives, but it almost derives directly from the main purpose of the project. Specifically, if CONCORDIA sets its primary goal on building communities[1], we can say that all project's activities revolve around leveraging these communities to improve cybersecurity. In this regard, "Threat Intelligence" sharing represents a necessary step for communities to discuss today's digital threats and, its implementation (within the work of T3.1 and T3.2), represents a basic building block to face the aforementioned threats together and fight them collectively.

8.1. Platform Definitions and Scope

Before discussing the CONCORDIA Platform for Threat Intelligence, its scope and the elements defining its structure and boundaries, it is helpful to go back to the definition used by the project to describe Threat Intelligence.

According to Gartner[2], Threat Intelligence is:

> *"**Evidence-based knowledge**, including context, mechanisms, indicators, implications and actionable advice **about an existing or emerging menace** or hazard to assets that can be used **to inform decisions regarding the subject's response** to that menace or hazard."*

The previous definition focuses on three key aspects (in bold):

- The "evidence-based knowledge" part emphasizes the origin of threat intelligence information. This is often obtained from extended analysis and likely validated (e.g., in a testing environment). For this reason, CONCORDIA generally refers to Threat Intelligence as high-quality data assuming a process (e.g., incident investigation) behind its creation
- The phrase "about an existing or emerging menace" clarifies the meaning of the data. Threat Intelligence provides information either about concrete cyberattacks (e.g., already happened and recorded in the wild) or potential ones (e.g., plausible cyberattacks exploiting known vulnerabilities). For this reason, CONCORDIA assumes that Threat Intelligence is a piece of information (either technical, operational or strategical)[3] providing context to a given cyberattack
- Finally, the phrase "inform decisions regarding subjects' response" indicates that not every piece of information about cyberattacks should be considered "Threat Intelligence" by default, but only those that are useful to respond (or better prepare) against the related attacks. For this reason, CONCORDIA assumes that Threat Intelligence is "actionable" data, ready to be used to face or counteract a given threat.

[1] Objective #1: "CONCORDIA positions the CONCORDIA ecosystem, a Cybersecurity Competence Network with leading research, technology, industrial and public competences to build the European Secure, Resilient and Trusted Ecosystem (…)"

[2] https://www.gartner.com/en/documents/2487216

[3] https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/

With a definition of Threat Intelligence and a set of assumptions based on the aspects described above, we can think at a platform handling this information as a technological solution allowing partners to effectively share and manipulate data such that the assumptions hold. In other words, the CONCORDIA Platform for Threat Intelligence *creates a space where high-quality information about cyberattacks is stored as well as retrieved and leveraged by partners to improve their capability to respond or prepare against threats.*

The scope of the CONCORDIA Platform for Threat Intelligence conceivably extends to the limit of the previous definition and could potentially cover any type of high-quality information about cyberattacks as well as provide any kind of service capable of manipulating that information to make it "actionable" for a given partner. Concretely speaking, the set of possible information types and services has been defined by CONCORDIA relevant stakeholders and planned in relation to the timeframe and the priorities of the project. For this reason, the scope of the CONCORDIA Platform for Threat Intelligence corresponds today to the extent by which the platform is capable of operating from an "Architectural", "Technological", "Data" and "Operational" perspective.

What follows is an overview of these perspectives and a description of the properties and components that each perspective covers.

8.1.1 The "Architectural" Scope

The architectural scope represents the structure of the platform, its building blocks, and their relationships, internal as well as external, towards the rest of the "CONCORDIA Ecosystem". This scope also includes the possible ways in which the building blocks can communicate and, thus, the standards (e.g., languages, protocols, data formats) leveraged by each one of them to exchange information. This should not be confused with the employed technologies (covered in the "technological scope") where the focus stands on the actual instantiations and implementations and, thus, the libraries and tools used by the platform.

As introduced in Section 2.3, the CONCORDIA Platform for Threat Intelligence is inspired by the principles of microservice software architectures where single software components, each one responsible for a specific task, are deployed as separate units. This approach provides enhanced scalability and a high degree of decoupling within the platform.

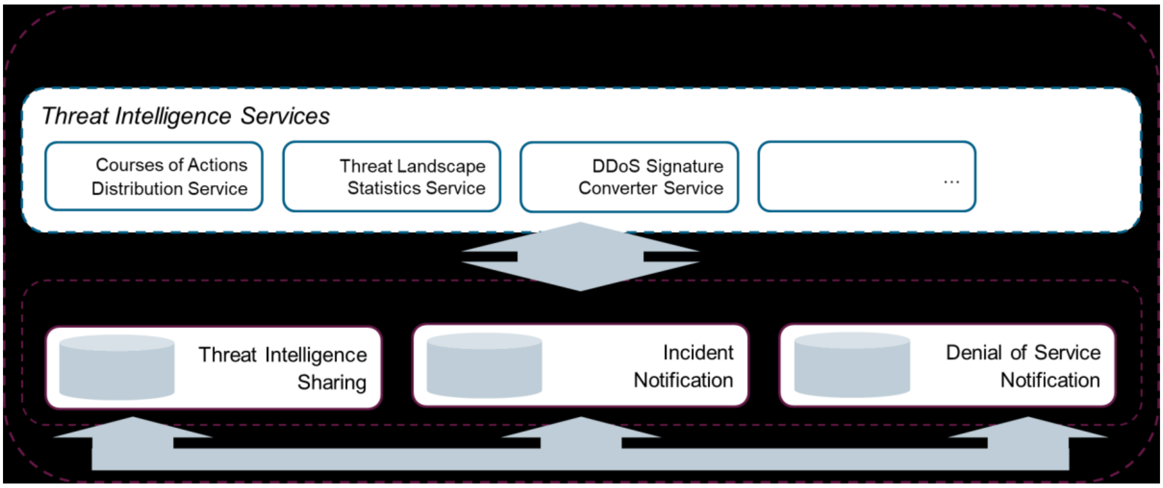

Threat Intelligence Services
Courses of Actions Distribution Service
Threat Landscape Statistics Service
DDoS Signature Converter Service
...
Threat Intelligence Sharing
Incident Notification
Denial of Service Notification

Figure 44: Platform Architectural Scope

As shown in Figure 44, in our case, the services or components, can be divided in two groups: the core components and the accessory ones. The **core components** represent the basic services provided by the platform and correspond to three objectives defined by Siemens, DFN-CERT and SIDN respectively at the beginning of the CONCORDIA project. The first aims at organizing and supporting the sharing of cybersecurity relevant information among CONCORDIA stakeholders. The second provides a way to register network resources and obtain early notification of any security-related activity associated to those resources. The third delivers mechanisms for analyzing Denial of Service attacks and deploying the related countermeasures.

The three core components exchange information with one another and support the execution of the **accessory components**, namely those services designed and developed within CONCORDIA to widen the set of features available in the CONCORDIA Platform for Threat Intelligence. The accessory components cover a broad spectrum of tasks handling sometimes very different types of information. Examples are: the *Course of Action Distribution Service* storing and organizing information related to incident response playbooks (e.g., list of actions to be performed to solve specific cybersecurity incidents), the *Threat Landscape Statistics Service* providing overviews and data about on-going or potential threats, the *DDoS Signature Converter Service* implementing the transformation of data about distributed denial of service attacks into intrusion detection signatures.

While, at the time of writing, just a few components have been developed and are currently under testing[1], CONCORDIA aims to further expand the collection of services aligning this Threat Intelligence Service Ecosystem to the main CONCORDIA Ecosystem outlined by project goal number one.

It is worth mentioning that the CONCORDIA Platform for Threat Intelligence, does not provide a unique access point to all these services. This design decision goes under the name of **virtual platform principle** stating the possibility of accessing each component independently from another. The virtual platform principle strongly influences the state of the platform as it affects both choices related to technologies and processes involved in its utilization (as described in the next two sections).

The interconnection among all components (core and accessory) implements the key idea of the CONCORDIA Platform for Threat Intelligence. Any service can be built on top of others and leverage already implemented platform features without "reinventing the wheel". However, this approach assumes the possibility of easily exchanging information across components. This assumption subsumes under the **compatible models and structures principle**. According to this principle, each component of the platform should explicitly expose information to the others in a conventional way. This translates in the use of well-known software architecture approaches (e.g., the presence of previously agreed APIs) and, especially, the use of widely adopted standards and data formats.

Among the most important standards and data formats included in the platform's architectural scope there are:

- STIX – The *Structured Threat Information eXpression* is a serialization language for cyber threat intelligence. Developed within OASIS, the standard is a machine-readable, semi-structured format based on JavaScript Object Notation (JSON). STIX provides a taxonomy revolving around two main concepts: Domain Objects

[1] A description of those components and their current status can be found in Sections 2 and 3.

(SDOs) describing characteristics of a cybersecurity piece of information and Relationship Objects (SROs) describing the relationships among those characteristics.

- MISP Format – Beyond the tool itself, MISP provides a set of data models mostly defined by its community. On top of the core format, based on JSON, these data models allow to exchange a huge variety of events and attributes in a standardized manner.[1] Events and attributes can also be further enriched by the so-called complex objects (new attributes defined outside the standard set delivered by MISP) and galaxies (custom taxonomies and ontologies integrating the information provided by each MISP event).
- ACDC Data Formats – As part of the original development of the Incident Clearing House in the ACDC[2] project, a set of JSON-based data formats and workflows was defined that govern the interaction with the Incident Clearing House[3]. The data formats define the scope of data that can be submitted and received from the Incident Clearing House.
- OpenC2 – the *Open Command and Control* standard aims at formalizing representations of command and control (actions) mechanisms for cyber defense systems. The non-proprietary format is used for security orchestration and automation independently from the underlying technologies by using function-centric interfaces.
- CACAO – The *Collaborative Automated Course of Action Operations* is the first format trying to standardize generic incident response procedures. Introduced within IETF and, later, developed within OASIS, the CACAO standard focuses on "courses of actions" objects (e.g., actions to be taken to resolve a particular cybersecurity issue) and define ways to interconnect those courses of actions thanks to a well-defined procedural logic. The main objectives of the format are incident response automation and inter-organizational sharing of incident handling playbooks.
- XARF – the *eXtended Abuse Reporting Format*, is a standardized set of schemas originally designed and developed by Abusix for describing abusive behavior or abusive content. Designed to be shared via email, the overall objective of XARF is to improve the ability of recipients of abuse reports to operationalize the data paving the way to improved and automated incident response.

8.1.2 The "Technological" Scope

While the "Architectural" scope outlines the roles and functions of all building blocks of the CONCORDIA Platform for Threat Intelligence, the "Technological" one focuses on the related implementation choices. In this regard, this section describes the set of technologies used within the platform as well as the actual data those technologies are able to store, analyze and exchange.

Due to their central role within the foreseen ecosystem of threat intelligence services, the core components have been defining and driving the set of technologies used within the

[1] At the time of writing, the number of different MISP types is 567 (https://www.misp-project.org/datamodels/)

[2] https://www.acdc-project.eu/

[3] http://acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.7.2_Data_Format.pdf

platform since the beginning of the project. For this reason, in what follows, we provide a "per-component" overview of the employed tools and solutions.

Threat Intelligence Sharing Service

The threat intelligence sharing service is implemented by MISP and a collection of tools exchanging information with it. As shown in Figure 45, MISP leverages different open-source technologies arranged in a hierarchical structure.

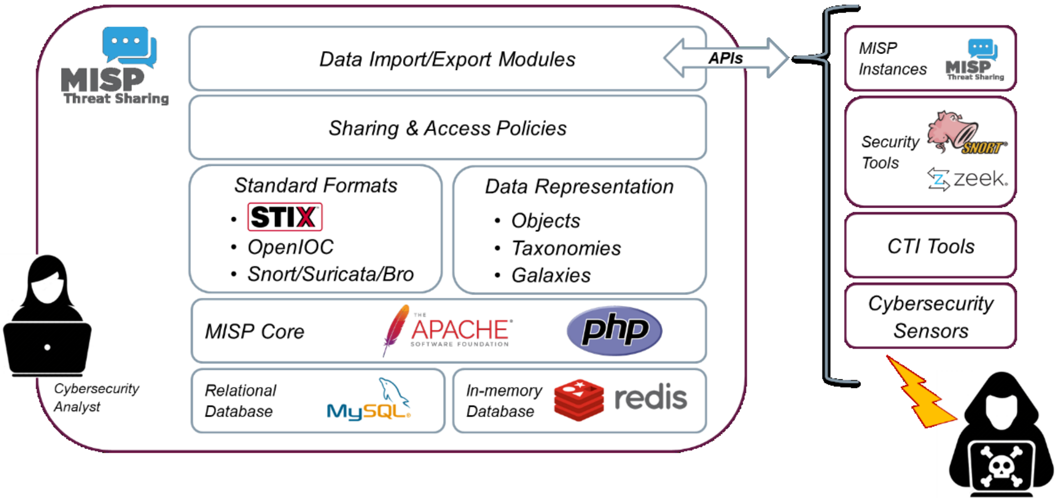


Figure 45: Threat Intelligence Sharing Service

At the base, the tools responsible for storing and organizing threat intelligence data are well-known and widely-used database management systems (DBMS):

- *MySQL*[1] is an open-source relational DBMS created and maintained by Oracle Corporation. Developed to conform as closely as possible to the ANSI SQL and ODBC SQL standards, MySQL has stand-alone clients that allow users to interact with the database. However, as in the case of MISP, MySQL is often employed directly within other tools basically implementing their relational database capabilities and features.
- *Redis*[2] (*REmote DIctionary Serve*r) is an open source, in-memory "key-value" data structure store commonly either as standalone database solution or as cache and message broker. Originally developed as a VMWare-spin-off, Redis is, nowadays, the most popular key-value database.

In the same way, also the MISP core elements develop around notorious technologies employed today in numerous applications:

- The *Apache HTTP Server*[3], or more commonly *Apache*, is the name of a free web server developed by the Apache Software Foundation. It is considered the most popular modular web server platform in the world and can operate on a great variety of operating systems. Apache can count on a development history of nearly 30 years and a very large community of developers with continuous updates both in terms of new features and security patches.

[1] https://www.mysql.com/
[2] https://redis.io/
[3] https://httpd.apache.org/

- *PHP*[1] is a general-purpose scripting language commonly used for web development and employed to implement the majority of modules and features in MISP around the aforementioned Apache HTTP Server.

Outside MISP, the set of solutions employed within the CONCORDIA Platform of Threat Intelligence (as well as locally on partners' premises) to leverage (e.g., analyze, transform, etc.) MISP data includes again a huge variety of tools. Above all, intrusion detection systems represent the best example of solutions making the threat intelligence information stored in MISP "actionable" (e.g., transforming the raw data about cyberattacks into actual detection rules). In this regard, the most used technologies are:

- *Snort*[2] – an open-source IDS/IPS developed by Martin Roesch in 1998. Widely known to the open-source community, the tool runs on Linux, BSD, MacOSX and Windows and is used today by hundreds of thousands of users around the world, including private and commercial consumers. Snort performs two main activities: packet logging and real-time traffic analysis. While the first simply relates to the capability of storing and later loading network packets, the second focuses on a flexible and powerful processing language to define rules and thus monitor and alert events observed in an IP network.
- *Zeek*[3] (formerly known as *Bro*) – a network traffic analyzer employed in different domains such as security monitoring and performance measurement. Developed by Vern Paxson in 1997 at the University of California Berkeley, Zeek gained traction over the years becoming one of the most popular open-source tools in the security community and an actual product in 2013 under the name of Corelight. The tool builds upon the concepts of efficiency, flexibility and adaptability. First, Zeek targets high-performance networks and has been extensively tested for monitoring large sites (e.g., entire corporate networks). Second, this efficiency does not diminish the variety of use cases to which Zeek can apply. For example, the tool can work with different intrusion detection approaches (e.g., anomaly-based, specification-based) and does not necessarily rely on signatures. Finally, adaptability is the most relevant characteristic. Zeek provides a Turing-complete scripting language that allows users to choose, select and analyze any network event of their choice (e.g., connection establishments, specific network packets, files).

Incident Notification Service

The incident notification service is carried out by the Incident Clearing House (ICH). As for the threat intelligence sharing, also in this case, several technologies contribute to the implementation of the different features. Figure 46 shows an overview of the related infrastructure and its key elements.

[1] https://www.php.net/
[2] https://www.snort.org/
[3] https://zeek.org/

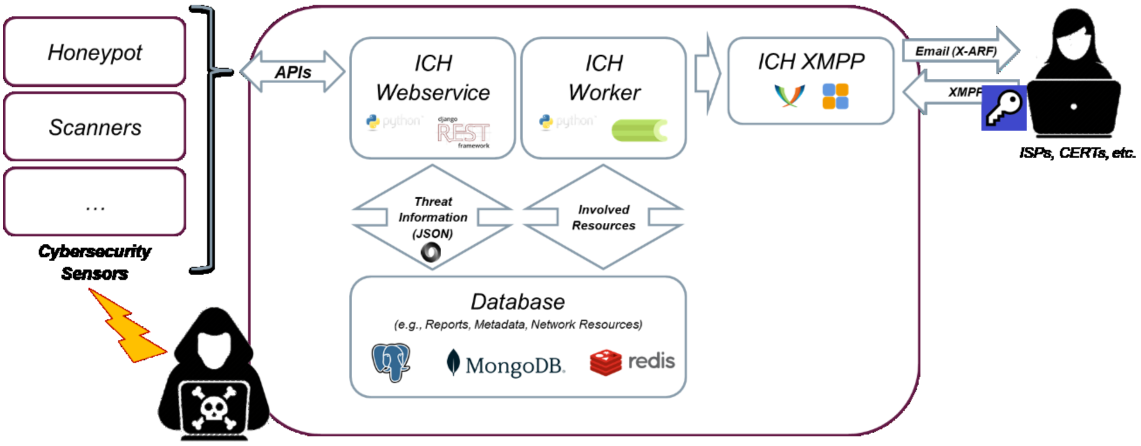


Figure 46: Incident Notification Service

The storing capabilities of the Incident Clearing House are built on top of three database solutions. Besides Redis (already discussed in the previous sub-section), those are:

- *PostgreSQL*[1] – an object-relational DBMS released under a free license. As for MySQL, PostgreSQL uses the SQL language to query for data. These are stored as a series of tables with external keys serving as "links" among related data. The main strength of PostgreSQL is its "programmability", making it well-suited to build applications for the real world.
- *MongoDB*[2] – a non-relational, document-oriented DBMS. The approach used by MongoDB replaces the concept of tables employed in relational databases with JSON-style documents. These documents are based on a dynamic schema (BSON format) whose adoption makes the data integration of a variety of applications easier and faster.

The core web service exposed by the Incident Clearing House uses in turn the following technologies:

- *Django REST Framework*[3] is a toolkit for building Web APIs. Developed according to the "Model-Template-View" paradigm, the framework provides a number of features that facilitate the rapid development of web content management applications. Among these, we find the abstraction of the "object relational database", the possibility to add "generic views" (avoiding the repetitive drafting of code for common cases), and the capability of installing new functionalities through "plugins".
- *Celery*[4] is a simple and flexible task queue solution providing real-time data processing. In the context of web application, Celery is used to implement asynchronous task (or job) queues based on distributed message passing.
- *XMPP*[5] represents the set of instant messaging protocols developed by the XMPP Standards Foundation. Based on XML, this technology allows for near-real-time exchanges of structured data between network entities and is designed to be extensible beyond its original goal solely based on instant messaging. Examples of

[1] https://www.postgresql.org/
[2] https://www.mongodb.com/
[3] https://www.django-rest-framework.org/
[4] https://docs.celeryproject.org/en/stable/getting-started/introduction.html
[5] https://xmpp.org/

these extensions are Voice over Internet Protocol (VoIP) applications and file transfers.

- *Prosody*[1] is a cross-platform XMPP server. Easy to set up and configure, the software focuses on an efficient use of system resources and provides a powerful and flexible support to the development of web functionalities.
- *Python*[2] is an interpreted high-level general-purpose programming language widely employed nowadays for a number of different applications and use cases (e.g., machine learning, distributed software, etc.). Python is considered a multi-paradigm language as it supports object-oriented programming, structured programming, and many functional and reflection programming features. Simplicity and flexibility are among Python's key characteristics (also in comparison with other major programming languages).

Denial of Service Notification Service

The denial of service (DoS) notification service is implemented by the DDoS Clearing House (DDoS-CH). As for the other two core components, the DDoS-CH includes several different open-source technologies as well as custom solutions developed within the CONCORDIA project. Figure 47 depicts a high-level overview of the related building blocks.

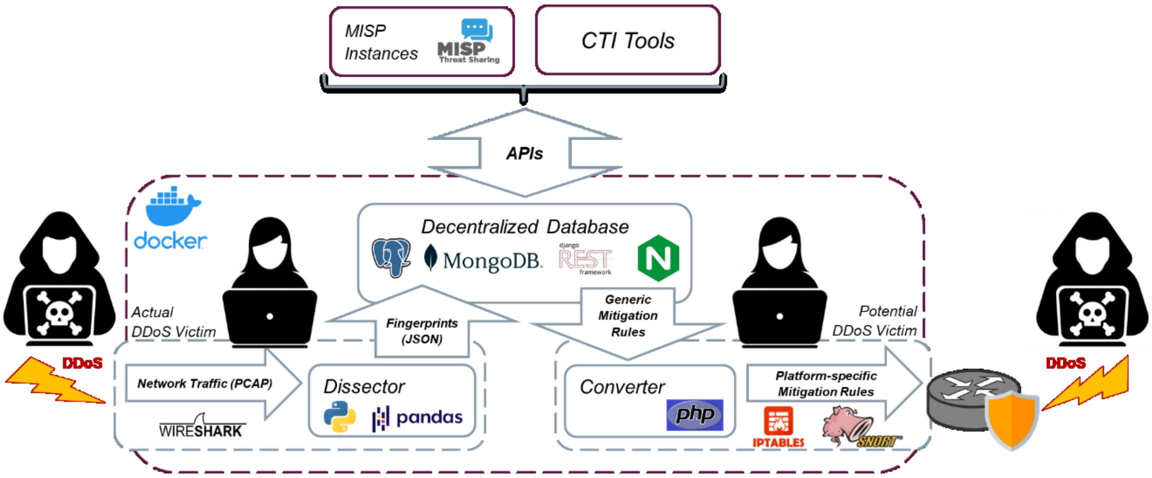


Figure 47: Denial of Service (DoS) Notification Service

The decentralized database leverages a heterogeneous set of applications and DBMS solutions. Beyond PostgreSQL, MongoDB and the Django REST Framework (described in the previous sub-section), we find:

- *NGINX*[3] – a lightweight and high-performance web server, commonly used as a reverse proxy, load balancer, HTTP cache and email proxy. Designed to handle heavy workloads, it focuses on efficient memory usage at the expense of a limited flexibility (compared to other web server technologies such as Apache).

Core elements of the DDoS-CH use, again, common programming languages such as Python and PHP but integrate specific libraries and tools, such as:

[1] https://prosody.im/
[2] https://www.python.org/
[3] https://www.nginx.com/

- *Pandas*[1] – an open-source data analysis and manipulation tool, built on top of the Python programming language. Pandas is flexible and provides several features among which data structures and operations for manipulating numeric tables and time series.
- *Tshark*[2] – a widely-known software for network protocol analysis. Its use spans from network troubleshooting, to pentesting, to the analysis and development of protocols and communication software. Its functionality is quite similar to other applications (e.g., tcpdump), but the tool comes also with a graphical interface (*Wireshark*) and extra sorting and filtering capabilities.
- *IPTables*[3] – a tool that allows flexible configuration of IP packet filter rules of the Linux kernel firewall. Iptables operates by comparing network traffic against the given set of rules. Each rule defines what characteristics a network packet should have to match the rule, and the action that should be executed for the packets that match.

Finally, many technologies of the DDoS-CH are executed within *Docker* containers to ensure consistent and isolated environments.

8.1.3 The "Data" Scope

Intrinsically related to the "technological" scope, the "data" scope delineates the set of data types handled by the technologies employed in the CONCORDIA Platform for Threat Intelligence. These data types represent the extent of the platform's semantic power and allow to share a common language across all platform's users.

One important aspect of the "data" scope relates to the extension of its borders. Most of the technologies mentioned in the previous chapter come with a standard set of supported data types. Nonetheless, the same technologies often include mechanisms to extend these data types in order to express new concepts (or better shape the established ones). This fact makes the borders of the "data" scope prone to change depending on how the related technology is used.

In what follows, we discuss the "data" scope in regards to the standard data types. Again, we find it convenient to divide the section according to the "core" components.

Threat Intelligence Sharing Service

As mentioned in section 8.1.1, the MISP format is prominently used to share information across partners. Over the years, the format has standardized around a fixed set of attribute types as well as an open-source library of objects (maintained by CIRCL but continuously updated and refined by the entire MISP community) .

Table 6 collects all MISP attribute types. Each type belongs to one (or multiple) MISP categories which define a semantic context where the attribute type assumes a given meaning. The categories are:

[1] https://pandas.pydata.org/

[2] https://www.wireshark.org/

[3] https://www.netfilter.org/

- **Antivirus detection:** Information related to a malware identified by a given antivirus product
- **Artifacts dropped:** Information about an artifact created by a malicious program (e.g., a malware)
- **Attribution:** Information about a threat actor
- **External analysis:** Information about an attack analysis (e.g., malware forensics)
- **Financial fraud:** Information related to a financial fraud
- **Internal reference:** Information used to reference a given MISP event at the publisher side
- **Network activity:** Information about the network traffic generated by the attacker
- **Other:** Any information not matching a specific category
- **Payload delivery:** Information about how an attacker delivers data to the target system
- **Payload installation:** Information about how an attacker might install malicious code on the target system
- **Payload type:** Information about the malicious code residing in the target machine
- **Persistence mechanism:** Information about how the attacker maintains presence on the target machine
- **Person:** Information about a physical person
- **Social network:** Information about social networks involved in the attack
- **Support tool:** Information about the tools used to detect, mitigate or respond to an attack
- **Targeting data:** Information about the target system and the related data content

Table 6: MISP Attribute Types

AS	email	filename|sha512	ja3-fingerprint-md5	place-of-birth	target-location
aba-rtn	email-attachment	filename|sha512/224	jabber-id	place-port-of-clearance	target-machine
anonymised	email-body	filename|sha512/256	jarm-fingerprint	place-port-of-onward-foreign-destination	target-org
attachment	email-dst	filename|ssdeep	kusto-query	place-port-of-original-embarkation	target-user
authentihash	email-dst-display-name	filename|tlsh	last-name	port	telfhash
bank-account-nr	email-header	filename|vhash	link	primary-residence	text
bic	email-message-id	first-name	mac-address	process-state	threat-actor
bin	email-mime-boundary	float	mac-eui-64	prtn	tlsh
boolean	email-reply-to	frequent-flyer-number	malware-sample	redress-number	travel-details
bro	email-src	full-name	malware-type	regkey	twitter-id
btc	email-src-display-name	gender	md5	regkey|value	uri
campaign-id	email-subject	gene	middle-name	sha1	url
campaign-name	email-thread-index	git-commit-id	mime-type	sha224	user-agent
cc-number	email-x-mailer	github-organisation	mobile-application-id	sha256	vhash
cdhash	eppn	github-repository	mutex	sha3-224	visa-number

chrome-extension-id	favicon-mmh3	github-username	named pipe	sha3-256	vulnerability
comment	filename	hassh-md5	nationality	sha3-384	weakness
community-id	filename-pattern	hasshserver-md5	other	sha3-512	whois-creation-date
cookie	filename|authentihash	hex	passenger-name-record-locator-number	sha384	whois-registrant-email
cortex	filename|impfuzzy	hostname	passport-country	sha512	whois-registrant-name
counter	filename|imphash	hostname|port	passport-expiration	sha512/224	whois-registrant-org
country-of-residence	filename|md5	http-method	passport-number	sha512/256	whois-registrant-phone
cpe	filename|pehash	iban	pattern-in-file	sigma	whois-registrar
dash	filename|sha1	identity-card-number	pattern-in-memory	size-in-bytes	windows-scheduled-task
date-of-birth	filename|sha224	impfuzzy	pattern-in-traffic	snort	windows-service-displayname
datetime	filename|sha256	imphash	payment-details	special-service-request	windows-service-name
dkim	filename|sha3-224	ip-dst	pdb	ssdeep	x509-fingerprint-md5
dkim-signature	filename|sha3-256	ip-dst|port	pehash	ssh-fingerprint	x509-fingerprint-sha1
dns-soa-email	filename|sha3-384	ip-src	pgp-private-key	stix2-pattern	x509-fingerprint-sha256
domain	filename|sha3-512	ip-src|port	pgp-public-key	target-email	xmr
domain|ip	filename|sha384	issue-date-of-the-visa	phone-number	target-external	yara
					zeek

All MISP attributes can be combined to form more complex objects and, thus, widen the "data" scope. These objects deepen the descriptions of information in several contexts, from specific tools (e.g., Splunk), to special topics (e.g., facial recognition). An updated list of objects is maintained on the MISP official website[1].

Finally, MISP allows users to further enrich the description of events (and even specific attributes) with taxonomies and "Galaxies". These features are commonly represented in the form of labels (or "tags") and used to classify information within pre-defined categories. Important examples of these taxonomies and "Galaxies" are the Traffic Light Protocol (TLP) and the ATT&CK framework. Also in this case, the related lists of available taxonomies and "Galaxies" are available on the MISP official website[2].

Incident Notification Service

To represent the submitted information, the ICH uses the previously mentioned ACDC Data Format that specifies the scope of information that can be shared over the service. This data format specifies the different types of information – called "reports" in the ICH – that can be shared as well as their attributes and possible relations between them. The complete set of supported report types and subtypes can be seen in Figure 48. The details including report attributes, attribute formats and schemata to verify reports can be found in the complete specification[3].

[1] https://www.misp-project.org/objects.html

[2] https://www.misp-project.org/taxonomies.html

[3] http://acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.7.2_Data_Format.pdf

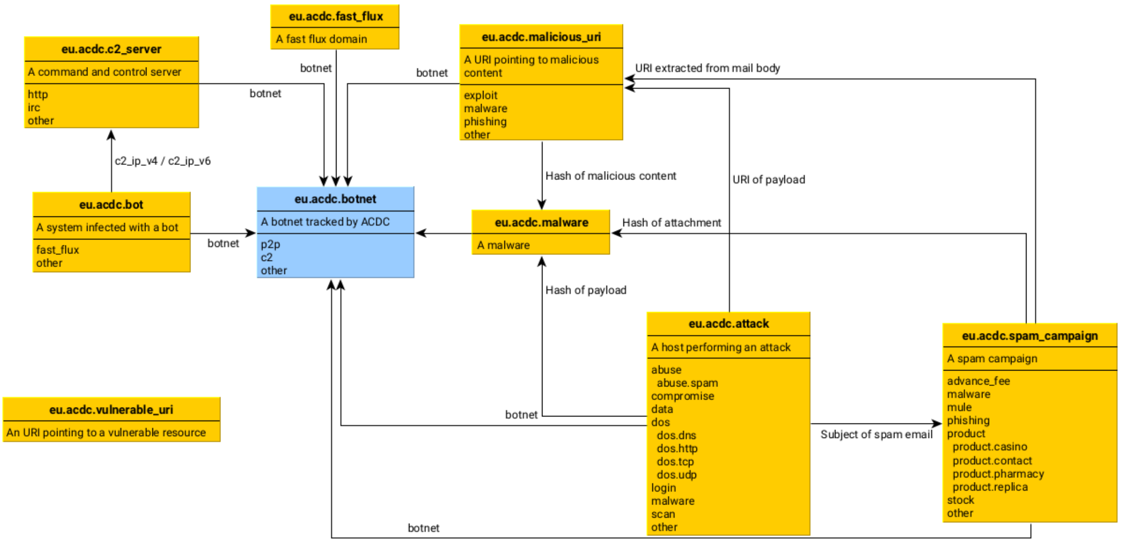


Figure 48: Report types in the Incident Clearing House

Denial of Service Notification Service

The DDoS-CH uses a custom JSON schema to capture all information related to denial of service attacks. The schema has been tailored to the implemented mechanisms for extracting data from PCAP and FLOW files (captured during an attack) as well as to the likely tools to use in order to later detect or stop the same attack (e.g., firewalls or intrusion detection systems).

The JSON schema always includes the following information to outline the basic attributes of each given attack: *"start_time"*, *"duration_sec"*, *"total_dst_ports"*, *"avg_bps"*, *"total_packets"*, *"ddos_attack_key"*, *"key"*, *"total_ips"*, *"tags"*. Additionally, the actual information used to represent the key indicators of compromise might vary depending on the kind of denial of service attack.

The following two tables include all possible indicators of compromise:

Table 7: DDoS-CH Attributes (PCAP file)

Attributes	**Protocol**
DNS query name	DNS
DNS query type	DNS
Ethernet Type	Ethernet
Ethernet Frame Length	Ethernet
HTTP Request	HTTP
HTTP Response	HTTP
HTTP User Agent	HTTP
ICMP type	ICMP
ICMP code	ICMP
IP destination	IP
IP Flags	IP

IP Fragmentation offset	IP
IP proto	IP
IP source	IP
IP TTL	IP
NTP priv reqcode	NTP
TCP destination port	TCP
TCP destination port	TCP
TCP flags	TCP
TCP source port	TCP
UDP destination port	UDP
UDP Length	UDP
UDP source port	UDP

Table 8: DDoS-CH Attributes (FLOW file)

Attributes	**Protocols**
ICMP code	ICMP
ICMP type	ICMP
In bytes	IP
In packets	IP
IP destination	IP
IP proto	IP
IP source	IP
IP TTL	IP
TCP destination port	TCP
TCP flags	TCP
TCP source port	TCP
TCP Type of Service	TCP
UDP destination port	UDP
UDP source port	UDP

An updated version of the tables is also available on Github[1].

8.1.4 The "Operational" Scope

The "operational" scope represents the set of mandates and processes regulating the access to the CONCORDIA Platform of Threat Intelligence as well as its collaborative usage. This scope goes beyond the technical aspects and is in-place not just as an additional description of the platform but as a guarantee for the CONCORDIA partners of knowing and understanding what happens when they use it. A major example of this guarantee relates to data. Before pushing threat intelligence to the platform, each partner should be informed about possible requirements and constraints (e.g., each piece of information should come from a reliable source and not exceed a certain size) but also aware about what happens after data are ingested (e.g., the threat intelligence will be stored at a given location and might be processed by other partners).

[1] https://github.com/ddos-clearing-house/ddos_dissector

The different aspects of the "operational scope" are planned to be publicly available to all partners and CONCORDIA stakeholders in the so-called **"Code of Engagement"**. The "Code of Engagement" (CoE) represents a set of rules and conventions each user of the CONCORDIA Platform for Threat Intelligence agrees on before accessing and using the related services. Differently from a standard contract, the Code of Engagement is not a typical multi-lateral agreement but allows instead for more flexible extensions. These extensions do not encompass only possible new participants but also include the presence of new rules as well as new services available in the platform. The flexibility of the Code of Engagement was a condition outlined by several internal discussions and stemming by the context in which the CONCORDIA project developed over the years. With the continuous acquisition of new partners and the numerous requests for external collaborations, the work on the CONCORDIA Platform for Threat Intelligence has faced the challenge of ensuring quality of services (e.g., secure access to the stored information) to an increasingly heterogenous audience of interested parties. With the parallel development of new components as well as the integration of contributions coming from the different partners, the idea of a rigid contract was not feasible. For this reason, the suggestion from the legal experts available within CONCORDIA, namely Arthur's Legal, brought to the development of a new kind of legal agreement later summarized in the Code of Engagement. The presence of this document implements the third and last principle at the foundation of the CONCORDIA Platform for Threat Intelligence. The **uniform engagement rule principle** was introduced to ensure that the platform was not solely a technological solution but comprehensively described all interactions performed by CONCORDIA partners and stakeholders. The Code of Engagement comprehensively describes that and provides extra context and valuable information.

The Code of Engagement[1]

The content of the Code of Engagement could be essentially divided into two parts. The first one includes information about the goals of the CONCORDIA Platform for Threat Intelligence as well as the key values and benefits. As already mentioned, the goal of the platform was, since the beginning, to *build one central point of contact for all services related to threat intelligence*. More precisely, the Code of Engagement refers to all stakeholders leveraging the platform as a community that "actively participates, connects with other professionals, contributes, obtains and otherwise shares certain relevant trusted threat intelligence, and otherwise collaborates, engages, tests, tries, iterates, calibrates, matures, mitigates risks, optimizes results and succeeds". The key values and benefits are also described in detail and divided among the platform's core components. Among the most important we found:

- The crucial advantage of sharing actionable information about attackers' offensive behaviors and preferred methods
- The importance of providing users with actionable data on malicious network activity via a distribution platform with access to numerous network resource owners
- The emphasis of collaboratively and proactively combating Distributed Denial of Service attacks

[1] The complete draft of the Code of Engagement will be published within D4.3. By the end of the CONCORDIA project, the final version will also be available on the CONCORDIA website at https://www.concordia-h2020.eu/liaison-between-threat-intelligence-platform-and-ddos-clearing-house-tasks/

Furthermore, some benefit related to the technological choices made in the project are also made explicit. For example, in the case of MISP, the Code of Engagement informs all stakeholders about its "extensive durability due to structured, modular architectures and by-design approach in accordance with the most demanding regulatory frameworks and industry standards, and due to the community support and its world-wide adoption."

The second part of the Code of Engagement discusses the management of the platform and the process of "decision making". Furthermore, it gives information on how the Code of Engagement itself should be amended and, thus, reflect any update on the CONCORDIA Platform for Threat Intelligence or its members. First and foremost, the Code of Engagement defines a "Platform Steering Committee" responsible of governing the platform and approve any change. This committee will also be responsible for resolving disputes and, ultimately, approve a new member joining or leaving the community (upon suggestion of the community itself). The action of the committee is in turn governed by EU laws and obligations (e.g., GDPR) and conforms to its jurisdiction (unless otherwise specified).

In regard to "decision making", the Code of Engagement, emphasizes once more the "virtual nature" of the platform and, thus, the capability of its core components to also act as independent entities. This translates, for example, in the possibility of updating a core component by simply notifying the partners and stakeholders registered for that component (without necessarily wait for the approval of the entire community). Differently, changes having a comprehensive impact on the platform (e.g., strategic, material governance, legal terms, etc.) would instead require the involvement of all members.

Finally, management includes requirements and constraints in the members' capabilities to operate with the CONCORDIA Platform for Threat Intelligence. For example, each member would be responsible for any content contributed or otherwise made available in the platform. Furthermore, all members will be responsible of the security of the platform to the extent that they contribute to its operations. This translates to specific indications such as having, monitoring, maintaining, and keeping up-to-date appropriate technical and organizational measures.

8.2. Connection to CONCORDIA's Cybersecurity Roadmap for Europe

The Platform for Threat Intelligence provides a diverse set of services in an extendable ecosystem. The services cover aspects such as understanding potential threats, protecting against threats, learning about problems in your infrastructure, and eradicating problems in your infrastructure. This broad positioning provides multiple connections to support the challenges identified in CONCORDIA's Cybersecurity Roadmap for Europe[1].

8.2.1. Threat Landscape

The platform provides a complementary view to the Threat Landscape detailed in the Cybersecurity Roadmap. While the latter stems from an analysis of known current and emerging threats, the platform provides a view on observed threats and their prevalence. When combined, this can be a valuable addition to evaluate the individual risk. However, care has to be taken in the interpretation as the data in the platform is, like all collections

[1] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/CONCORDIA_Roadmap.pdf

of data, not free of bias. Some of the threats in the Threat Landscape are not amenable to a collection of data that is typically shared in these kinds of platforms. This includes threats from the legal or organizational threat groups. For other threat groups, data might not be included in the platform because there is no corresponding data source feeding the platform. This may be due to the source simply not being connected to the platform, or the source not sharing the information due to technical, organizational or legal constraints.

8.2.2. Roadmap for Research and Innovation

The DDoS Clearing House is directly connected to the **DDoS Protection Services** challenge in the network layer of the roadmap as it puts its participants in the position to detect and protect against identified attacks. The whole platform is also relevant for the **Monitoring and Data Collection Infrastructure** challenge in the same layer as it provides data to understand and contextualize current and emerging threats. This can be used to complement other internal and external sources of information.

Especially MISP is relevant to the **Malware Detection and Analysis challenge** of the System layer. MISP was originally developed as a Malware Information Sharing Platform and thus provides a valuable source of malware information.

The platform can be used to support the **Fighting Disinformation in Europe** challenge of the User layer by enabling the quick distribution of relevant information to stakeholders. This is exemplified by the MISP project setting up a dedicated instance to fight COVID-related threats and disinformation[1].

8.2.3. Roadmap for Economics

Determining the risk a system is exposed to, as identified by the **Security Analysis and Risk Analysis** challenge, can be informed by different services of the platform. In particular, MISP can be used to share different aspects of current and emerging threats that a system might face. The Security Metrics can provide context on the prevalence of certain attacks informing the evaluation of the likelihood. The DDoS Clearing House collects fingerprints of attacks that anti-DDoS coalition members have handled in the past. Finally, the Incident Clearing House can be used to notify participants of vulnerable systems in their infrastructure as identified by external scanning. This can augment the identified attack surface of systems under consideration.

8.2.4. Roadmap for Legal and Policy

While the challenges identified in the legal and policy domain can only be fully addressed on that level, the platform can support the objective of **Trusted Experience Sharing** by providing a tool for sharing that can be extended to address certain properties of trust. The Code of Engagement for the Threat Intelligence Platform is in itself a building block to increase trust in the sharing process by defining a clear and reliable framework for sharing data over the platform. The DDoS Clearing House on its own also requires a legal and policy framework for instance based on the Code of Engagement. The members of the Dutch anti-DDoS coalition have set up a consortium agreement that has a similar purpose.

[1] https://www.misp-project.org/covid-19-misp/

This approach can be augmented by further measures. The Incident Clearing House, for example, uses stakeholder specific trust anchors to govern the registration of new members and their network resources. This ensures parties submitting data that only the proper contacts receive it. For CSIRTs this role is fulfilled by the Trusted Introducer Service[1] by the TF-CSIRT[2] task force of the European GÉANT project.

8.2.5. Community Building

Although being a minor part in the Know (Your Enemy and Know) Yourself objective, the platform can be used as a source of information on malicious actors and their modes of operation.

[1] https://www.trusted-introducer.org/

[2] https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx

9. Appendix T3.2: DDoS Clearing House Dissector deployment model

DDoS Dissector deployment specifics

Authors: João Ceron (previously SIDN Labs), Cristian Hesselman (SIDN Labs) and Thijs van den Hout (SIDN Labs)

Version November 3, 2021

The goal of this working document is to create instructions for how Members of the Dutch Anti-DDoS Coalition can analyze their DDoS traffic with the Dissector. This insight will (1) help us at SIDN Labs understand how to package the Dissector for easy use and (2) to develop a Best Common Operation Practice (BCOP) for Members to use the DDoS Dissector and upload fingerprints to DDoSDB. We first discuss the Dissector's generic deployment model and its key operational properties and requirements. Next, we enable Coalition Members to add details about how they expect to obtain DDoS traffic samples in their specific network setup, for use by the Dissector.

Generic Deployment Model of the Dissector

The Dissector is one of the core software components of the DDoS Clearing House, together with the DDoS-DB and the Converter. The Dissector is responsible for determining the characteristics of a DDoS attack that hits a Coalition Member and for summarizing it in a textual description called a "DDoS fingerprint". The software is open-source and publicly available on Github[1]. A more detailed discussion on the functions of the DDoS Clearing House is available on the website of the Dutch anti-DDoS coalition[2].

Figure 49 shows the Dissector's generic deployment model.

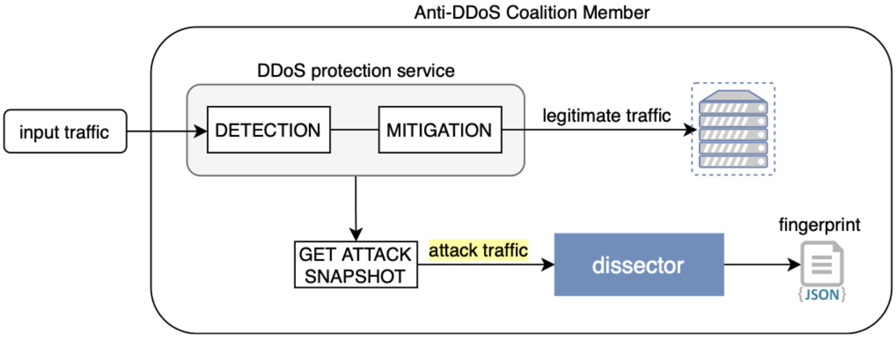


Figure 49: Dissector generic deployment model

The top part of Figure A shows the live traffic flow of a Coalition Member, which usually passes incoming attack traffic through a DDoS Protection Service, which detects and mitigates the attack. The mitigation service can be a set of onsite appliances, a cloud service, or a combination thereof. Potential DDoS victims will often first use their local

[1] https://github.com/ddos-clearing-house

[2] https://www.nomoreddos.org/en/increasing-the-netherlands-ddos-resilience-together/

appliance to filter out the DDoS traffic and if that doesn't work, send the traffic to a cloud provider they work with (e.g., Arbor). Other Coalition Members may only rely on on-site mitigation systems, as is the case for the NaWas[1]or example. The detection system is an on-site facility and is responsible for detection attacks., for example. The detection system is an on-site facility and is responsible for detection attacks., for example. The detection system is an on-site facility and is responsible for detection attacks.

The bottom part of Figure 1 shows the use of the Dissector. As shown, the Dissector is **not applied in-line with the incoming traffic**. It is a stand-alone program that **does not need to be integrated in the network**. The only requirement to run the Dissector is a network traffic sample of the DDoS attack. Members can get the traffic in different ways, such as through a network TAP (Traffic Access Point), a port mirror for traffic redirection, or by getting the DDoS traffic from their mitigation provider. Members can process the traffic using tools such as *tcpdump* and *nfdump* to get chunks of traffic limited and provide them to the Dissector. In general, sample files of around 100 Mbytes enable the Dissector to produce an accurate fingerprint of the DDoS attack. Members only need to have access to such a traffic sample (e.g. PCAP) to use the Dissector. Therefore, the Dissector doesn't have to be on-premises; it might just as well be called from a laptop at home, as long as the network traffic capture sample of the DDoS attack is available.

The Dissector is an off-path application with a single task

We specifically designed the Dissector to process DDoS attacks **off-path** and to carry out that task locally, so no traffic captures need to be uploaded to the internet. This means the network flow of an organization is never intercepted or compromised by the Dissector, both in case of a DDoS attack as well as under normal circumstances. The Dissector application is run **on demand** and is **not** a service that runs continuously.

The advantage of this deployment model is that the Dissector can never disrupt incoming traffic and therefore **cannot adversely affect the services that a Coalition Member provides** to its users and customers. It is up to the Coalition Member to detect the attack, sample the DDoS traffic, and run the Dissector application to generate a fingerprint of that traffic sample.

The Dissector is a client system, which means that it **does not (and cannot) accept incoming connections**. A Coalition Member can enable the option to automatically upload fingerprints to a DDoS-DB. In that case, the Dissector will upload the DDoS fingerprint (not the traffic capture) to the DDoS-DB. In no other case will the Dissector communicate with the internet or other networks in any way. If the Member's Dissector sends the fingerprints to ddosdb.nl (at SIDN Labs in the pilot phase), then other Members of the Anti-DDoS Coalition will receive them as well. If the Member shares the fingerprints with a local instance of DDoS-DB, then Members will be able to share fingerings with other teams within their organization. Of course, they can also do both.

The Dissector **has only one task**, which is to create DDoS fingerprints. It is not an Intrusion Detection System, nor does it have any functions that could affect your customers' traffic. A user must run the application for it to generate a fingerprint.

[1] https://www.nbip.nl/en/nawas/

Generic Operational Requirements

To run the Dissector software, Coalition Members need to:

1. **Install the Dissector:** The only requirement for a machine on which the dissector is installed is for it to have access to a network traffic capture sample of a DDoS attack; **it doesn't have to be installed on a machine connected to the operational network**. The easiest way to use the Dissector is in a Docker container; instructions for which are provided in the GitHub repository. Using docker, the Dissector's dependencies need not be installed separately. Alternatively, you can set up the Dissector by downloading the Dissector python code and its dependencies, along with two system dependencies: tshark and nfdump. The Dissector does not require privileged mode (root) to run and there are no specific memory and CPU requirements, although more resources will enable the Dissector to process more DDoS traffic more quickly. An Internet connection is optional (for sharing with other Coalition Members through DDoS-DB). The Dissector machine does not expose any services (open ports).

2. **Get attack snapshots:** The Dissector requires a network sample of the DDoS attack. Coalition Members themselves must detect, filter, and save a snapshot of the attack traffic in PCAP or FLOW format. A network traffic file size of around 100 Mbytes (up to 200 Mbytes) is usually enough for the Dissector to produce a representative fingerprint of the DDoS attack.

Legal prerequisites

Members will need to **sign the Coalition's data sharing agreement** to **share** fingerprints with other Coalition Members and receive fingerprints from them. Sharing fingerprints takes place through the **DDoS-DB**, which is hosted by SIDN in the project's pilot phase. They will give new Clearing House participants access to ddosdb.nl and they will countersign the agreement because they will be the data processor. The Coalition will select a new DDoS-DB Operator when the project transitions into production.