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

Cyber security cOmpeteNCe fOr Research anD InnovAtion [†]

Work Package 3: Community Impact and Sustainability

Deliverable D3.2: 2nd year report on Community Building and Sustainability

Abstract: D3.2 provides an overview of the key WP3 achievements in Y2 of CONCORDIA. We present a high-level overview of the results we attained in each of the five tasks, our lessons learned, and our way forward for Y3.

Contractual Date of Delivery	*M24*
Actual Date of Delivery	*30.12.2020*
Deliverable Dissemination Level	*Public*
Editors	*Marco Caselli (T3.1)* *Cristian Hesselman (T3.2)* *Reinhard Gloger (T3.3, D3.2)* *Felicia Cutas (T3.4)* *Aljosa Pasic (T3.5)*
Contributors	*Siemens* *SIDN* *CODE/MUNI/BADW-LRZ* *EIT Digital* *ATOS*
Quality Assurance	*Atos Spain S.A ** *Siemens* *ISI* *University of Insubria*

[†] 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
SURFnet bv	SURFnet bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a 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 a replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
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

Document Revisions & Quality Assurance

Internal Reviewers
Jose Francisco Ruiz, Atos Spain S.A * (review lead)
Marco Caselli , Siemens
Barbara Carminati, University of Insubria

Revisions:

Ver.	Date	By	Overview
1.0	*2020-12-30*	*Reinhard Gloger*	*Submission*

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, and starting up new businesses. WP3 utilizes WP1's technology developments and WP2's industry pilots. This inter-workpackage cooperation has been successfully enhanced in Y2.

The overall Year 2 WP3 achievements include the following:

- Task 3.1 has successfully met Y2 targets to establish the groundwork for information sharing of cyber threats. The Threat Intelligence Platform is under development and utilizes the MISP open source threat intelligence platform that was successfully validated at DFN-CERT. Testing with WP2's Telecom and Finance pilots has commenced.
- Task 3.2 is on track toward carrying out the pilots in the Netherlands and Italy. In Y2, we fleshed out the technical system, for instance in terms of its architecture, the maturity of its components, and its interworking with MISP to form the CONCORDIA Threat Intelligence Platform. In Y3, T3.2 will focus on coupling the DDoS Clearing House to the production systems of pilot partners in the Netherlands, further increasing the technical maturity of the system, and publishing the first version of the cookbook.
- Task 3.3 is on track to create a cyber security ecosystem to validate and demonstrate CONCORDIA's results and to foster cyber security trainings. A steadily growing inventory of tools, cyber range platforms, and training offerings have been created. The KYPO Cyber Range Platform is released as open-source. Sharing topology and training content across cyber range platforms in CONCORDIA have been prototyped.
- Targeting the development of an EU-wide cybersecurity educational ecosystem, Task 3.4 has developed the methodology for creating courses for professionals, developed content for the pilot course targeting cybersecurity consultant profile and defined the associated skills certification scheme. Task 3.4 also initiated collaboration with the other three pilot projects (SPARTA, ECHO, CyberSec4Europe) and is currently leading the CCN Education cross pilots' group.
- Task 3.5 addressing of community building activities to support startups is on track. After the identification and analysis of stakeholder motives, incentives and challenges, an initial scouting of startups has been completed. In the beginning of year 2 a startups community mailing list and communication channels have been established. In parallel, sub-task on incentives for data sharing have been started.

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)
- Starting up new businesses (T3.5)

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 startups
- *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 teachers (as part of the EEEC)	M, UC	T3.4
A *"factory" for starting new cybersecurity businesses* (start-ups), for instance in terms of IPR management and data sharing	M, UC	T3.5

The rest of this report provides an overview of the main results and lessons learned of WP3 in 2020, with a separate section for each of WP3's tasks (Sections 2 through 6). We conclude with the overall status of WP3 and an outlook for 2021 in Section 7.

Merge of tasks T3.5 and T5.1

In task T3.5 the concept of a "startup factory" evolved in a "startup community". This is in line with the envisioned merge of tasks T3.5 and T5.1 that was dealing with startups incubators and accelerators. Contract amendment was signed on 30.11.2020 and most of the work that was done in T3.5 is therefore included in this deliverable. We also refer to D5.3 for the last month of this year and the future activities, such as continuous "scouting" of "startup community" stakeholders that will continue to function under the name "Pan-European Cybersecurity Startup Community (PECS-UP)". All achievements of T3.5, such as the PECS-UP mailing list, quarterly newsletters, or work on data sharing incentives, will continue in the task T5.1, now much better integrated and aligned with the exploitation strategy and roadmaps.

COVID-19 Pandemic Effects

The overall impact of COVID-19 on WP3 activities was well contained. Despite the shutdown effects, the WP3 activities were adapted to fully achieve the task/WP objectives. While some in-person events, e.g., Capture the Flag, naturally had to be postponed, overall WP3 innovatively sustained its activity cooperation with the expanded use of virtual project management tools such as Confluence, Github, Teams and others. The task-specific solutions can be found in the respective sections, as applicable.

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 a wide variety of threat indicators in a trusted way. The platform will be able to automatically analyze threat information and seamlessly distribute appropriate event notifications. Its implementation will be based on 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 Status

Task 3.1 is on track and fulfilled the envisioned targets of Y2. 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 DoA such as "incident response automation". In the second half of the project, we plan to complete all development activities and focus more on processes and operations ensuring the correct and effective use of T3.1's solutions by all CONCORDIA partners.

2.3 Key achievements Y2

CONCORDIA Platform for Threat Intelligence

In the context of T3.3 ("Developing the CONCORDIA's Ecosystem: Virtual Lab, Services and Training"), T3.1, as well as T3.2, fit 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.

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

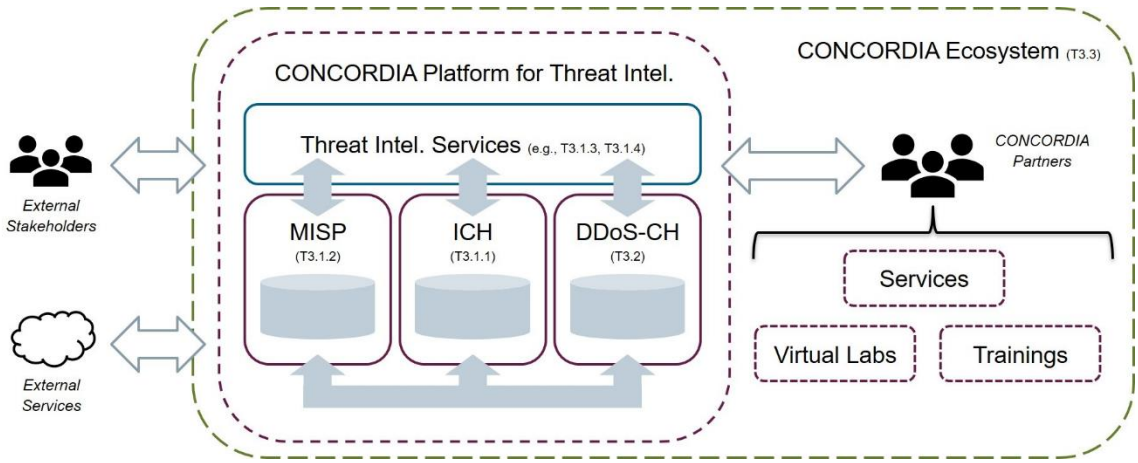


Figure 1: CONCORDIA Platform for Threat Intelligence

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 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. 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 – Created in 2011, MISP is an open-source threat intelligence sharing platform supported by the Computer Incident Response Center Luxembourg (CIRCL). Originally developed cooperatively by CIRCL and NATO, the platform emerged as an effective and efficient solution to share Indicators of Compromise (IoCs) which, at that time, were exchanged only by email as unstructured textual data (e.g., PDF documents). With the increase of cyberattack sophistication and the consequent need for collaborative analysis operated by distributed teams of security experts, the advantages of using MISP became clear and the project expanded to support a growing number of users: from individuals to worldwide private organizations as well as national and supranational CERTs (e.g., CERT-EU). 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 June 2019 and is currently managed cooperatively by Siemens AG (principal and formal responsible) and DFN-CERT itself. 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 November 2019 paving the way to the official rollout face in 2020. Among the active partners, it is worth mentioning that over Y2 FORTH worked on customizing and deploying security solutions (e.g., honeypot and firewall) 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

[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/

misused systems, but also vulnerable set-ups like running services that expose known vulnerabilities to the internet.

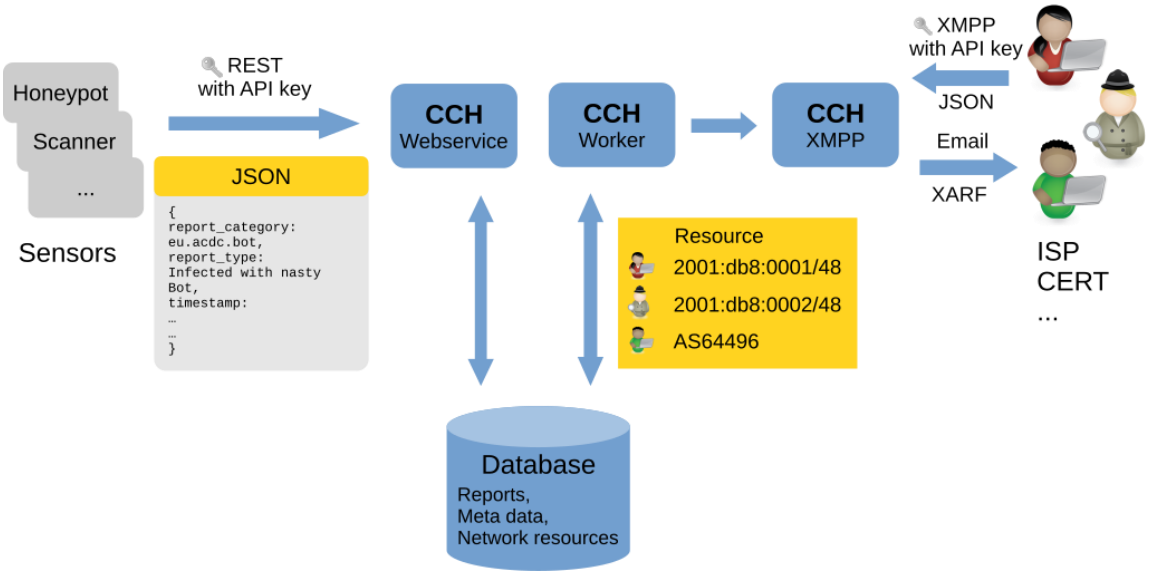


Figure 1a: Incident Clearing House architecture

The architecture of the ICH is depicted in Figure 1a. 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 – Discussed in Ch. 3.

Cross-T/WP 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 T3.5 on data sharing incentives, the key driver to enhance access to the solutions developed in T3.1 and their adoption in operational contexts.

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. 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.
- 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.
- 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).
- T4.2 on the definition of a legal framework to regulate the overall sharing process among the partners and pave the way to its extension beyond the scope of the CONCORDIA project.

Incident Clearing House

In accordance with the developing definition of CONCORDIA's Platform for Threat Intelligence in the T3.1/T3.2 Liaison, work on designing and implementing the integration of the ICH as a component into this virtual platform has started in Y2. This includes modifications to the data formats to support the linking of information between the different components of the platform and updates to the corresponding APIs.

The prototype of the metric computation on ICH reports has been completed and validated in a testing environment. The component is based on previous research on metrics done in WP1 and provides a first step in providing a threat landscape view as part of the threat intelligence platform. The deployment in the production environment is in preparation.

Investigating integration with infrastructure and tools available to and deployed by prospecting users of the platform, the ICH currently accepts new information over a REST API and supports two ways of accessing information: in real-time as JSON via XMPP and as XARF via email.

Submitting new information to the ICH requires an HTTP POST request with the information to be reported represented in JSON. The reports must conform to the ICH JSON schemata available online from the website of the originating ACDC project[1] and in a future release also directly from the ICH. This might require a translation of existing data into the ICH format to support unified handling of different data sources in the ICH. The data format supports to include the original representation of the data in order to retain all details that might be lost due to this translation. This could be further supported in the future by providing translations of widely used formats for example from IDSs (intrusion detection systems) to the ICH format either as open-source software components or in the ICH API itself.

Consuming the per user JSON feed is possible using any XMPP client, XMPP being a well-established and standardized messaging protocol. The JSON format equals the format accepted by the ICH extended by metadata like the timestamp of processing and the source of the report. There are specialized tools and frameworks that directly support this type of information. Most of these tools use their own internal data format, requiring a translation of the ICH format as part of the tools' configuration.

IntelMQ[2] is a "solution for IT security teams for collecting and processing security feeds using a message queuing protocol". The project is closely connected to the IHAP (Incident Handling Automation Project) group in the European CERT/CSIRT community and has received funding by the CEF framework. IntelMQ supports consuming information directly via XMPP. The information is processed in IntelMQ using a network of interconnected functional units called bots; processing the ICH reports would require the implementation of a parser bot that translates the information from the JSON reports into IntelMQ's information model, which is based on a similar model of objects based on key-value pairs.

SIEM systems are used in larger organizations to monitor and analyse security alerts related to the organization's infrastructure. In addition to standard software and hardware components, these solutions often support custom data sources by configuring a translation to their internal data model. This ensures that custom data can be correlated with other data sources. Examples of SIEM solutions that support JSON data like the ICH format include

[1] https://acdc-project.eu
[2] https://intelmq.readthedocs.io

Splunk Enterprise Security[1], IBM QRadar[2], and Exabeam[3] as well as open-source projects like ElasticSIEM[4], Apache Metron[5], and OSSIM[6]. Only few of these supports to consume information directly via XMPP, but can be connected to the ICH data for example via 1) a small component that connects to XMPP and streams data to the SIEM or stores it into files for the SIEM to consume or 2) using Apache NiFi[7]. Apache NiFi is an "easy to use, powerful, and reliable system to process and distribute data" that can be used to consume data from multiple interfaces, process it, and forward the results to multiple sinks. The project is currently working on supporting XMPP as a data source, which would allow to use NiFi to consume the ICH data, transform it to the format required and provide it in a multitude of ways including streaming it to a process or writing it to a file or network location.

IETF's MILE working group[8] (Managed Incident Lightweight Exchange) developed an XMPP extension called XMPP-Grid[9] in RFC 8600 that describes how XMPP can be used to collect and distribute security-relevant information between network-connected devices. Information is organized into different topics using a publish-subscribe pattern where information published to a topic is received by all current subscribers of said topic. ICH reports could be forwarded using such a set-up by the ICH itself requiring minor development work or preferably by an extra software component run together with an XMPP-Grid set-up that consumes the reports from the ICH and publishes them. Due to the sensitive nature of the information, the ICH provides the reports only to the party that is responsible for the affected network resources making a publish-subscribe pattern unsuitable for the ICH itself. A larger organization consuming its reports can, however, use such a set-up to distribute the reports for example to group information, drive processes, or automate incident response actions.

Sending reports via email uses XARF[10], the eXtended Abuse Reporting Format. Every email consists of two parts: a human readable part explaining in plain text the issue at hand and a machine-readable part that contains the original report submitted to the ICH adapted to conform to the XARF standard. Schemata describing the machine-readable format are available online and referenced in each report. The machine-readable information itself is a flat object of key-value pairs written in YAML[11] being also readable by humans. This allows scaling the processing of reports from the ICH from small entities with only manual incident handling processes to larger automated set-ups.

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

[1] https://www.splunk.com/en_us/software/enterprise-security.html
[2] https://www.ibm.com/products/qradar-siem
[3] https://www.exabeam.com
[4] https://www.elastic.co/de/siem
[5] https://metron.apache.org
[6] https://cybersecurity.att.com/products/ossim
[7] https://nifi.apache.org
[8] https://datatracker.ietf.org/wg/mile/charter
[9] https://www.rfc-editor.org/info/rfc8600
[10] https://www.abusix.com/xarf
[11] https://yaml.org

to quickly and effectively respond to these threats. 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 "CoA Deployment Architecture" is shown in Figure 2.

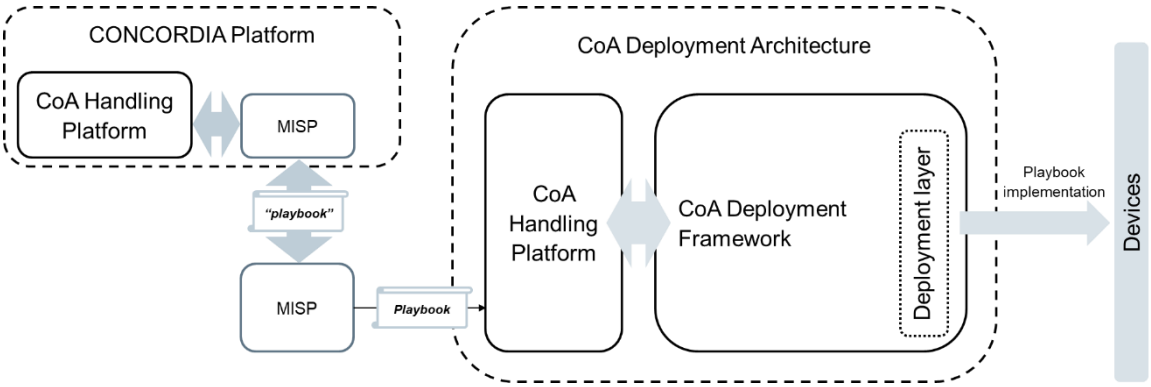


Figure 2: Incident Response Automation Overview

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. The work on this building block kicks off from a discussion among project partners aiming at collecting a set of requirements for modeling incident response activities. Some of the identified requirements are common and shared among all partners (e.g., compact and unambiguous representations of such activities). Others are sector-specific and come from specific needs (e.g., representations of activities intrinsically related to telecommunications, finance, etc.). To represent incident response activities, we investigate available standards such as the "Open Command and Control" Language (OpenC2) and newly proposed ones such as the "Collaborative Automated Course of Action Operations" (CACAO). Finally, we examine how these standards fit the use of the MISP threat intelligence sharing platform.

- The second building block 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 related to the specific environment in which they are going to be used (e.g., the digital infrastructure lying within the responsibility of a CERT). The activities presented within this building block are implemented within the so-called "CoA Deployment Architecture" shown in Figure 3.

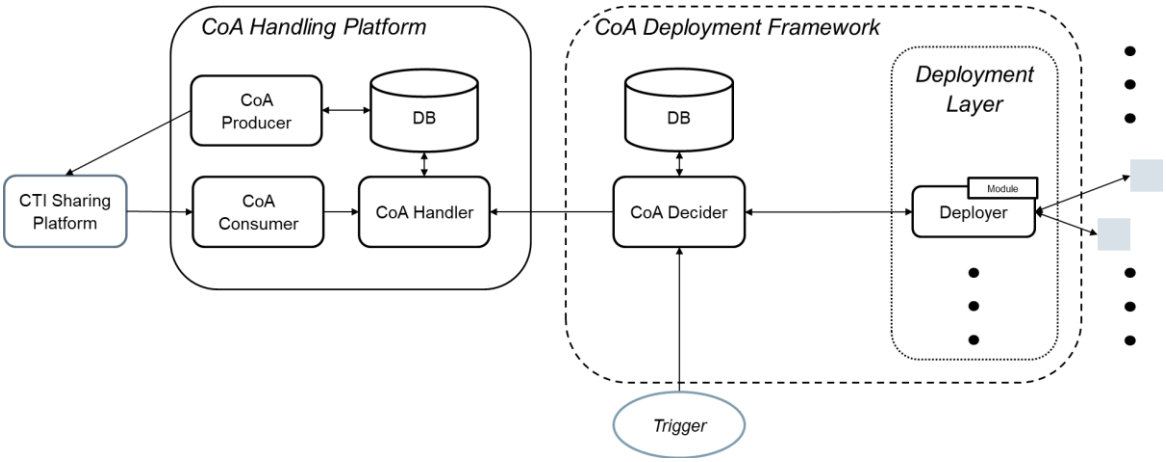


Figure 3: Course of Action Deployment Architecture

- 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 a course of action 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. Deployers are state-less and thus do not maintain information on the status of the environment in which they are operating (with a notable exception related to storing credentials). Furthermore, Deployers do not take decisions but they only execute operations chosen and coordinated by the CoA Decider. An overview of Deployers and their interaction with the CoA Decider is shown in Figure 4.

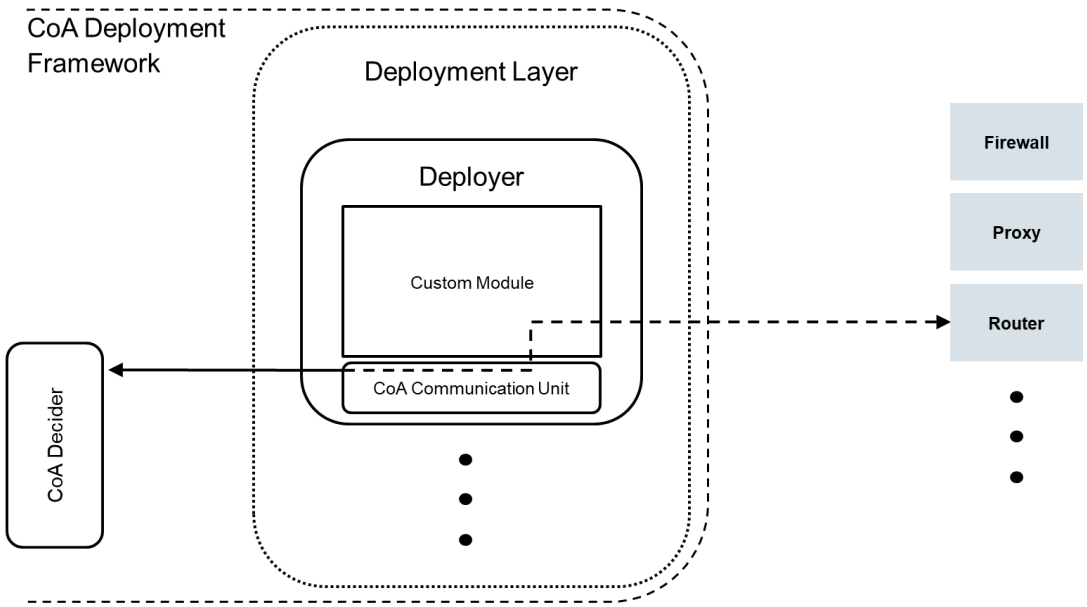


Figure 4: Course of Action "Deployer"

We plan to demonstrate the feasibility of the overall approach and show a proof-of-concept implementation of the three building blocks. In the current setup, the representation of

simple incident handling “playbooks”, their interpretation within the CoA Integrated Platform and their final deployment via the Deployment Layer will be tested in a realistic scenario.

Relationship to the T3.1/T3.2 Liaison

As already suggested by Fig. 2, the "CoA Deployment Architecture" fits and contributes to the "T3.1/T3.2 Liaison". In fact, the "CoA Handling Platform" represents one of the services envisioned to run within the CONCORDIA Threat Intelligence Platform. Figure 5 shows the detail of the components implementing a service for storing and distributing a formal representation of incident handling playbooks. These playbooks will be available directly to the CONCORDIA partners or used by further services running within the CONCORDIA Threat Intelligence Platform.

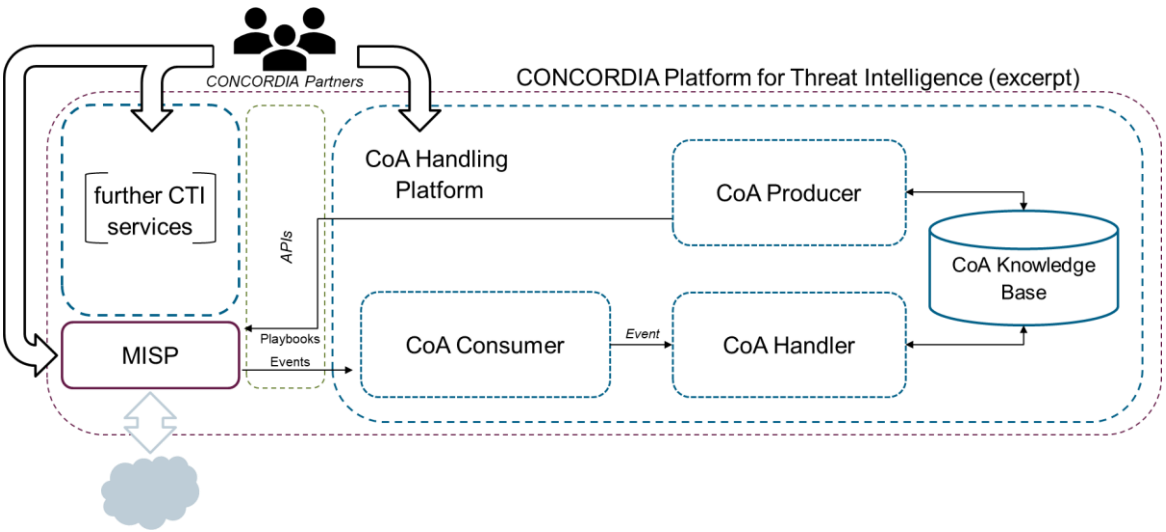


Figure 5: CONCORDIA Platform for TI & Incident Response

At the moment of writing, two use cases of the CONCORDIA Threat Sharing Platform take advantage of the CoA Handling Platform as well as an illustrative CoA Deployment Architecture locally deployed by one partner of the CONCORDIA project.

2.4 Outlook Y3

During Y3, we are going to further 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 advantages 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).

Furthermore, as described in the previous section, we continue working and enhancing the solutions for incident response automation. This work will conclude with the implementation of a proof-of-concept showcasing approach feasibility and emphasizing the possible improvements to the overall incident handling process.

Finally, in the upcoming year, the metrics computation on the ICH will be evaluated in the production environment. Further developing this towards a threat landscape view, it will be explored how the component can be extended or supplemented to compute metrics for other parts of the platform for threat intelligence.

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 **key deliverables** are a pilot in the Netherlands and in Italy as well as a DDoS clearing house "cookbook" that enables other groups of organizations to set up and operate their own clearing house.

3.2 Status

T3.2 is **on track** toward carrying out our pilots in the Netherlands and Italy, which is the task's ultimate objective. In Y2, we fleshed out the technical system (see Key Achievements), for instance in terms of its architecture, the maturity of its components, and its interworking with MISP to form the CONCORDIA Threat Intelligence Platform. Our work resulted in a more advanced prototype of the DDoS Clearing House, which we will refine further next year (see Outlook Y3).

The work in Y2 built on our results of Y1 (see D3.1 [D3.1]), which focused on getting the Clearing House's basics in place (e.g., a first running version of the system, legal documents to be able to share DDoS metadata, and organizational matters).

The T3.2 partners decided on a **demo-driven** approach for Y2, which means that we continually work towards a new demonstrator of the Clearing House, with the most recent version available for actual demonstrations (e.g., for EC Reviews). In Y2, we developed three versions of the demonstrator (v2.1 through v2.3), showing functions such as the automatic creation and upload of fingerprints and the visualization of fingerprints. We used the Clearing House demonstrator for both EC reviews in Y2, which we passed successfully (see EC Review Reports).

We presented T3.2 and our work on the DDoS Clearing House 14 times, both outside of CONCORDIA (10 times) as well as within the project (4). We published five blogs and one peer-reviewed paper.

We were fortunate that the COVID pandemic had a minor impact on our work except that we missed face-to-face meetings for sharing and generating ideas. We were able to compensate because we made a clear division of responsibilities across the partners based on the DDoS clearing house's interdependent components (see Figure 9), which allowed us to closely collaborate and advance the work.

3.3 Summary of the Achievements regarding DDoS Clearing House Concept

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, in particular with societies more and more connecting 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 **reduce Europe's digital sovereignty** (and that of digital societies elsewhere) because they result in the loss of control over critical processes. 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].

This last event led to a member of the Netherlands' parliament submitting parliamentary questions to the Dutch Government [Keijzer20], which shows an increased societal awareness of the problem. The impact of DDoS attacks may even extend to physical space [Hesselman20], for instance when they disrupt future services such as unmanned aerial vehicles (cf. Task 2.4) and connected ambulances (cf. Task 2.5).

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 when 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 larger 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 parties 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.

A complicating factor is that many critical service providers such as financial institutions use commercial **third-party services** to handle DDoS attacks (e.g., scrubbing services), often developed and operated by organizations outside of Europe (e.g., Arbor, Akamai, or Verisign, all US-based companies). A typical setup is that the victim has a basic DDoS mitigation service on-site to handle smaller attacks (e.g., through a DDoS appliance) and redirects attack traffic to the third party if they cannot handle the load anymore. From that point on, the victim is essentially "blind" and it depends on its contract with the third party to see what happens with the metadata of the attack. There are exceptions to this model, such as NBIP, a membership-based not-for-profit scrubbing center based in the Netherlands that offers scrubbing as a shared service to its member organizations.

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 control over 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 real-time 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 ADCs are ISACs, 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 and member of the

Dutch national ADC. ADCs can also work without such shared mitigation facilities, in which each member is responsible for providing their own.

Another type of ADC member is law enforcement agencies, who can potentially use the DDoS metadata for criminal investigation and subsequent court trails. For such members, the ADC needs to offer safeguards that prevent incorrect data from entering the legal system, such as an accurate timestamp that indicates when DDoS metadata was generated, cryptograph proof that it was not tampered with, as well as legal constructs, for instance to draw a clear line between gathered information (through the Clearing House) and using it for criminal investigation (by law enforcement agencies). The latter is important considering the ongoing discourse on the role of the private sector actions in fighting cybercrime [eSilva19].

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 6 illustrates this for three service providers (SP1, SP2, and SP3). SP2 gets hit by DDoS attack A, generates a fingerprint that covers A (FP(A)), and shares it with the other members of the ADC (SP1 and SP3), with SP2's operations team potentially adding pointers as to the best way to mitigate A. The operations teams of SP1 and SP3 use the fingerprint to derive traffic filtering rules (R1 and R3) and install them in their network equipment in case A comes their way next. Alternatively, SP1 and SP3 can request their upstream transit providers to block A's address blocks (e.g., using DOTS [DOTS18]). The three service providers also use the Clearing House to get fingerprints of past attacks and compare them to in-progress attacks on their infrastructure.

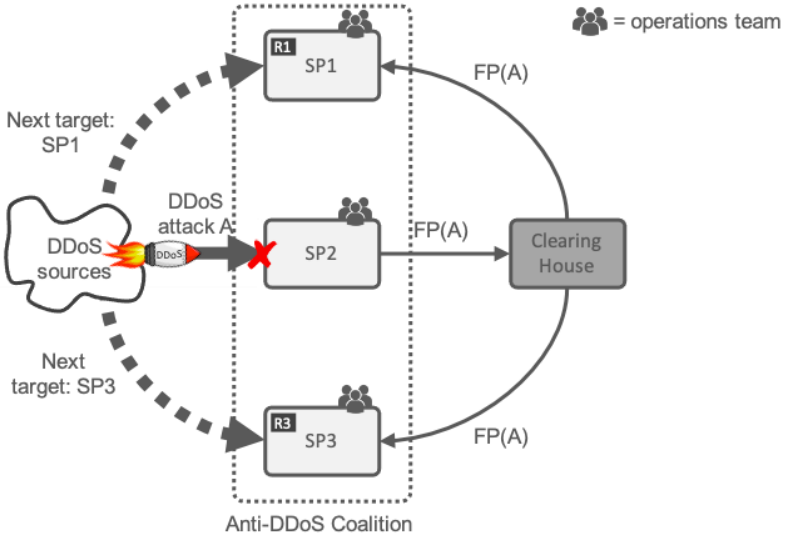


Figure 6: Example of an ADC and their DDoS Clearing House.

The advantage of the Clearing House is that the fingerprints help its members to more quickly derive packet filter rules for DDoS attacks that haven't hit them yet, which is work that usually takes place under intense pressure. For example, if SP1 were to be the next target of DDoS attack A without having A's fingerprint, then SP1's operations team would have to inspect the incoming DDoS traffic, write a packet filtering rule (R1) for the different types of equipment in their network, and push it into their network while, at the same time, the availability of SP1's services might start degrading. Having A's fingerprint beforehand gives them more time to implement R1, which increases the probability that they will be able to effectively mitigate the attack.

Figure 7 shows an example of the DDoS fingerprint of an attack that uses the Network Time Protocol (NTP). The fingerprint for instance lists the set of source IP addresses from which the NTP traffic originated (line "src_ips"), the number of sources addresses (line "total_src_ips"), the protocol that was used (line "service"), and the duration (line "duration_sec").


```
{
 "multivector_key": "fa0a8f21a1816a6531acb543743124ec",
 "key": "fa0a8f21a1816a6531acb543743124ec",
 "src_ips": [
  "109.26.226.136",
  ... ],
 "dst_ports": [80],
 "src_ports": [123 ],
 "ip_protocol": "17",
 "service": "NTP",
 "additional": {"ntp_reqcode": 42 },


 "total_src_ips": 1798,
 "total_packets": 2387741,
 "duration_sec": 120.32017302513123,
 "start_time": "2014-12-22 11:12:56",
 "avg_bps": 9545941.59169052,
 "avg_pps": 19844.893337223457,
 "start_timestamp": 1419243176.663222
}
```


Figure 7: Example of a DDoS fingerprint (from [Conrads19]).

Progress beyond the state of the art
While the concept of collaborative DDoS defense has been around for a long time [DDOS13] [BloSS19] [Meng15], **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 a limited insight into other parameters other than technology. 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 (see Key achievements Y2).

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

We discuss our ongoing and planned work across these tasks below.

3.4 Key achievements Y2

Developed DDoS Clearing House-in-a-box
One of our key accomplishments is that we implemented the high-level architecture of the DDoS Clearing House that we presented in Y1's D3.1 [D3.1]. Our implementation revolves around the new notion of a **"DDoS Clearing House-in-a-box"** (see Figure 8), which is a complete DDoS Clearing House in the form a Virtual Machine (VM) that every member of an ADC runs in their local infrastructure.

Conceptually, each instance of the DDoS Clearing House-in-a-box, depicted in Figure 8, generates and stores fingerprints of the DDoS attacks that the member handles on its network. The member's operations team enhances the fingerprints with rules that they have used to mitigate the attack (e.g., IP tables rules or Snort rules) for the specific equipment they are using in their network. They also check fingerprints of new attacks against known ones to quickly classify the attack and look up how to mitigate it.

The advantage of the DDoS Clearing House-in-a-box concept is that it eases the deployment of the Clearing House, because members only need to install the VM. In addition, the VM enables members to locally test and improve the Clearing House software, perhaps by adding their own custom extensions. This is particularly important in CONCORDIA because we have different partners working on different software components (see Figure 9).

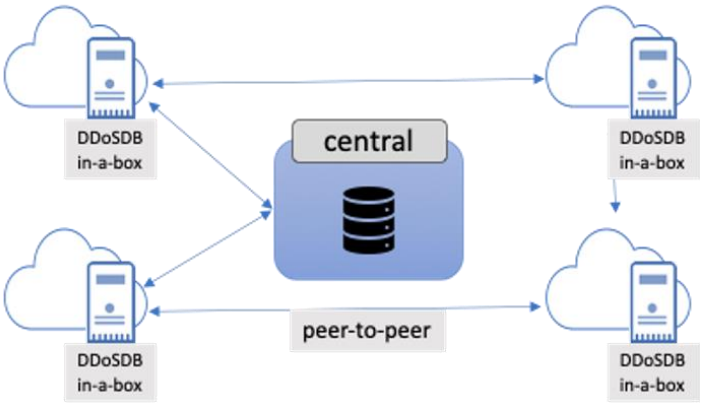


Figure 8: DDoS Clearing House-in-a-box.

At the same time, the DDoS Clearing House-in-a-box enables operations teams to share DDoS fingerprints with other members through a central database that all members can write to and read from. Since the central repository may become a DDoS target, we envision that we will ultimately replace it with a more distributed system in which different instances of the DDoS Clearing House-in-a-box share DDoS fingerprints with each other directly (see Outlook Y3).

The DDoS Clearing House VM is publicly accessible via our repository at **https://github.com/ddos-clearing-house**.

Refined clearing house architecture
We refined the functional architecture of the DDoS Clearing House by splitting it into three types of components with clearly defined interfaces between them:

- **Core components:** enable operations teams to generate, store, distribute, and use fingerprints based on actual or simulated DDoS attack traffic.
- **Supplementary services:** enrich and visualize fingerprints and make them available through the CONCORDIA Threat Intelligence Platform.
- **System management:** components that get the latest version of the Clearing House software from GitHub and automatically deploy it in the VM.

Figure 9 provides an overview of these components, which we will discuss in more detail in the next sections. The transparent components are the core components, the grey ones are the supplementary services (for readability, Figure 4 does not show system management components). The logos in Figure 9 indicate which T3.2 partners are responsible for which components. NBIP is a partner in the Dutch Clearing House pilot and provides DDoS network traces to develop and test the system. This is a voluntarily effort to support the research community because they are not in CONCORDIA.

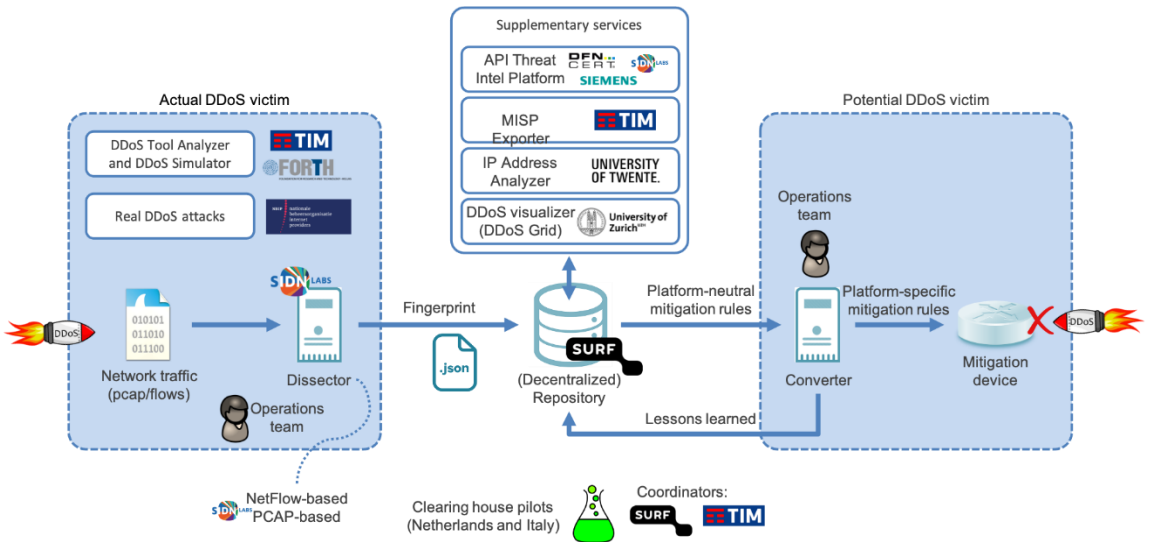


Figure 9: Clearing House key components and data flow.

The arrows in Figure 9 illustrate how a fingerprint typically flows through the system, from its creation at the member that gets hits by the DDoS attack (left) to its use by a potential victim (right). Each member of an ADC runs all of the Clearing House's components through the DDoS Clearing House-in-a-box VM, but for simplicity Figure 9 only shows each component only once.

Table 2 provides an overview of the function of each of the components, an indication of their maturity level, and the T3.2 experts working on them (owners underlined). SURF and TIM will handle the pilots in the Netherlands and in Italy, respectively.

Table 2: Clearing house components.

Name	Function	Maturity	Experts (owner)
Dissector	Generate DDoS fingerprints based on PCAP files and flow data	High	João
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High	Remco, João
Converter	Generate mitigation rules based on DDoS fingerprints	Low	João, Marco, Paolo
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High	Bruno, Muriel
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low	Ramin, Mattijs
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low	Christos
MISP Exporter	Generate MISP events based on DDoS fingerprints	Low	Madalina, Marco, João, Christian
Synthetic traffic generator	Generation of DDoS fingerprints using a TIM's DDoS traffic simulator	Low	Paolo

In Y2, we also developed the high-level design of the **"CONCORDIA Threat Intel Platform"** [CTIP20], a "convergence layer" that integrates resources from three databases:

The Incident Clearing House (Task 3.1), MISP (Task 3.1), and the DDoS Clearing House. The CONCORDIA Threat Intel Platform will be available as a Web service.

We defined several use cases of the platform [CTIP20], such as booter detection and incident response automation. The MISP Exporter forms the bridge between the DDoS Clearing House and MISP.

Improved core components
We improved the core components of the clearing house, which are responsible for generating, storing, and using fingerprints.

Dissector (SIDN). Generates fingerprints based on DDoS network traffic traces. In Y2, we implemented new clustering algorithms to fingerprint various types of DDoS attacks, so we can cope with the evolving characteristics of DDoS attacks. We added support for amplification attacks (one or multiple protocols) and GRE-based DDoS attacks, and we are working on additional ones. The new techniques have improved the accuracy and processing time to generate a DDoS fingerprint.

We also developed a new type of Dissector that can work with network flows and that complements our PCAP-based Dissector. We developed the flow-based Dissector on request of the partners in the Dutch ADC because they can deploy them more flexibly in their infrastructure than the PCAP-based Dissector.

We added several fields to the fingerprint format, such as attack vector (amplification attacks) and several labels that describe the attack's characteristics, such as “amplification” and “suspicious packet length”. We improved the Clearing House software, so it uploads fingerprints to repositories using an encrypted channel and we allow support teams to configure multiple repositories to upload their fingerprints too. The latter enables them to directly share fingerprints with other members of an ADC rather than through the central repository, which contributes to increasing the resilience of the DDoS Clearing House.

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 Y2, we extended the central repository to support encrypted communication and developed a module that can synchronize fingerprints between pairs of DDoS-DB instances, local or shared ones.

We also improved the web interface to make searching for fingerprints more intuitive for operations teams. For example, it is now possible to browse all fingerprints and filter or order them based on properties such as size, duration, or submitter. This is easier than entering search terms to find (types of) fingerprints, which can be difficult at first if one is unfamiliar with the associated search terms. Uploaded fingerprints can also be edited, allowing comments to be added to them. This can be useful for providing mitigation notes that may help other operators to handle the attacks. Editing is limited to either operators of the DDoS-DB or the original provider of the fingerprint, to prevent tampering with ill-intent.

Converter (SIDN, TI, SAG). Generates mitigation rules based on DDoS fingerprints. In Y2, we developed the first basic converters. The current version uses the Linux firewall (Iptables) to filter attack characteristics described in the fingerprints. We are investigating

if and how we can use MISP to author and distribute mitigation rules. This is a challenge because the current Snort converter native to MISP only generates very simple rules and does not consider some of the parameters in a fingerprint (e.g., destination port, layer 4, and application layer protocols). This is why we do not have an owner for the Converter yet, because we first want to investigate the option of using a MISP-based converter (see MISP Exporter below).

We developed the core components such that they are self-contained and so they can be executed either in different systems or in one machine.

Improved supplementary services
We improved the Clearing House's supplementary services, which aim at enriching fingerprints and making the system intuitive to use for operations teams. Together, they further enhance the added value of the core components.

MISP Exporter (TI, SAG, SIDN, DFN-CERT). Generates MISP events based on DDoS fingerprints. In Y2, we developed the first version of the MISP Exporter. It takes as an input a fingerprint file describing a DDoS attack and maps fingerprint attributes to the attributes of a MISP event. For example, it stores the fingerprint's source IP addresses in the MISP attribute Network activity/ip-src and the original fingerprint itself in the MISP attribute External analysis/attachment. Next, the Exporter publishes the event to the CONCORDIA project's MISP instance.

The open challenge is that the MISP platform only supports very simple Snort mitigation rules, which additionally only use the ip-src attributes in MISP events. We are therefore investigating how we can make these rules more expressive, for instance to include the protocol and port attributes of a fingerprint. One of the solutions is to keep the MISP Snort rule generation routine unmodified and directly store Snort rules in MISP by means of the Network Activity/snort attribute. Another possibility is to develop a more complex rule generation engine, which would also enable operations teams to author mitigation rules through MISP.

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 strikes. These tools include hping3 [HPING], nmap [NMAP] (mostly used for scanning purposes though), ddos simulator [DDOSIM], and others.

In Y2, we created a testbed that automatically creates fingerprints of "popular" DDoS tools and shares them via the DDoS Clearing House-in-a-box. We deployed a service that starts capturing network traffic as soon as it receives an alert from an Intrusion Detection System (IDS). The alerts are based on the rules that we have set. For example, we instruct the IDS to generate an alert if it detects TCP traffic that exceeds a rate of 10.000 packets/sec. Our automatic service sends the captured traffic to the Dissector, which creates the respective fingerprint and uploads it to the local DDoSDB instance at FORTH.

Currently, the tools tested include nmap, hping3 and ddos_sim. However, our setup enables us to also add new DDoS tools to the Analyzer, create more fingerprints and share them through the DDoS-DB.

DDoS Grid (UZH). Provides a dashboard for the visualization of DDoS fingerprints based on PCAP files or DDoS fingerprints. In Y2, we developed a fully functional proof-of-

concept of the DDoS Grid, which allows operations teams to visually analyze PCAPs (traces of packet capture), generate fingerprints (based on the Dissector's API), and analyze fingerprints stored in DDoS-DB (using DDoS-DB's API). Besides network operators, we expect that these functions will also be useful for researchers to conduct experiments or for education purposes. We have not yet integrated the DDoS Grid into the DDoS Clearing House-in-a-box package yet, which is work for Y3.

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 provided by this component intends to give network operators and researchers a better understanding of the similarities and differences between various attacks and attacking hosts. In Y2, we studied datasets that could potentially be used for this purpose and started the implementation of the first version of the IP-Address-Analyzer component.

Synthetic DDoS traffic generator (TI). Generates DDoS fingerprints using a DDoS traffic simulator at TI. In order to fully verify the robustness of the developed Clearing House software (e.g., the Dissector), extensive security tests have to be performed. In Y2, TI generated synthetic traffic traces and used them to test the Dissector installed at our premises. We found a few issues with the Dissector, which we promptly reported to the Dissector's owner.

At the end of Y2, we decided to shift TIM's focus on the integration of the DDoS clearing house with MISP and stop the work on the traffic generator. This is more important because it incorporates the DDoS Clearing House into the CONCORDIA Threat Intelligence platform. Also, we obtained PCAPs of actual DDoS attacks through the Dutch ADC (partner NBIP), which reduced the added value of the traffic generator.

Coupled components through APIs

A critical element in our modular architecture is the interaction **between** the Clearing House's components, which is an activity that **all T3.2 partners are involved in**.

In Y2, we assessed which Clearing House component requires which DDoS-DB entries and determined which components needed an API to interact with each other. Figure 10 illustrates the interfaces between the components, which we labeled A through F. The Dissector is the source of a fingerprint and passes them up the diagram to other components that consume them (e.g., the databases and supplementary services).

In Y2, we developed a prototype in which the DDoS Grid gets fingerprints from DDoS-DB (interfaces D, E and F), thus allowing visual exploration of fingerprints. The design of the APIs is based on REST and can easily be extended to support new supplementary services. We also refined interfaces A and B and we will be fleshing out the others (e.g., interface C) in Y3, as depicted in Figure 10.

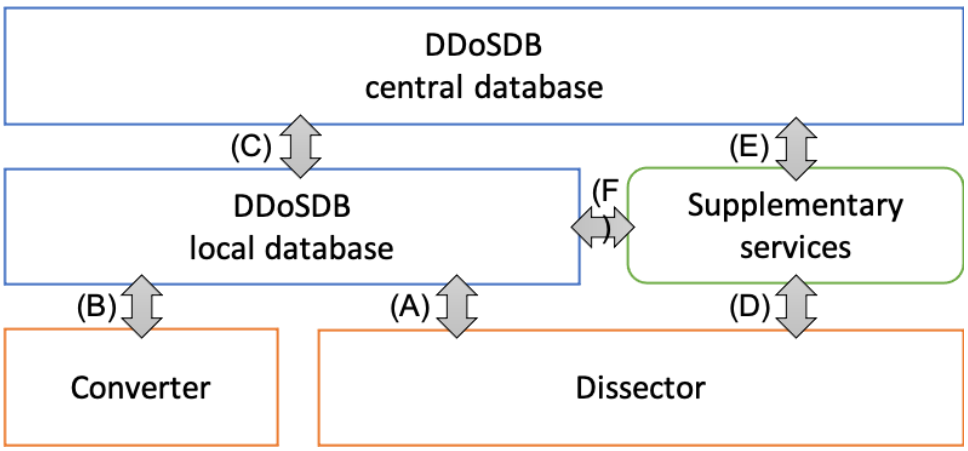


Figure 10: Communication interface between software modules.

Completed initial pilot preparations
In Y2, we went through our initial preparations for our pilots in the Netherlands and in Italy.

Netherlands (SURF, SIDN). SIDN set up a system to process DDoS attacks handled by NBIP, one of our partners in the Netherlands that provides DDoS scrubbing services. Using a shared volume, our Dissector can access the network files (pcap), process them, and upload the generated fingerprint to our repository (DDoS-DB). We have processed more than 50 attacks, including amplification, SYN flood, and fragmentation attacks.

In addition, SURF enhanced the "DDoS Clearing House-in-a-box" concept to ease the pilot phase. The novelty is an auto-update function that checks code repository updates (minor or major) on a nightly basis. Whenever such an update is available, the VM is automatically updated by pulling in the changes and running dedicated update scripts. This is an advantage because it reduces the downtime of the Clearing House, which is important to make software changes during the pilots, in particular for the central DDoS-DB instance. The enhanced version of the Clearing House-in-a-box is based on a clean Linux machine and improved versions of the core components.

Italy (TI). In Y2, we have set up the DDoS Clearing House in TIM's Security Lab, dedicated to the pilot in Italy. The lab setup consists of the core components (Dissector, DDoS-DB and Converter) in a virtualized environment, the traffic generator tools, the probes used to monitor the traffic and generate the PCAP files. The testbed is also connected to the MISP instance through the MISP Exporter. We started a preliminary investigation into the possible usage of real traffic captures. We will also be looking into the legal and privacy issues involved, based on the experience gained with the Clearing House in the Netherlands.

Helped advancing Anti-DDoS Coalition in the Netherlands
SURF, SIDN, and the UT continued their active contribution to the Dutch ADC, which focuses on critical service providers across the sectors of the Netherlands.

Specific accomplishments are:

- Translated the data sharing agreement that we use for the pilot in the Netherlands to English and made it available to all CONCORDIA partners.

- 5 members of the Dutch ADC signed the agreement to share data through the central instance of DDoS-DB at SIDN Labs. We planned the actual exchange of fingerprints through the system for Y3 (see below).
- Helped start the Legal Working Group of the Dutch national ADC, with a legal expert from SIDN joining the WG.
- Actively disseminated the CONCORDIA results in the Dutch Anti-DDoS Coalition and wrote a joint blog series (see below).

Dissemination results

Tables 3, 4, and 5 show our dissemination results for Y2 in the form of presentations (10 outside of CONCORDIA and four within the project), peer-reviewed papers, and blogs, respectively.

Table 3: Task 3.2 presentations in Y2.

Month	Event
Dec-20	C. Hesselman, "CONCORDIA's Cross-sector Cybersecurity Infrastructure", Cyber Competence Network Concertation Event
Nov-20	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2) – Status Update GA5", 5th CONCORDIA General Assembly
Oct-20	J. Ceron, "IoT security and the DDoS Clearing HouseDDoS Clearing House", INTERSCT kickoff
Sep-20	C. Hesselman, "DDoS Clearing House for Europe (Task 3.2) – Cross-sector Pilot Demo", CONCORDIA 2nd Review
Sep-20	J. Ceron, "DDoS Clearing House: technical updates", Plenary Session of the Dutch Anti-DDoS Coalition
Sep-20	J. Ceron, "DDoS Clearing House: setup and updates", Dutch ISPs Plenary
Sep-20	J. Ceron, YouTube Channel with instructions on how to run the Clearing House, https://www.youtube.com/channel/UCYpLwD-86GybRVF61PlaSww/featured
Sep-20	C. Hesselman. J. Jansen, E. Lastdrager, „Internet of Things: kansen, keerzijdes én oplossingsrichtingen", SIDN Webinar (in Dutch)
Jun-20	C. Hesselman and J. Ceron, "DDoS Clearing House for Europe", Concordia General Assembly
Jun-20	C. Hesselman, "The DNS & the Internet of Things: Opportunities, Risks & Challenges", High Interest Plenary Session, ICANN68
May-20	J. Ceron, "DDoS Clearing House for Europe Cross-sector Pilot", Council of European National Top-Level Domain Registries (CENTR) Jamboree
Feb-20	J. Jansen, "The IoT and the DNS", ETNO Working Group Meeting
Feb-20	C. Hesselman, "Increasing the Netherlands' DDoS resilience together", SURF Security and Privacy Conference, Tilburg University, Netherlands
Jan-20	C. Hesselman and R. Yazdani, "DDoS Clearing House for Europe Cross-sector Pilot Demo", 1st CONCORDIA review, Brussels, Belgium

Table 4: Task 3.2 papers in Y2.

Month	Venue
Sep-20	M. Franco, E. Sula, B. Rodrigues, E. Scheid, B. Stiller: ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections; International Conference on Economics of Grids, Clouds, Software and Services (GECON 2020), Izola, Slovenia, September 2020, pp 1-12. URL: https://bit.ly/3lw6uoS

Table 5: Task 3.2 blogs in Y2.

Month	Event
Sep-20	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/
Sep-20	J. Ceron and R. Poortinga-van Wijnen, "New version of the DDoS Clearing House core components", https://www.sidnlabs.nl/en/news-and-blogs/new-version-of-the-ddos-clearing-house-core-components
Jul-20	R. Poortinga-van Wijnen and J. van Dijk, "SURF's TAO approach to Cybersecurity", https://www.concordia-h2020.eu/blog-post/surfs-tao-approach-to-cybersecurity/
Apr-20	C. Hesselman, R. Poortinga-van Wijnen, G. Schaapman, and R. Ruiter, "Dutch Anti-DDoS Coalition: lessons learned and the way forward", https://www.concordia-h2020.eu/blog-post/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward/
Apr-20	C. Hesselman, R. Poortinga-van Wijnen, G. Schaapman, and R. Ruiter, "Setting up a national DDoS clearing house", https://www.concordia-h2020.eu/blog-post/setting-up-a-national-ddos-clearing-house/
Apr-20	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/

Key lessons learned

We identified several key lessons learned based on our work in Y2. The first is that our **modular design** based on clearly defined APIs is the key for the development of a **decentralized Clearing House architecture**. We observed this in particular when we interconnected the DDoS-DB and the DDoS Grid. Also, our loosely coupled system design enabled us to work with component owners and advance the work on multiple components in parallel.

As for MISP, we learned that **the MISP platform is likely a good candidate for DDoS signature sharing**. This is because the MISP platform supports ADCs (through MISP communities), allows for local and shared instances of the DDoS-DB (through MISP instances), and supports synchronization among these servers. At the same time, MISP also has limitations related to the type of attributes it offers for storing the fingerprint parameters and the generation of snort rules. We will investigate this further and address these issues in Y3.

As for fingerprint generation, we learned that the Clearing House needs to support **multiple types of Dissectors** (e.g., PCAP and flow-based) to enable the members of an ADC to flexibly deploy the system that best first their networks.

Finally, we learned that our **way of working** enabled us to get the work done despite the COVID pandemic. For example, the **demo-driven** approach that we took allowed the T3.2 team to set clear objectives for each next increment, while having the latest software versions available for demonstration (e.g., at the EC review). In addition, we were able to compensate for the missed out face-to-face meetings because we **associated an owner with each of the components** (except for the Converter), which stimulated collaboration because the components depend on each other. The owner is responsible for the development process and the interaction with other software components.

We also learned that the **diversity** of the T3.2 team (e.g., in terms of gender, Member State, interests) is an important added value for the work but requires even clearer communication than in more homogenous teams (e.g., describe the task/features in simple yet precise terms to avoid misunderstood or reworking).

We summarized our Y1 lessons learned in a blog series [DDoSCH20], which we published on the CONCORDIA site, amongst others.

3.5 Outlook Y3

In Y3, T3.2 will focus on three challenges: (1) coupling the DDoS Clearing House to the production systems of pilot partners in the Netherlands, (2) increasing the maturity of the Clearing House's core components and supplementary services and their integration into the overall system, and (3) publishing a first version of the cookbook, preferably as a paper. In addition, we will continue our joint work with T3.1 on CONCORDIA's Threat Intelligence Platform and with various other tasks, such as T4.2 (legal constructs).

Coupling with production systems. To carry out the pilot in the Netherlands, we will need to connect the Clearing House to the production systems of the Dutch partners to create fingerprints from the DDoS attacks they handle. We expect that this will be a major challenge from an organizational perspective. For example, for large corporations such as ISPs, this may be a tedious task because they need to convince multiple layers of management of the necessity, make the infrastructure changes (e.g., realize a port mirror to capture network traffic), and potentially also update their working procedures. An important requirement to make this happen is that the Clearing House software must be stable and pilot partners are able to test the Clearing House on a test network.

Maturing and integrating the Clearing House's components. In Y3, we will further improve the Clearing House's core components (Dissector, DDoS-DB, and Converter), which is key to increasing confidence in the concept and convince the pilot partners to connect to the Clearing House. Examples include additional fingerprint generation algorithms for the Dissector, mechanisms to share fingerprints between clearing house instances without using a central DDoS-DB, and refined APIs. We will also further flesh out the supplementary services. This includes the interaction with MISP, for instance in terms of an improved MISP Exporter that transparently adds the Clearing House as a dataset to the MISP platform and a MISP extension for authoring and distributing DDoS filtering rules. It also includes a more advanced version of the IP Address Analyzer (e.g., to associate a "reputation score" with IP addresses) and the DDoS Tool Analyzer (e.g., to

automatically fingerprint a tool when an updated version is available). The work will also require some research (e.g., on the IP-Address-Analyzer), which will be our bridge into T1.2.

First published version of the cookbook. Our third objective next year will be to aggregate our pervious documents and lessons learned into a first version of the DDoS Clearing House cookbook. It will help organizations in Europe and elsewhere to set up their own DDoS Clearing House. We aim to publish the report in the form of a paper. The Task Leader recently approached the editors of Springer's Journal of Internet Services and Applications (JSAC) and they appear to be interested in publishing a paper on the DDoS Clearing House from a multidisciplinary perspective.

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

- T1.2 (Network-Centric Security): for research that might be required to develop new types of Dissectors or to measure attackers' infrastructure.
- T2.1 (Threat Intelligence for the Telco Sector): to study if the Clearing House can help mitigating flooding attacks on 5G network infrastructure.
- T3.1 (Building a Threat Intelligence for Europe): to refine the CONCORDIA Treat Intelligence Platform and its interaction with the DDoS Clearing House.
- 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 8.

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 training that correspond to the evolving cyber threat landscape.

4.2 Status

The first steps in Services and Training for exchanging scenarios in Cyber Ranges were done as well as the cooperation with other H2020 projects in Year 1. Therefore, the work in Y2 is built on the results of Y1 described in Delivery D3.1 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 **Boosting the CONCORDIA's Cyber Security Ecosystem: Virtual Lab, Services and Training** scheduled to motivate CONCORDIAns to cooperate esp. in virtual labs. In addition, we contributed with videos and with important task 3.3 output (Services and Cyber Ranges) to the CONCORDIA stories (Task 5.2).

4.3 Key achievements Y2

This chapter is structured as in DoA: Virtual Labs, Services and Training.

Lessons learned: Systems and data sharing need special engagement

We addressed partners to support and include existing or future planned (virtual) labs, e.g., digital forensics, reverse engineering or malware analysis. We add them to our list to be part of CONCORDIA's ecosystem for virtual labs, services, and training. This requires strong motivation: Not only the project will gain from it, this is a typical win-win situation with added value to the organization as well. By adding labs, partner will get publicity, reputation, and most likely also feedback. Feedback helps to refine the lab and to improve the research.

Virtual Lab

As CONCORDIA takes a holistic and scalable approach to cybersecurity, our vision is to provide a common portal via CONCORDIA's website as entry point for Cyber Range platforms, (virtual) labs, and services. All these services are bringing added value to CONCORDIA's 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 as a first milestone in year 2. This activity is ongoing to improve the offer.

Our final goal is to have a common portal via the CONCORDIA's 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) and their interfaces, policies, conditions - online virtual accessible, supplementary willingness to cooperate and share trainings data and content.
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 organisations 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.

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

Services
To provide a portfolio of tools and services to CONCORDIA and the wider community, a map with an overview of courses and trainings for professionals has been published and maintained[1] (see Figure 11). Any information of value is thus in one place and can easily be found.

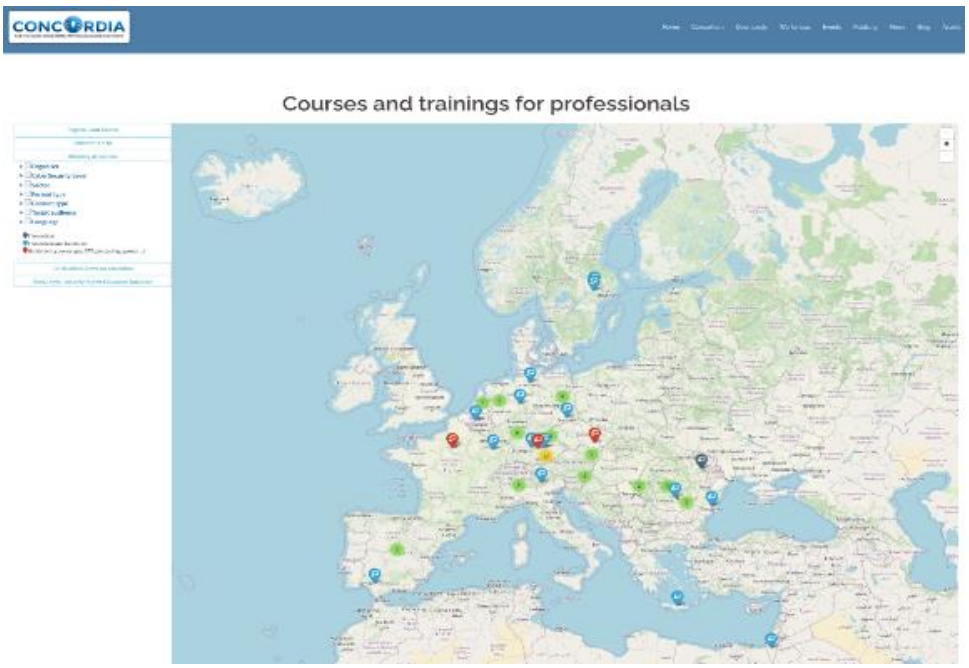


Figure 11: Courses and trainings for professionals

Every listed course and training are categorized as:

1. Theoretical.
2. Theoretical and hands-on or
3. Hands-on (cyber ranges, CTF, pentesting, games…) event.

Additionally, courses and trainings can be filtered/selected according to their:
1. Organizer (CONCORDIA partner or other EU course providers),

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

2. CyberSecurity Level (Device-centric, Network-centric, Software/System-centric, Data/Application-Centric or User-centric),
3. Sector (Telecom Sector, Financial Sector, Transport e-Mobility Sector, eHealth Sector, Defence Sector or Others),
4. Format type (Face-to-face, Online or Blended),
5. Content type (Theoretical, Theoretical and hands-on, Hands-on (cyber-ranges, CTF, pentesting, games…)),
6. Target audience (Corporates senior management, Corporates technical team, Corporates other departments, Start-ups/Scale-ups, Recent graduates, Students, Freelancers, Academia or Others) or
7. Language (English, German, French, Italian, Dutch, Slovene, Czech, Romanian or Spanish).

In order to have a better overview of the timing of events, ongoing work focuses on the integration of the courses and trainings found in the map (thus visualized by location) into the CONCORDIA cybersecurity events calendar [1] .

CTF Best Practice Guide
We started with a best practice guide for CTFs. 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 V1.2 of CONCORDIA tools after an 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
A new Python Tool called pyperpwn for "Automated Success Verification of Exploits for Penetration Testing with Metasploit" [3] was developed. Results have shown, that pyperpwn is more efficient than existing tools like Hail Mary or Autosploit to assist the Pentester. This is a great step forward to reach a Fully Automated Penetration Testing.

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

As T3.3 has focused on researching the possibility of interchanging testing and training content (e.g., base virtual images, network topologies, software configurations, and scenario descriptions) between cyber range platforms in year 1, the successful result of sharing content is shown by MUNI below.

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

[1] https://www.concordia-h2020.eu/cybersecurityevents
[2] https://www.concordia-h2020.eu/concordia-service-cybersecurity-tools/
[3] https://github.com/dial25sd/pyperpwn
https://www.youtube.com/watch?v=NXY7Fo6GMwE

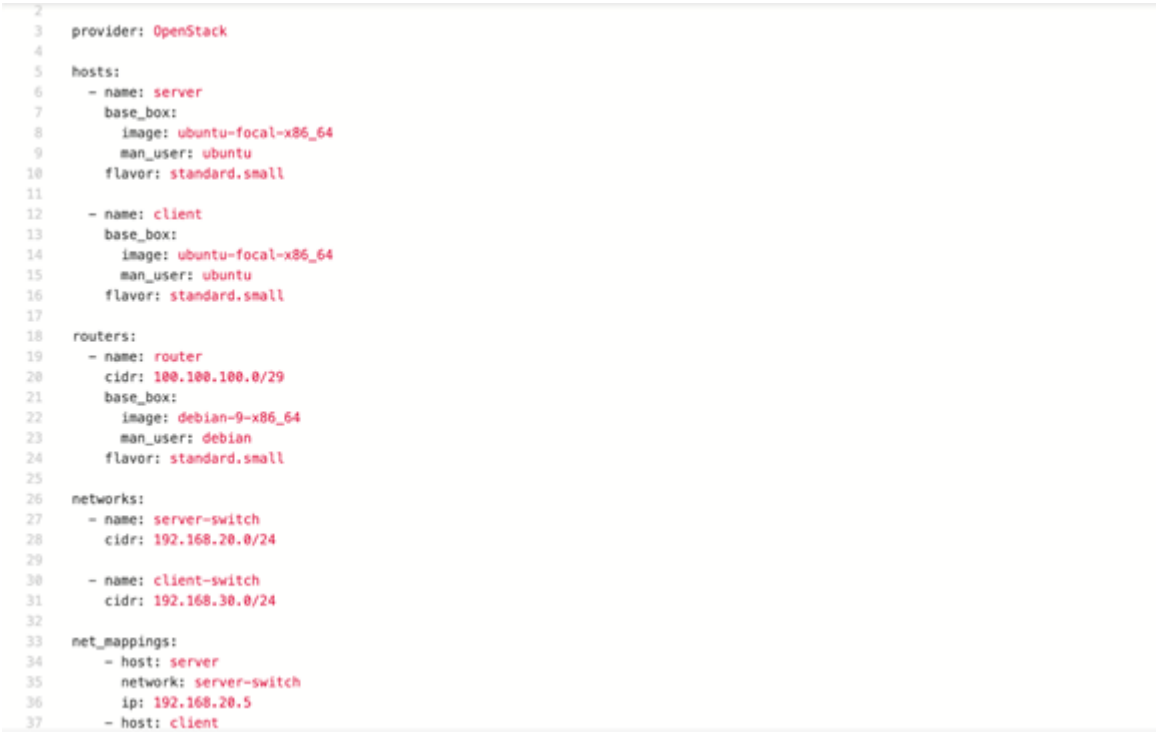
and leads one of the activities in the group. As the result of talks inside, Cyber Range Focus Group T3.3 organized CCN Webinar on Cyber Ranges to show different approaches to solve cyber range topics through the four pilots and foster cooperation between the pilots.

T3.3 prepared together with the help of T5.2 - Dissemination and communication activities microsites presenting capabilities of all CONCORDIA cyber ranges. Previously collected contacts were used to reach organizations developing and/or running a cyber range. Each organisation received a template with questions about their cyber range. Questions were emphasized on CONCORDIA's approach on building an ecosystem and possibilities of sharing content between cyber ranges.

KYPO Cyber Range Platform is Released by CONCORDIA as Open-Source[1]

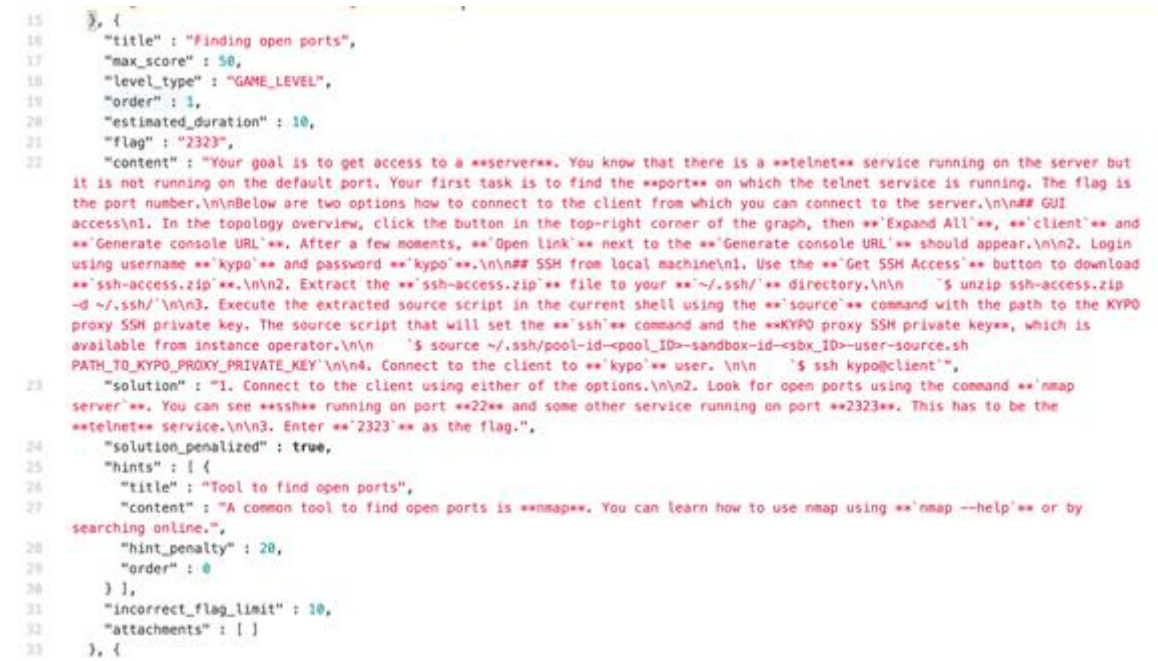
MUNI, as a member of CONCORDIA, released an open-source cyber range platform, so all consortium partners can use it to develop and run content for cybersecurity education. MUNI also delivered a network topology description format and the first prototype of an open format for sharing the content, so it is easy to share it around the consortium. The open-source cyber range makes hands-on cybersecurity education widely available for universities and organizations in Europe, as this is based on open infrastructure, open data, and open training formats, which provide a better chance of creating content. Furthermore, it can play the role of the basic instrument to form a new community around the platform that will exchange content and/or building blocks to improve training scenarios and make them reusable and available to everyone. For that reason, virtual machines, networks, and trainings are entirely described in human-readable data-serialization languages JSON and YAML or used open-source software packer to build virtual machines and ansible for describing machine content.

[1] https://www.concordia-h2020.eu/blog-post/do-you-need-a-cyber-range-the-kypo-cyber-range-platform-is-now-available-for-free/
https://cybercompetencenetwork.eu/ccn-webinar-on-cyber-ranges/
https://www.concordia-h2020.eu/
https://www.concordia-h2020.eu/kypo-cyber-range/



```
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 12: 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 13: Screenshot of a prototype of training description format

The following events were held with CONCORDIA's participation (see Table 6) that are directly related to the project[1] measurable KPI-DC-5 "More than four (4) Capture-the-Flag (CTF) competitions, training seminars, and training courses."
Corona pandemic prevented further f2f-courses. Several events have to be postponed.

Table 6: Training events in Y2.

CODE - CTF and CTF qualification– postponed	**27.-28.11.2020**
CODE's Jeopardy-style CTF involved multiple categories of challenges. The teams had to go through an online qualifying CTF. *The real event was postponed to 2021*	
UL – 2nd Security Management Course – postponed – details below	**16-20.11.2020**
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. URL: http://telecomnancy.univ-lorraine.fr/fr/security-management	

Security Management Course at Telecom Nancy with Cyber Range Practical Exercises

UL/Telecom Nancy has prepared the second edition of the **Security Management** course, with the development of **complementary cyber-range practical exercises** with respect to an APT1-oriented attack. Initially scheduled in November 2020, the event has been postponed to the second week of February (from February 8th, 2021 to February 12th, 2021), in the premise of the Telecom Nancy engineering school. This course aims at providing 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. These exercises permit to put in practice the covered security management concepts, as well as to analyze the decomposition of a cyber kill-chain, in particular considering the case of an APT-1-oriented attack (with different attack paths).

Discovery of Software Vulnerabilities using Cyber-Range Environment and Tools

UL/Telecom Nancy students have discovered new **evasion vulnerabilities over the Suricata intrusion detection system**, in the context of a **collaborative work with the CatenaCyber SME** (https://catenacyber.fr). An access to the cyber-range platform has been provided to this SME for experiments. The students have been acknowledged for this work by the Open Information Security Foundation (OISF) in October 2020 (https://suricata-ids.org/2020/10/08/suricata-6-0-0-released). Another collaboration with CatenaCyber SME permits to discover **vulnerabilities over the MySQL database management system** with the involvement UL/TELECOM Nancy students. The vulnerabilities have been discovered by extending the open-source OSS-fuzz fuzzing tool (https://www.oracle.com/security-alerts/cpuoct2019.html, https://www.oracle.com/security-alerts/cpujan2020.html), and students have received a Google Vulnerability Reward for this extension in February 2020. Finally, some DoS

vunerabilities affecting Facebook messenger have also been highlighted (and rewarded) by a student from the cyber-security curriculum in January 2020.

Scenario for cyber security specialists

A prepared and deployed scenario for cyber security specialists was developed by TUBS[1] in the Cyber range training section.
The ability to analyze software systems without access to the source code, offers many advantages including the detection of vulnerabilities so that they may be fixed before an adversary can exploit them in a zero day attack. This type of analysis also has an important role in education and continuous security training as it allows students/trainees to use their imagination and creativity in the exploration process. TUBS, in their work, uses two techniques for black-box testing based on their previous research efforts, where they demonstrated how library calls may be intercepted using wrappers as well as using the kernel to separate the memory of a process into regions, based on the (statically/dynamically) linked libraries that a program uses. By monitoring function calls to libraries or the main executable, they can determine if a high-level execution signature (which depends not only on the occurrence, but also the sequence and number of calls) fits a pattern of a possible attack against a system under test. They can, then, (a) determine whether a call should go ahead, (b) determine whether the arguments are acceptable, and (c) ensure that they will be informed when there is suspicion of foul play. They then demonstrate how these techniques may be used in student exercises to explore the structure of software systems and determine how such systems respond to specific input sequences designed to trigger bugs or demonstrate unexpected behavior. These scenarios can also be applied to different domains in the context of training and evaluating trainees on their actions and response when an attack is performed.

4.4 Outlook Y3

Our plans for T3.3 in Y3 are:

Virtual Lab

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

Services

It has been found that a lot of knowledge in organizing different types of events is available in the CONCORDIA consortium. Nonetheless, this knowledge is spread among many partners and only difficult to find and access at the moment without prior knowledge. For the upcoming year, we plan to create best practice guides for the organization of cyber

[1] *Marinos Tsantekidis and Vassilis Prevelakis, "Software System Exploration using Library Call Analysis" in the 2nd Workshop on Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), Virtual, 2020. https://doi.org/10.1007/978-3-030-62433-0_8*

trainings such as capture the flag (CTF) or cyber range events. We want to increase number of tools and training opportunities into the portfolio. 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 2021, 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.
- MUNI plans to create a community around KYPO Cyber Range Platform (released 11/20) and build a content ecosystem around the platform. All content will be described in the open format, which's the prototype was already introduced with the platform. MUNI will also encourage other organizations inside and outside the consortium to use the open format in their cyber ranges and be a leading example in developing cyber ranges content.

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 Status

Task 3.4 is progressing as planned. The work performed in the second year on setting up the Cybersecurity Competence Network (CCN) - Education group[1] and coordinating the cross pilots' collaboration on Education contributed to further develop the European Education Ecosystem for Cybersecurity. The methodology for the development and deployment of courses for cybersecurity professionals and the feasibility study for a Cybersecurity Skills Certification Scheme were published. Further, they were started to be implemented via the first pilot course and the pilot certification scheme targeting the cybersecurity consultant profile.

5.3 Key achievements Y2

In Year 2 (2020), under Task T3.4 the main effort was allocated to the following actions:

- *Action 2.* Design and develop a Cybersecurity specific Methodology for the creation of new courses and/or teaching materials;
- *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; and

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

- *Action 6.* Contribute to building a European Education Ecosystem for Cybersecurity.

Besides these actions, Task 3.4 continued acting on the *Action 1*. Pooling, assessing and disseminating existing courses and started shaping the *Action 5*. Teach the Teachers. Figure 14. depicts these 6 actions where the green colour illustrates the progress we made under the different task actions (totally green means completed and white means to be done).

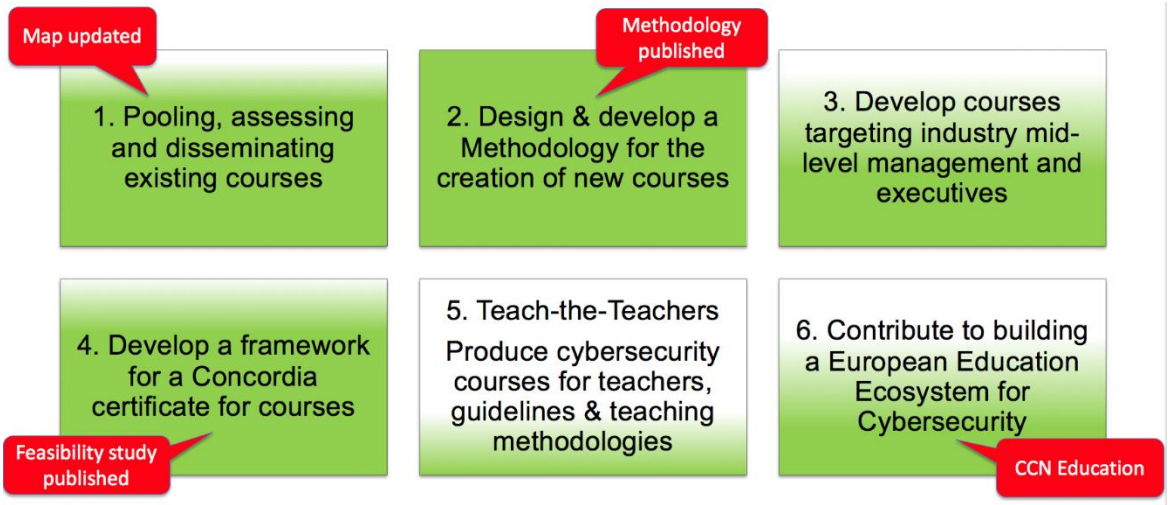


Figure 14: Structure of the Task T3.4 actions and progress.

5.3.1. Updating the CONCORDIA map on courses for cybersecurity professionals

The database of the CONCORDIA courses was updated at the beginning of year 2020. Consequently, Task 3.4 updated the information on the website, both the map[1] and the calendar. FORTH partner (T5.2 Communication) is continuously supporting this task with the addition of new functionality in the respective webpages of the CONCORDIA website.

By November 2020, 70+ courses were displayed on the map, organised by either (a) CONCORDIA partners or (b) external consortium course providers. Following several discussions with ENISA in relation to the possible merging the CONCORDIA database of courses for professionals with the Agency's Cybersecurity Higher Education Database[2], we agreed, for the moment, to implement the cross promotion between the maps. Thus T3.4 included a mention and direct link from the CONCORDIA map to the ENISA HEI map (cf. Figure 15 top). Similarly, ENISA included a pointer from their FAQ to the CONCORDIA map (cf. Figure 15 bottom).

[1] https://www.concordia-h2020.eu/map-courses-cyber-professionals/.
[2] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

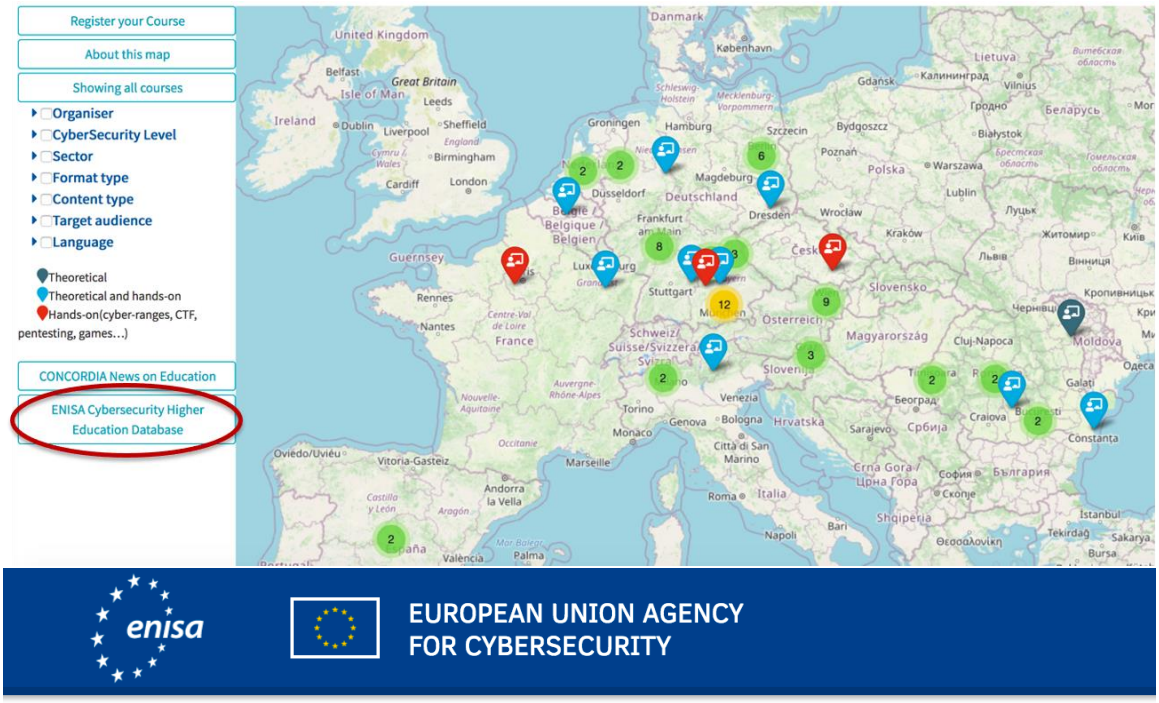


Figure 15: Cross promotion ENISA-CONCORDIA maps

5.3.2. Methodology for the creation and deployment of new courses

At the beginning of Year 2, Task 3.4 finalized and afterwards published the CONCORDIA Methodology for the creation and deployment of new courses and/or teaching materials for cybersecurity professionals[1].

The Methodology paper used as input the outcome of the Assessment of the CONCORDIA courses paper and the Feasibility study on existing skills certification schemes. In the process of building it, Task 3.4 started from the EIT Digital expertise in developing and deploying courses for professionals. Then Task 3.4 invited the CONCORDIA partners contributing to the task to comment on the process and provide input on best practices to help identify the key elements to be mentioned in the Methodology, and to include them as examples.

The Methodology document describes the process for designing and deploying a course while also detailing different steps and proposing a timeline for the process implementation. Further, it provides details on the individual Methodology topics based on the following structure: a rationale, a "How-to" non-exhaustive guidance on its implementation, and an "Example box" pointing to a concrete case and/or providing useful links and suggestions. Finally, the document summarizes the elements of Methodology as

[1] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf

a checklist which can be used as a support for course providers in their work of developing new content.

Annex A includes an executive summary of the Methodology. The full document is downloadable from the CONCORDIA website.

5.3.3. Developing courses for Cybersecurity Consultant profile

The development of courses for Cybersecurity Consultant profile followed and applied the Methodology developed in the previous task action. The overall process Task 3.4 followed is depicted in Figure 16.

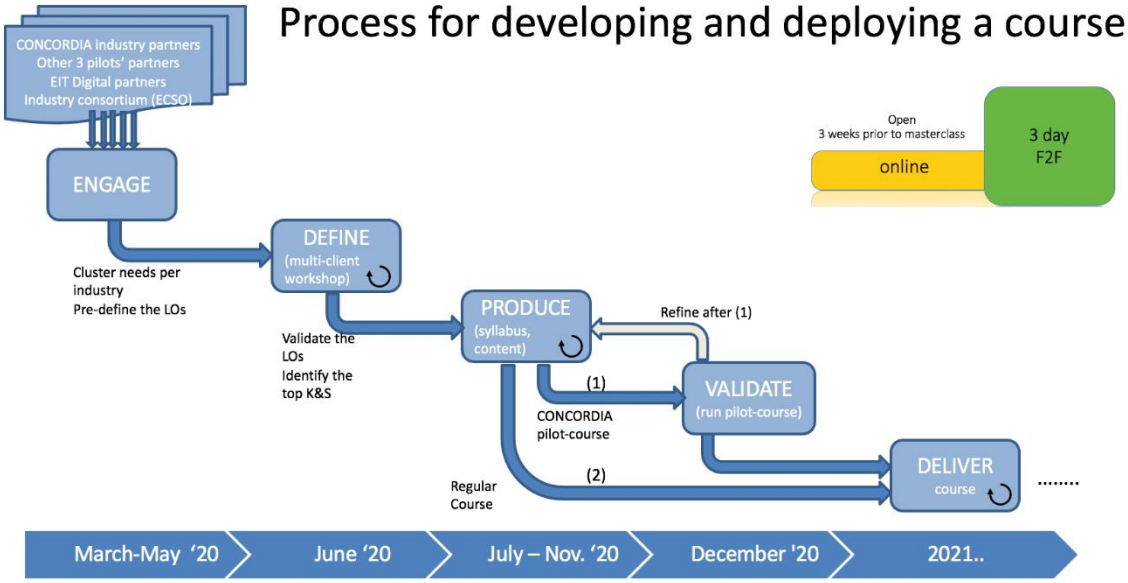


Figure 16: The process for developing and deploying the course

The initial planning for developing the content for the first course was planned to be performed during the months of March to September, with a first pilot course scheduled to be run at the beginning of November. However, because of the COVID-19 pandemic, Task 3.4 had to postpone the organization of the workshop from April to June in order to get organized for a fully online hands-on workshop. Although the timeline was delayed by approximately 2 months, the new format of the workshop allowed the task partners to interact with more stakeholders than initially planned (e.g. 70+ participants to the webinar as compared to the 20 seats allocated for the physical workshop). This increased interaction allowed Task 3.4 to refine the outcomes of the workshop and better tailor the course content.

As part of the **ENGAGE** phase, Task 3.4 conducted 2 surveys:

- Survey 1 was opened for 2 weeks in March and was composed of mainly open questions. The objective of the survey was to evaluate the relevance of the profile (Cybersecurity Consultant) and of the Learning Objectives (*i.e.*, Threats, Technology, and Economics and Business)

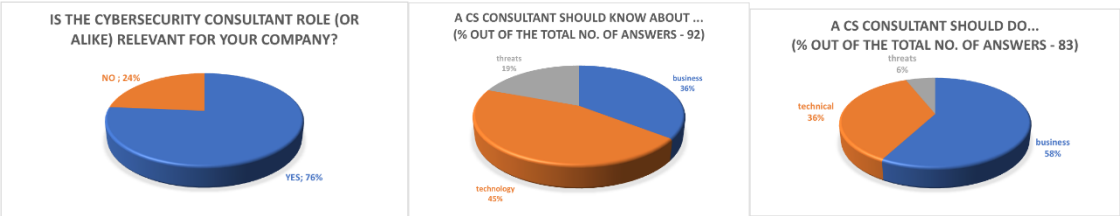


Figure 17: Statistics linked to the results of the first survey

- Survey 2 was opened for 3 weeks in May and was conducted on a platform specifically designed by University of Twente (UT) for this purpose. The objective of this second survey was to collect structured input on Knowledge and Skills linked to the targeted profile. The database of the platform was prefilled with 200 knowledge and 90 skill pre-selected from the NICE Cybersecurity Workforce Framework[1]

The **DEFINE** stage was materialized in an online workshop which ran on June 2nd-3rd, 2020.
The workshop was organized in two strands linked to the activities on (a) developing a framework for skills certification and (b) course content creation for cybersecurity professionals. Following the workshop, Task 3.4 published a Education Post-workshop Report[2] presenting the outcomes of the different hands-on exercises More specifically the following information was presented:

- The determination of a Role Profile of a Cybersecurity Consultant - by collecting input from the participants to the workshop on the most important and important set of Knowledge and Skills considered relevant for the European market. This exercise was a continuation of the Survey 2 mentioned above. Figure 18. depicts an instance of the survey results linked to the Knowledge. The colors illustrate the aggregated result of the selection done by the different contributors on the importance of individual Knowledge in relation to the Cybersecurity Consultant profile (i.e., green- very important, yellow – important, red – not important).

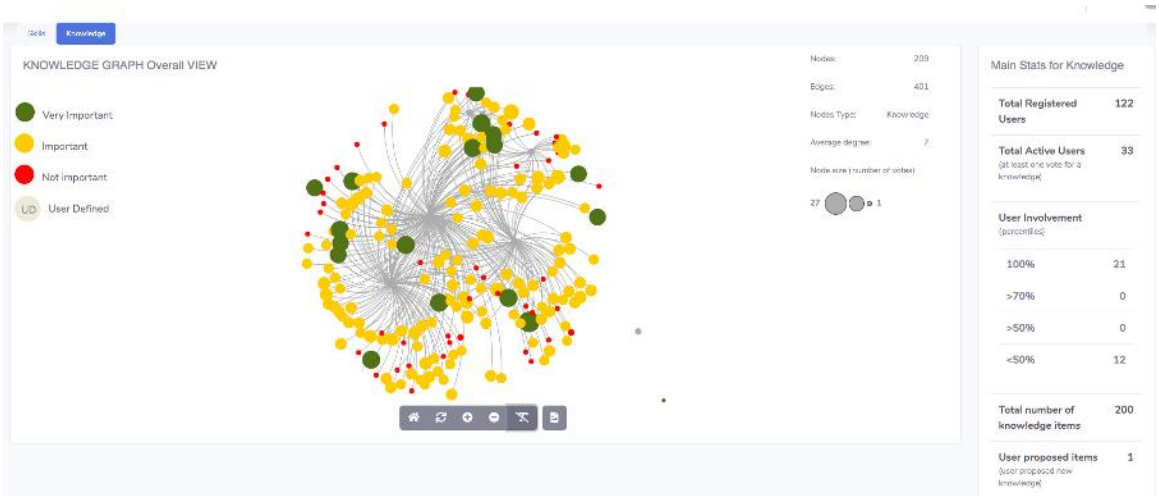


Figure 18: Network view of the Knowledge based on their importance

[1] https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[2] https://www.concordia-h2020.eu/wp-content/uploads/2020/07/CONCORDIAWorkshoponEducation2020-forpublication.pdf

- The definition of the content for previously defined Learning Objectives for the implementation of the relevant course, tailored per industries. In view of reaching this objective Task 3.4 (a) selected together with the participants to the workshop the Top 10 Knowledge and Top 5 Skills per Learning Objective (THREATS – TECHNOLOGY – ECONOMICS&BUSINESS) to be addressed in a course and (b) identified the most important technologies per targeted industry to be addressed in a course. The Figure 19 below illustrates the aggregated opinions of the participants to the workshop on the relevance of different technologies for specific industries.

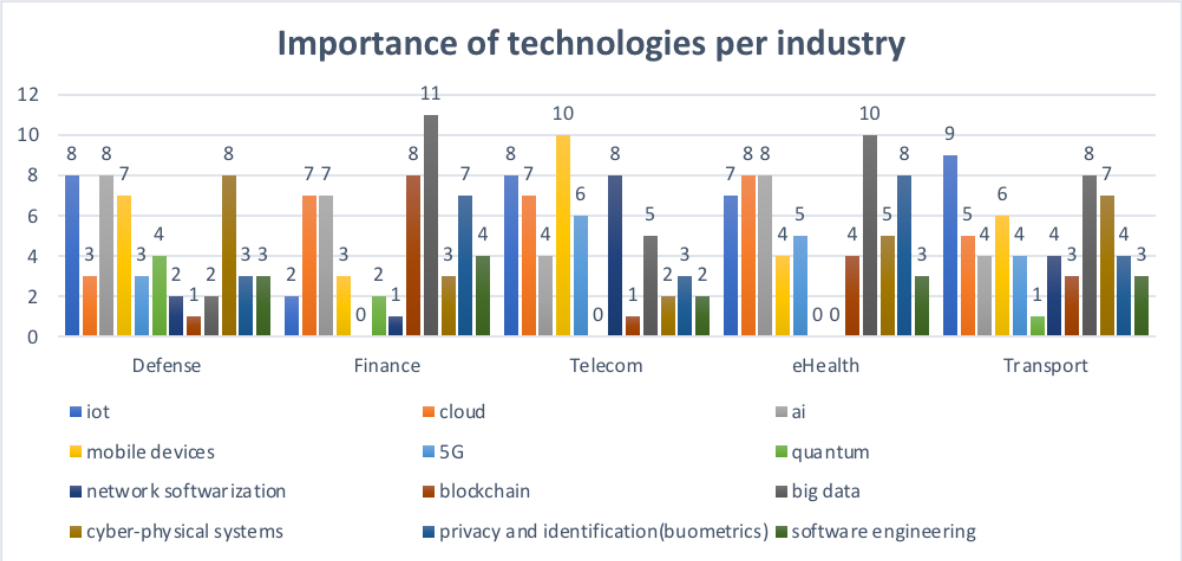


Figure 19: Importance of different technologies per industry – clustered per industries

The Report post Workshop was published on the CONCORDIA website and promoted via social-media channels and on the project Newsletter. The Executive Summary of the Report is presented in Annex B and the document can be downloaded from the CONCORDIA website.

In the **PRODUCE** phase, together with the partners involved in the task and coordination the work under the 3 Learning Objectives (Threats – partner UMIL, Technology – partner UL, Economics and Business – partner UZH) Task 3.4 "translated" the list of the most important Knowledge and Skills identified in the previous step in a concrete syllabus. The different lessons defined under the syllabus address at least one of the targeted Knowledge/ Skills and are structured under 4 modules as depicted in the Figure 20 below.

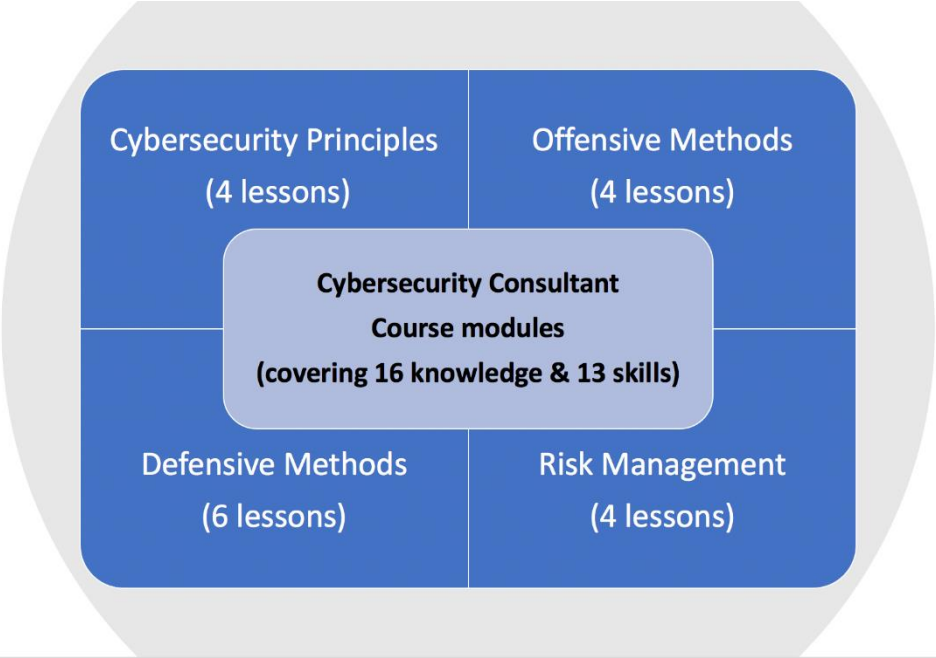


Figure 20: The 4 modules of the online course for Cybersecurity Consultant

The syllabus and a mapping of the different Knowledge and Skills against the learning objectives and the modules of the syllabus could be found in Annex C. Content wise we build primarily on the outcomes of the tasks T4.1 (Threats), T4.2 (Legal aspects) and T4.3 (Economics) while also bringing additional expertise from the consortium to cover the part of the topics identified during the process but not directly related to the main 3 tasks listed above. Currently, the team working on developing and delivering the course involves 8 partners (UNIMI, UL, UZH, ALVB, UI, BD, ISI, UM), both from the academia and the industry side.

The initial plan was to use one single studio to film all the video-lessons. Because of the COVID-19 pandemic which drastically limited the mobility of the people cross border and of interactions, we decided that all partners in charge of filming lessons to will do it locally, using the available resources. To ensure a certain level of homogeneity of the videos, the platform OBS studio[1] was selected as it is an open-source one. This approach led to additional delays in the process because of the time needed to accommodate with the platform. Yet, the online content was delivered still in Q4 of 2020 and is ready for running the pilot course. It currently contains a total of 18 lessons deployed over 57 videos and 21 quizzes, covering about 9 hours of study.

As described in the Methodology, the course will comprise two parts: (a) an online module and (b) a face-to-face/webinar module. The online module is hosted on the Coursera platform and could be accessed via the following link: https://www.coursera.org/teach/becoming-cybersecurity-consultant/. The online module is aimed at covering general theoretical concepts while also introducing some examples. It will help set the common grounds for the participants, on which we will build further during the face-to-face/webinar. The content for face-to-face/webinar on the other hand, will be industry specific in the sense that we will choose as examples to be discussed and for the hands-on exercises, real cases relevant to the industry targeted by the specific instance of

[1] https://obsproject.com/

the webinar. For the first pilot, we have selected the Telecom industry. The e-health and e-finance industries will follow.

5.3.4. Towards a Cybersecurity Skills Certification Scheme

This activity ran in collaboration with task T5.3 - Certification.

In Year 2 (2020) Task 3.4 finalized and made public the Feasibility study for a Cybersecurity Skills Certification Scheme[9] assessing the need for the creation of such a certification scheme, and identifying profiles not currently covered by relevant known certification schemes. The study looked mainly into the existing initiatives for cybersecurity careers and studies, cybersecurity body of knowledge, existing Cybersecurity skills certification schemes, and mapping existing certification schemes to competencies and levels.

Based on the conclusions of the Feasibility study Task 3.4 started developing a Role Profile (since there was no one in existence for the selected Role of Cybersecurity Consultant) and after that a Certification Scheme. At the same time, Task 3.4 started the development of a Framework for the Certification of Cybersecurity Skills, based on the best practices identified for the Cybersecurity training of professionals. The Certification of Cybersecurity Skills Framework document will provide an overview of the components for the certification of Cybersecurity Skills - from the submission of the application to the achievement and the preservation of their certification, including the examination mechanisms proposed by CONCORDIA for the certification of knowledge, skills and other competences of the related professionals, and the type of supporting technology to be used in the implementation of the framework. The Certification of Cybersecurity Skills Framework will be made public in 2021 and is currently being piloted through the design and implementation of the Skills Certification Scheme of the Cybersecurity Consultant. In preparation for this action, Task 3.4 ran a survey to collect input from the stakeholders on the skills certification framework and organized an online workshop to present the findings of the feasibility study and help define the Cybersecurity Consultant profile role in view of certification, as mentioned in the Section 5.3.3. above.

The summary of the Cybersecurity Consultant Role Profile is described in Annex D. and the full paper can be consulted online via LINK[1] [*currently the document is available solely for the EC review process]*.

5.3.5. Teach-the-Teachers

The work on this action started in June 2020. In the context of information and awareness about Cyber-safety, the partner CUT organized experiential workshops for teachers and students. Specifically, 9 teachers and 46 students attended Cyber-safety courses at their school environment in Cyprus. The main purpose of the courses was to spread awareness and show the teachers how to provide education and help the students to understand and consolidate the online social network dangers and teach them how to cope with them appropriately. Furthermore, both the teachers and the students were informed about the latest technology findings that can help them address the online threats towards a safer

[1] http://concordia-h2020.eu/other_files/concordia-Cybersecurity%20Consultant_v0.5.2.pdf

social network life. The initial results were captured in the newsitem Cybersafety workshops in school[1]

Based on the outcome of these experiential workshops Task 3.4 started building a survey aimed at collecting information from a larger 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 (enough) covered 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.
The CONCORDIA Survey - Teaching cybersecurity in high-schools[2] was built on the EU survey platform in English and launched online in December 2020. Starting January 2021 it will be translated in some EU official languages such as German, Spanish, French, Italian, Greek and will be disseminated on social media.

Starting January 2021, Task 3.4 intends to promote the survey in the European Schools system[3] as it will help us collect feedback from diverse cultural perspectives performing in the same environment. After collecting initial input via the survey, we will run a series of interviews to further refine the answers and get more in-depth feedback.

5.3.6. Building the Ecosystem

Setting up and coordinating the CCN Education cross-pilots group

Beginning of the year 2020 Task 3.4 initiated a collaboration with the other 3 pilot projects ECHO, SPARTA and CyberSec4Europe and build the Cybersecurity Competence Network CCN-Education group and started exchanging on existing and future outcomes on which the pilots can collaborate or build on. In this process task 3.4 invited to assist and provide guidance both the EC DG CONNECT and ENISA representatives as to ensure that our work is aligned to the policy developments, and engaged with ECSO by exchanging on the results and cross-promoting initiatives.

The initial cross-pilots group covered all the Education related activities ran by the four pilots, cyber-ranges included. Yet, after the second meeting, we decided to split the group in two in order to allow the cyber-ranges group to explore more in-depth the technical part of these activities and the federated cyber-ranges approach. Thus, while the CCN-Education group continued to be led by CONCORDIA project, the Cyber-ranges group leadership was moved to SPARTA project.

Currently, the CCN Education group covers four main strands: skills framework, mapping of courses, certification and the ecosystem. Apart from the periodic meetings documented on the EC platform CIRABC, the CCN Education group successfully ran in June an online

[1] https://www.concordia-h2020.eu/news/cybersafety-workshops-in-school/
[2] https://ec.europa.eu/eusurvey/runner/6e30ed0b-3888-eff4-e85f-0d7c92f178db
[3] https://www.eursc.eu/en

workshop on Education hosted by ENISA during which we agreed on specific options for collaboration and timelines per individual strands.

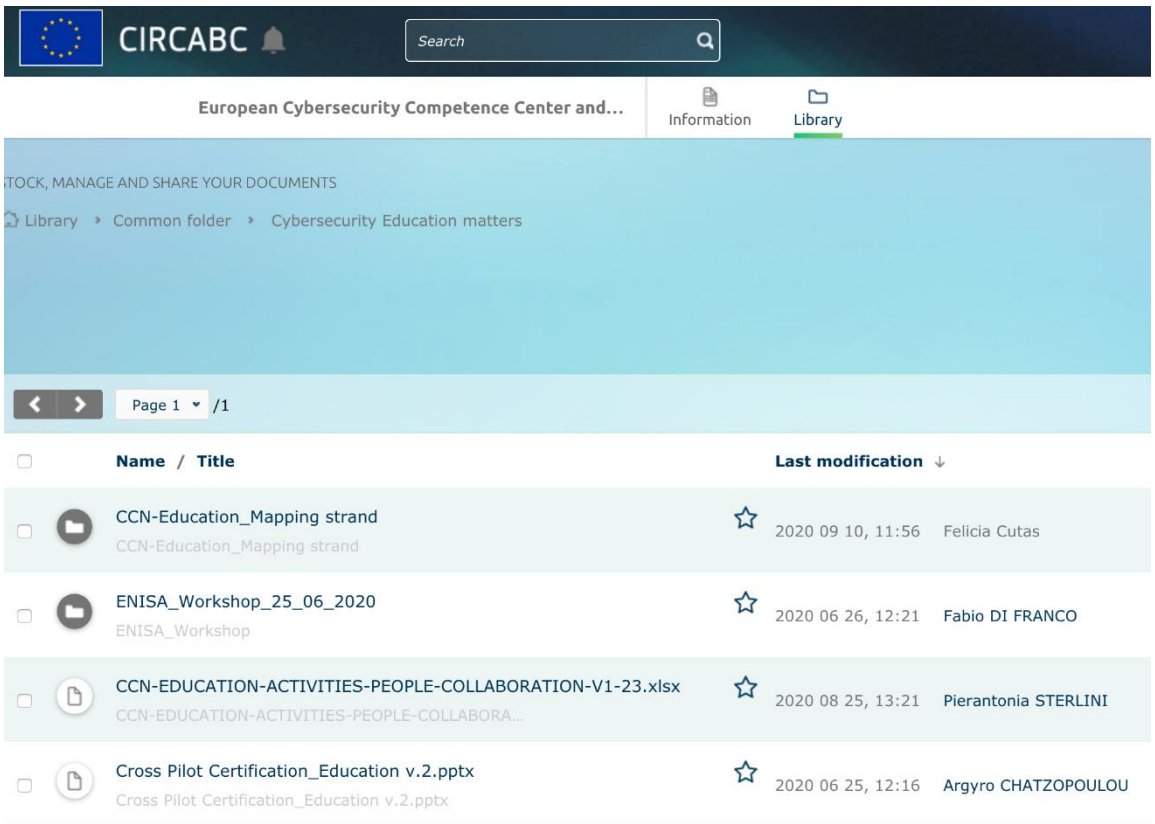


Figure 21: Excerpt from the Cybersecurity Education library on CIRCABC

The collaboration with the other pilots is beneficial also in terms of complementarities but also in terms of sustainability of the individual pilots' work. Following the ENISA workshop we have decided to explore further the possibility of collecting all the information on courses and trainings under a single map, having in mind the end-user and the support the pilots can offer on the long run in building their career path.

For the time being, given specificities of individual maps and the technical restrictions, the map Task 3.4 built for displaying the courses for professionals (the CONCORDIA target audience) is complementing the ENISA map on Masters and PhD programmes to which SPARTA and CyberSec4Europe will contribute by exporting their databases. And a cross promotion between CONCORDIA map and ENISA map was implemented as mentioned in the Section 5.3.1 above. Yet, it is foreseen for the future that ENISA map will incorporate all the information linked to different cybersecurity education options within Europe.

In the year 2020 CCN-Education also went public by presenting in the CONVERGENCE event the results of the collaboration so far and the plans for the year 2021. For the session Four Pilots, One Goal – a Strong European Education Ecosystem for Cybersecurity[1], Task 3.4 contributed with shaping the format, proposing the speakers, creating the script of the panel and drafting the text announcing the objectives of the CCN Education group and of the panel itself.

[1] https://cybercompetencenetwork.eu/convergence/education-focus-group/

Figure 22: Structure of the CCN-Education panel during CONVERGENCE event

Communicating with the Ecosystem

In view of easing the access to the CONCORDIA Education related information, Task 3.4 was allocated and contributed to the design of a special area on the CONCORDIA service board called Cybersecurity skills[1].

In our effort on engaging with the stakeholders and collect input and feedback on our different activities, Task 3.4 wrote a blogpost Let's talk about Education in cyber[2] and promoted it on social media.

As during the year Task 3.4 made public several Education-related content, we considered important to improve the user experience on the CONCORDIA website and help them faster retrieve specific papers. Consequently, we grouped all this content under a dedicated section called News and Reports on Education[3]. Besides, tagging functionality has been introduced in the various items of the website so that the education-related items can be easily filtered and displayed.

For the needs of the CONCORDIA workshop on Education for Cybersecurity professionals[4], the respective webpages were compiled and the event was present on the project's website as well.

The content produced in the year 2020 was the subject of a Communication campaign which was deployed in September with the support of task T5.2 Communications. In view of tailoring the communication campaign, Task 3.4 defined the target audience (course providers, cybersecurity professionals, corporates), proposed content, drafted messages

[1] https://www.concordia-h2020.eu/concordia-service-cybersecurity-skills/
[2] https://www.concordia-h2020.eu/blog-post/lets-talk-about-education-in-cyber/
[3] https://www.concordia-h2020.eu/concordia-news-and-reports-on-education/
[4] https://www.concordia-h2020.eu/workshops/workshop-education-2020/

and provided feedback on the visuals. The results of the communication campaign are depicted in the Figure 23 below.

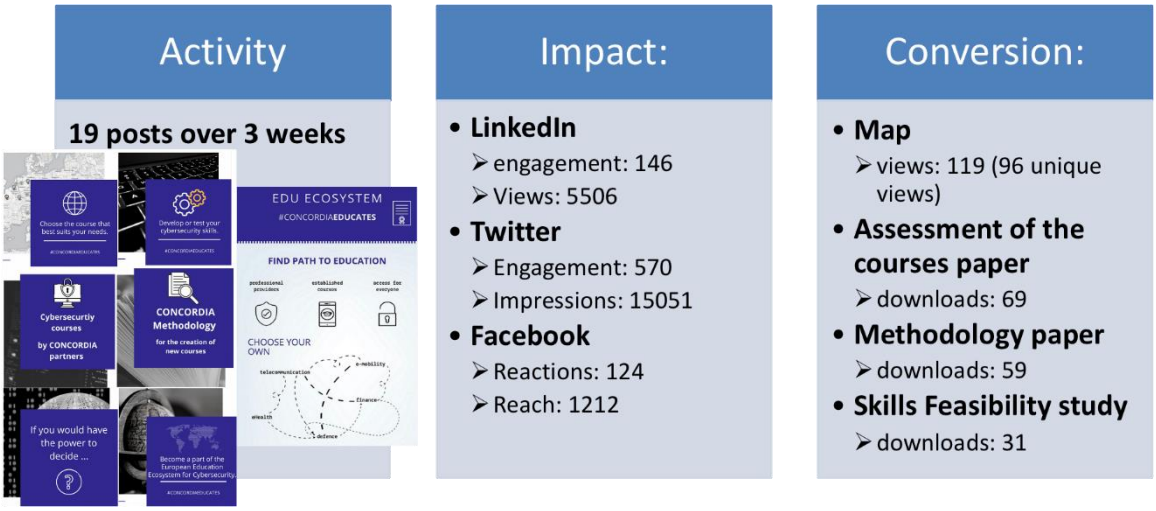


Figure 23: Structure of the Communication campaign on Education and the results

The Education for cybersecurity professionals' topic was also the subject of two sessions during the CONCORDIA Open Door COD2020. The Education track was part of day-one of the event which ran under the title EU Sovereignty and Education. As part of T3.4 contribution Task 3.4 proposed and invited the speakers of the panels, and helped draft the script of the panel. The panel discussion was recorded and can be viewed via the **link**[1]. The second session covered the specific offer CONCORDIA has for cybersecurity professionals.

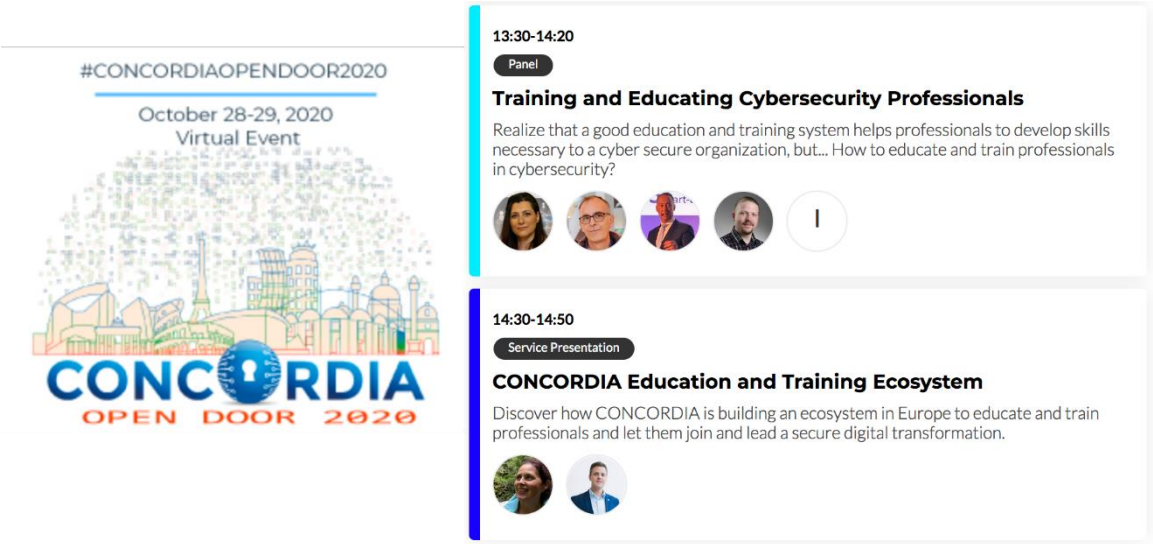


Figure 24: Content of the Education track during COD2020

5.4 Outlook Y3

In Year 3 (2021) we will continue updating courses map by (a) collecting the 2021 related dates for the already displayed courses and trainings, and by (b) making available new

[1] https://www.youtube.com/watch?v=MD56btIj6OQ&feature=youtu.be

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 pilot course will be used to refine the content and Task 3.4 will re-run the course, by adapting the topics to a new industry sector. Task 3.4 also plans to finalize running the pilot on Skills Certification for Cybersecurity Consultant by deploying the certification exams both the theoretical one and the practical one.

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

The work on CCN Education inter-pilots' group will continue with running the four strands in parallel. Beginning of the year 2021, since all the pilot projects will be delivering their work performed in the first two years of the project, a new assessment meeting will be organized in order to refine the different elements subject to collaboration, and agree on the new timeline.

6 Community building, support and incentive models (T3.5)

6.1 Task objective

Task 3.5 has two objectives. The first is related to early stage start-ups and services that CONCORDIA could deliver to these stakeholders, including support for the creation of future start-ups. The second objective of the task is to investigate motivations and evaluate incentive models for data sharing. At the end of the first year, important synergies with the other tasks have been detected, and the process of merging task T3.5 with T5.1 has been started in year 2. As of 30th of November 2020 task T3.5 is part of task T5.1. In the task T5.1 other stakeholders, which are relevant for the cybersecurity startup ecosystem (incubators, accelerators, venture capital), have been contacted and asked for collaboration with CONCORDIA. As of 30.11.2020 two communities previously separated (star-ups from T3.5 and incubator/accelerator community from T5.1) will jointly contribute towards the CONCORDIA overall project objective.

The second part of this task, namely analysis of incentives and motivations for data sharing, started in year 2, since its objective was depending on interim results and collaboration from the other tasks, namely pilots from WP2, tasks T3.1, T3.2, T3.3 and T4.2. Task objective is focused on incentives and motivations in threat intelligence data sharing, but inputs for data sharing incentives in general, as well as other information (e.g., motivational theory) are also considered to be in the scope and relevant for the objective.

6.2 Status

In Y1, we developed a first description of the concept “startup factory” and did so-called “start-up scouting”, mainly through personal contacts or by visiting cybersecurity start-up events. Start-ups have been invited to join CONCORDIA startup community in order to share their experience, but also to receive support for networking, visibility etc. Year 2

started with the launch of "Pan-European Cybersecurity Start-up Community (PECS-UP)" mailing list and a new person was hired to manage interactions with community members.

Quarterly newsletters, that have been already used in year 1 for communication about start-up funding opportunities, have received a new more attractive look and feel, with additional content such as interviews, best experience sharing etc. During year 2, besides four newsletters, so-called "flash news" format has also been used in order to communicate opportunities or news with fast approaching deadlines.

Besides Atos, other partners got involved in startup scouting for CONCORDIA PECS-UP community. University of Maribor, for example, has participated at PODIM conference for startups in the CEE region to collect data on active startups in Cybersecurity in that region. Telefonica, from task T5.1, was coordinating communication with incubators and investors, in preparation of merging two communities, that will happen in year 3.

Startup scouting was continued, as well as attendance (now online due to COVID) and dissemination at events related to start-ups, such as ECSO investors day or South Summit. The main event was, however, the CONCORDIA Open Door 2020, where panel session has been organized to discuss roles of startups and SMEs in relation to the future European Cybersecurity Competence Center and Network (see also annex).

Besides the organisation of this session, which is done in collaboration with T4.6, interactions with the other tasks also took place. In relation to the entrepreneurship, a review of methodology in T3.4 was done, while contacts with certain curricula, such as EIT Digital Master School[1], are maintained. In collaboration with T4.5, workshop focused on women in entrepreneurship was organised, while input for the roadmap was delivered to T4.4.

The second part of task T3.5, related to data sharing incentives, started with analysis of internal inputs (coming from T3.1, T3.2, and the WP2 pilots) in parallel with study of external literature.

Specific emphasis was on issues to consider and lessons learned from tasks T3.1 and T3.2. After the initial data gathering and e-mail exchange within WP3, participants from the other work packages have been contacted and a cross-WP task force was established to discuss possible directions for incentivization. The summary of finding after the first online meeting is presented in the annex.

[1] https://masterschool.eitdigital.eu/programmes/sap/

6.3 Key achievements Y2

There are four main achievements related to the start-up factory objective of T3.5:

- Establishment of PECS-UP community
- Organization of start-up panel at COD2020
- Contribution to ECSO letter of intent about the creation of funds for cybersecurity start-ups
- Publishing of several articles, interviews and blogs (see in the annex Quarterly Newsletter nr 4/2020 as an example)

In regard to external collaboration with ECSO, it is worth to mention that after the first-year cooperation on Cyber investor events, in the second year we continued with mutual support. Their activities on matchmaking between start-ups and investors have now also been used as a platform to promote more general investments in European cybersecurity start-ups and SMES. The letter of support for cybersecurity investment platform was prepared and distributed to stakeholders, with the purpose of creating a strong, competitive European cybersecurity ecosystem. The same initiative was also presented at the COD2020 event, where we organized panel session, that besides the ECSO initiative, brought an overview of different perspectives from a start-up that belongs to PECS-UP community, from a consulting company that elaborates cybersecurity startup radar, and from academic world linked to student entrepreneurship support.

When it comes to dissemination and newsletters, several articles and interviews have been done about best practices, as well as about specific cybersecurity technologies by and for start-ups.

The concept of a "startup factory", that has been developed in the first year, has been presented to several incubator and accelerator organisations that are contacted as a part of task T5.1. This vision is fully in line with message delivered to ECSO about need for the sustainable path to accompany researchers from starting their company, all the way to scale up and exit, always in the context of Europe's cybersecurity posture, including currently hot topics such as strategic digital sovereignty.

Although Europe has several cybersecurity regional hubs, and there are even specialised cybersecurity incubators or venture funds, go-to-market and product development capabilities of the local start-ups might remain limited compared to their global competitors, due to the fragmentation and difficulty to reach large clients elsewhere.

As it was already stated in year 1, solving finance issues does not solve all the problems for the startups. Investments from seed funds, for example, do not bring references and is not a guarantee for the solution deployment. Customers do not trust some existing references that come from research or innovation projects and often ask for references from the operational environment with customers that are like them in terms of size and market segment. In year 2 we supported the creation of synergies in relevant R&D&I funding schemes across Europe to facilitate a smoother access-to-market for start-ups and this concept will be further developed in year 3, maybe as a sort of "sandbox" scheme where start-ups, but also SMEs, could try cybersecurity solutions, but also let the others try solutions they might have.

Besides these key findings, we continued developing business support services for startups, addressing specific business model challenges, including cybersecurity startup value networks.

The second objective of T3.5, data sharing incentive and motivation analysis key achievements are related to analysis of literature, in parallel to analysis of lessons learned from CONCORDIA pilots and tasks with shared infrastructures (T3.1 and T3.2). This was complemented with discussion about the previous experiences (positive and negative) of partners in data sharing communities. Conclusions have been presented on October 14th to 15 CONCORDIA partners from different pilots and work packages. In addition, the preliminary work on typology, dynamics and stakeholders has been drafted in order to define context of data sharing (CoDS), as well as mapping of this context on motivation (e.g., trust, maturity etc).

As a result, relevant issues are clustered around several main areas or pillars:

- Expectations, where survey has been launched to understand and prioritize expectations of data sharing scheme participants.
- Trust, where trust scaling emerged as a primary challenge, although other elements of trust were also discussed.
- Governance, with legal issues and community organisation being highlighted as topics for the future.
- Platform and working methods, with some features and functionalities, e.g., automation or enrichment of IoC, being discussed in terms of their motivational value.
- Gamification and awards.

Finally, CONCORDIA stand on incentives for data sharing was also mentioned in World Economic Forum Report Cyber Information Sharing: Building Collective Security, from October 2020.

6.4 Outlook Y3

At the time of submission of this deliverable, the contract amendment has been signed, resulting in the task T3.5 merge with T5.1. This means that year 3 activities will target a wider type of stakeholders, with more involvement from venture capitals, incubators and others. We will also try to involve more mature startups and SMEs in the community that has been established in T3.5.

Merge with T5.1 will also affect the second objective, namely data sharing incentive analysis. We expect to start work on underlying economic or motivational theories, some of which have been mentioned by partners (e.g., two-sided markets, network effects, ecosystem value stream). In addition to these theories (that will also foster collaboration between new T5.1 and the task on economic of security), the work will start on incentivization strategy that might be suitable for CONCORDIA long term objectives (cross-sectorial and pan European data sharing).

As for the individual pillars that have been identified in the study (see annex), we expect to progress further with

- Expectation management, by increasing awareness and linking it to labelling and tagging activities.
- Trust scaling, with study of S3 model and experiences from T3.1 and T3.2.
- Governance, with legal analysis.
- Platform and working methods, that will be validated with satisfaction survey.
- Gamification and awards, to be proposed for piloting.

7 Conclusions and Outlook

As a community building and sustainability activity, WP3 has fully met its objectives for Year 2 and proactively explored enhancements beyond the baseline activities scoped in the DoA. All WP3 activities are currently on track and all tasks have outlined their Y3 work.

8 References

[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

Annex A: CONCORDIA Methodology for the creation and deployment of new courses and/or teaching materials for cybersecurity professionals (T3.4)

Executive Summary

Nowadays cybersecurity is not only a trending issue but also a very dynamic one. Under the light of many cybersecurity attacks that have caused havoc at European and International level and produced considerable damages, it became evident that cybersecurity shifted from an IT and operational matter only towards a business risk which needs to be continuously monitored and properly addressed.

The Assessment of the EU's educational portfolio for professionals including the CONCORDIA ones revealed heterogeneity both on the cybersecurity jobs market and on the cybersecurity courses offer. There is a variety of courses but not necessarily industry-specific, especially the ones addressed to middle managers and executives, the main audience we are targeting. Besides, they cover mainly academic and technical knowledge and to lesser extent business aspects and hands-on components for which the industry actors are interested in. The existing courses lack consistency in addressing a competence framework and a career path in their design thus making the effort of the individuals to choose the right course to cover their professional needs difficult. These findings were later confirmed by the ENISA report Cybersecurity Skills Development in the EU which "found that there are several issues affecting cybersecurity education, which include the lack of cybersecurity educators, poor interaction with the industry, little understanding of the labor market, outdated or unrealistic platforms in education environments and difficulties in keeping pace with the outside world."

The Methodology proposed in this document aims at addressing these gaps by considering the actual needs of both the industry impacted by cybersecurity (e.g. Telecom, eHealth, Transport, Defence) and the industry professionals. It is aimed at complementing the existing ENISA Good Practice Guide on Training Methodologies.

The document is structured in three chapters:
Chapter 1. provides an overview of the CONCORDIA findings so far with respect to the courses already offered by the consortium partners to the different categories of cybersecurity professionals, and the outcome of the CONCORDIA Feasibility study on existing Certification Schemes for skills. The conclusions of these analyses are used to tailor the Methodology to the specificity of the cybersecurity domain.
Chapter 2. describes the process for designing and deploying a course while also describing its different steps and proposing a timeline for the process implementation.
Chapter 3. starts with introducing the topics of the Methodology. As these elements are sometimes specific to one step of the process but most of the time-relevant to more than one of them, the chapter continues with mapping the Methodology topics against the process' steps. It gets afterwards into the details of the Methodology topics by providing for each individual topics a rationale, a "How-to" non exhaustive guidance on its implementation, and an Example box pointing to a concrete case and/or providing useful links and suggestions. The document ends with a checklist summarizing the elements of the Methodology and could be used as a support for course providers in their work of developing new content.

LINK to the document: https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf

Annex B: Workshop on Education for cybersecurity professionals -post workshop report - (T3.4)

Executive summary:

The work described within this document is mainly built around the outcomes of the different hands-on exercises. It reflects the efforts invested by the project team in (1) the determination of the Role Profile of the Cybersecurity Consultant and in (2) the definition of the content for previously defined Learning Objectives for the implementation of the relevant course, tailored per industries.

The project team faced the following challenges before the implementation of this workshop:
1) The Role of the Cybersecurity Consultant has been internationally identified but there is a lack of a concrete definition of the profile in all identified frameworks. To overcome this problem the project team had (though various processes) derived a proposal, which needed to be validated by the market.
2) In order to construct an effective and relevant to the market training course, it is of paramount importance to determine the Learning Objectives, the content to be covered considering the chosen Role Profile, and their variation between the different industries (the CONCORDIA project focuses on Telecom, Finance, eHealth, Defense, Transport). The project team had already determined a definition of the Learning Objectives (Threats, Technology, Economics & Business) but needed the different opinions of industry representatives with respect to the main content to be offered for the specific Role of the Cybersecurity Consultant in terms of knowledge and skills, ranked for each industry.

The implementation of the workshop produced the following results respectively:
1) The proposed 200 Knowledge and 90 Skills were validated and filtered down. The results of the workshop provided a ranking of the Knowledge and skills. By filtering the ranking results and further processing, the new Role Profile of the Cybersecurity Consultant was derived. The Role Profile is expressed in two different formats (based on the EU e-CF and based on the US NICE framework). The Role profile (EU e-CF) contains 13 Tasks and 15 e-competencies. The competences cover all five e-CF areas although there only one identified e-competence from the Run area, while all others are mostly balanced between the rest of the areas. This validates also the Mission of the Cybersecurity Consultant - providing advisory and technical expertise to help the client organizations design, implement, operate, control, maintain and improve their cybersecurity controls and operations.
2) The top 20 knowledge and top 10 skills per Learning Objective were further filtered down with respect to their relevance to specific CONCORDIA related industries. Looking into the results collected per Learning Objective, and with a specific focus on Telecom industry (the subject of the first pilot course) we have come to the following conclusions:

a) Learning Objective 1-Threats: the outcome of the workshop underline i) the need of basics knowledges on threats, vulnerabilities and CIA triad in connection to risk assessment and ii) the skills to apply such basic knowledges for an effective creation of security policies and risk evaluation to anticipate threats and mitigate risks. The workshop also underlined the importance of communicating the threats to the management board and identify and apply countermeasures based on basics knowledges on how a cyber-attack take place.

b) Learning Objective 2-Technology: the workshop points out the importance of mastering the networking environment and the components to be protected, as well as acquiring knowledge and skills related to security management in terms of both assessment and configuration. The overall technology ranking highlights big data, internet-of-things, and artificial intelligence as major topics of interest, followed by mobile devices and cloud computing. This is in phase with the current evolution of the Internet which can be seen as a great integration platform for interconnecting multiple and heterogeneous entities, from connected devices to data center resources, and building complex and value-added secure systems.

c) Learning Objective 3-Economics and Business: the analysis of the knowledge and skills selected indicates a high importance of abilities to understand not only cybersecurity main concepts and trends (for both vulnerabilities and protections) but also regulations and laws that impacts on the business and its operation. Thus, an in-depth understanding of the organization environment, processes, and exposed threats is critical to provide an effective analysis related to the economic impacts of cybersecurity on that. The project team will use the resulting Role of the Cybersecurity Consultant to develop courses targeting this profile -tailored for the needs of specific industries, and to pilot the CONCORDIA Cybersecurity skills certification framework. The pilot on certification is expected to be tried out after the implementation of the relevant CONCORDIA pilot training course, in Q42020.

LINK to the document: https://www.concordia-h2020.eu/wp-content/uploads/2020/07/CONCORDIAWorkshoponEducation2020-forpublication.pdf

Annex C: The Syllabus for the course targeting Cybersecurity Consultant profile and the Mapping of the Knowledge and skills against learning objectives and syllabus modules -(T3.4)

Module	Lesson code	Lesson title
A - CYBERSECURITY PRINCIPLES	A1	CIA Triad and Security Principles
	A2	Threat Weaknesses and Vulnerabilities
	A3	Privacy Principles to Manage Risks Related to Data
	A4	Accountability as success factor in this Digital Age Services,NFV, SDN, Mobile Devices
B -OFFENSIVE METHODS	B1	Attacks Capabilities and Attacks Stages
	B2	Emerging Security Issues and Evolving Attacks
	B3	Network Attacks: Scanning, DDoS, DNS, etc.
	B4	Internet Technologies: Definition, Principles and Top Threats
C - DEFENSIVE METHODS	C1	The Security by design Principle Approaches and Paradigms
	C2	Vulnerability Management Methods scanning)
	C3	Lessons on Network Protections Methods: Monitoring, firewalling, IDS/IPS, SIEM, VPN
	C4	Lessons on Application/OS Protections Methods: Antivirus, access control
	C5	Data Protection and Security
	C6	The SIM Approach
D - RISK MANAGEMENT	D1	Lessons on Risks: Risk Assessment and Threat Modelling
	D2	Risk Management with an Economic Bias ransomware (SEConomy)
	D3	Non-conformity/non compliance perspectives
	D4	Digital Sovereignity

			A - CYBERSECURITY PRINCIPLES				B -OFFENSIVE METHODS				C - DEFENSIVE METHODS						D - RISK MANAGEMENT			
		Description	A1	A2	A3	A4	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	D1	D2	D3	D4
LO1 - Threats	LO1-K1	Knowledge of cyber threats and vulnerabilities.		y		y														
	LO1-K2	Knowledge of confidentiality, integrity, and availability principles.	y			y														
	LO1-K3	Knowledge of emerging security issues, risks, and vulnerabilities.				y		y								y	y			
	LO1-K4.	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.			y	y										y				y
	LO1-K5.	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)				y	y													
	LO1-S2	Skill in applying confidentiality, integrity, and availability principles.									y									
	LO1-S3	Skill in assessing security systems designs.									y									
	LO1-S3	Skill in evaluating the adequacy of security designs.									y									
	LO1-S4.	Skill to anticipate new security threats.						y												
LO2 - Technology	LO2-K1.	Knowledge of computer networking concepts and protocols, and network security methodologies.							y											
	LO2-K2.	Knowledge of network security architecture concepts including topology, protocols, components, and principles.											y							
	LO2-K3.	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.										y								
	LO2-K4.	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).				y							y	y						
	LO2-K5	Knowledge of current and emerging cyber technologies.								y										
	LO2-S2	Skill in applying confidentiality, integrity, and availability principles.	y																	
	LO2-S3	Skill in creating policies that reflect system security objectives.											y							y
	LO2-S3	Skill in designing countermeasures to identified security risks.											y	y		y				
	LO2-S4.	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.											y	y						
LO3 - Economics & Business	LO3-K1.	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations													y					
	LO3-K2	Knowledge of emerging security issues, risks, and vulnerabilities.										y				y	y			
	LO3-K3.	Knowledge of integrating the organization's goals and objectives into the architecture.																y	y	y
	LO3-K4.	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.								y										
	LO3-K5	Knowledge of risk/threat assessment.				y										y	y			y
	LO3-K6.	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy																		y
	LO3-S2	Skill in conducting capabilities and requirements analysis.															y			
	LO3-S3	Skill in performing impact/risk assessments.															y			y
	LO3-S3	Skill to anticipate new security threats.											y	y						
	LO3-S4.	Skill to use critical thinking to analyze organizational patterns and relationships.															y		y	y
	LO3-S5.	Skill to understand the operational, financial and policy related parameters re. the effective implementation of cybersecurity in practice.																	y	y

Annex D: Creating a Role Profile – Cybersecurity Consultant (T3.4)

Executive summary:

This paper is part of the CONCORDIA effort in developing a cybersecurity skills certification framework for cybersecurity professionals. The activity ran under the task T3.4 in strong collaboration with task T5.3.

The first step of the process was to conduct a Feasibility study for a Cybersecurity Skills Certification Scheme[1]. The Feasibility study comprised of an analysis of the relevant existing Role Profiles, frameworks and certification schemes and aimed to identify possible gaps. The analysis showed that there are Profile Roles covered through a multitude of Certification Schemes (e.g. the ICT Security Technician) whereas others that are not directly connected to any Certification Scheme (e.g. the ICT Security Consultant).

The aim of the activities described in this document was to help select one of the profiles not directly connected to any Certification Scheme and create the Role Profile (in at least two of the existing Skills Frameworks – European and NICE), so that it may be piloted as part of the CONCORDIA training courses and Skills certification framework. The Cybersecurity Consultant Role Profile was the one developed in this respect.

LINK to the document: http://concordia-h2020.eu/other_files/concordia-Cybersecurity%20Consultant_v0.5.2.pdf

[1] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf

Annex E: Data sharing motivation and incentives (T3.5)

This annex is an executive summary of activities related to analysis of data sharing motivations and incentives, belonging to the task T3.5. Full report is an internal document circulated among contributing partners.

Methodology

In this part of task T3.5, which is dedicated to analysis of incentives and motivations for data and information sharing, we followed the methodology depicted below.

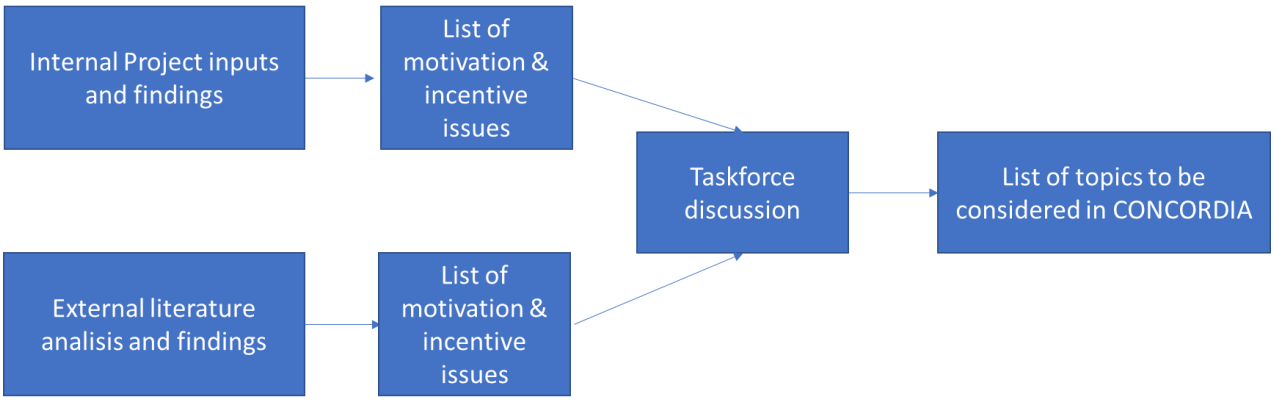


Figure 1: Methodology followed in data sharing incentive and motivation assessment

One of the relative constraints is that, as a part of task T3.5, incentive and motivation assessment activities are partially detached from tasks where data and information sharing happens. There was a risk that this would limit the participation and commitment of stakeholders, but thanks to the creation of cross-WP taskforce, a joint assessment has been performed. Nevertheless, we expect that the future merge of T3.5 and T5.1 (exploitation task) will improve participation and enhance results of the assessment.

External inputs and literature review

Several papers, published by ENISA, ECSO and other stakeholders, have been analyzed in order to obtain insight about different models, context and status of data sharing in general, covering a variety of communities, including CERT/CSIRT, ISAC or MISP-based threat intelligence sharing communities. Very few of these papers have explicit analyses or benchmarking of incentives and motivational elements, but nevertheless, a summary has been prepared and provided to interested participants of CONCORDIA.
ENISA published a report on good practices and recommendations related to ISAC, including the guide to Incentives and Barriers to Information Sharing [1]. According to that study, the most important is economic incentives stemming from cost savings and those stemming from the quality, value, and use of information shared, while main barriers are poor quality of information, misaligned economic incentives stemming from reputational risks and poor management. Besides the survey on motivational factors among private and public sector participants, ENISA also structures the context of data sharing among three main pillars.

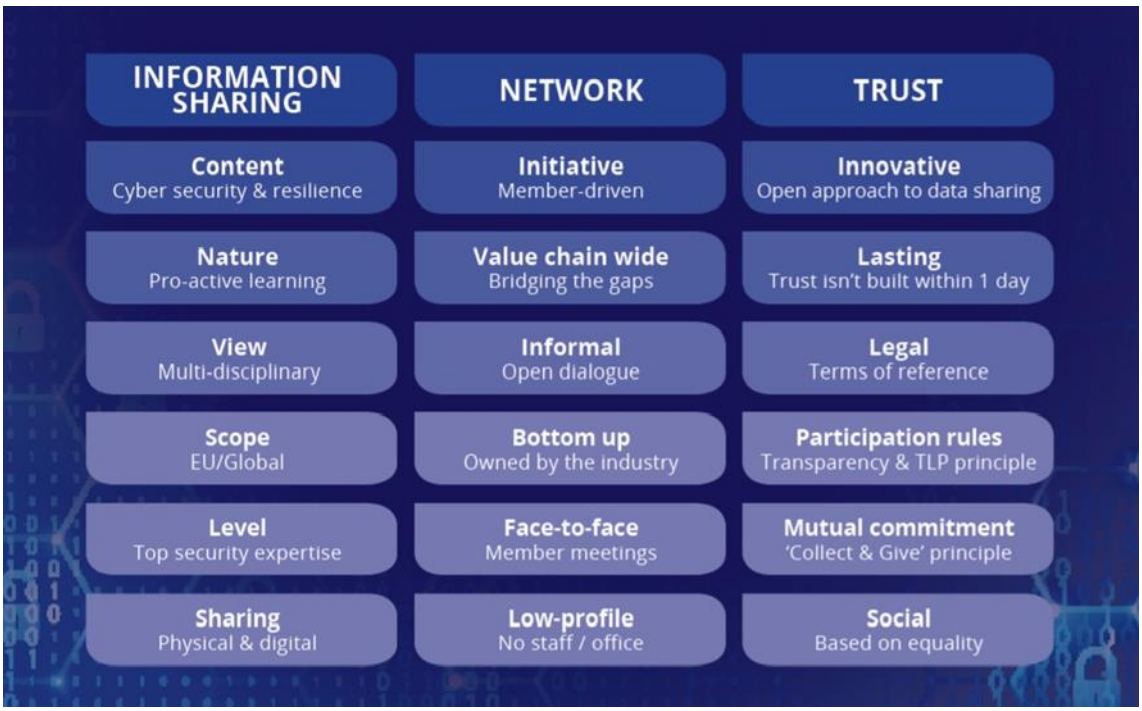


Figure 2: Relevant issues for the context of data sharing (Source: ENISA)

Information Sharing and Analysis Centres (ISACs) is **collaboration community** created for sector-specific national or international information sharing, and in another ENISA report [2] there are additional challenges, and best practices related to data sharing in these types of communities, especially when it comes to private sector stakeholders. **Incentives such as leadership positions for the private sector, or participation in steering committees** are a mentioned there, while differences related to cultural issues among Member States, regulatory requirement, or economic and social interests are also listed.

Several recommendations were also made by ECSO in their "Position paper of sector-specific ISAC" [3]. Building trust by "terms of reference and code of conduct" was described not to be enough. ECSO position was that ISAC should not impose any mandatory information sharing.

On June 29th we attended EU-ISAC event[1] that also provided some guidelines and best practices. Co-organised by the European Commission (DG Connect) and ENISA, this first EU-ISAC conference was also an opportunity to learn from practitioners from different EU member states. One of the speakers divided information sharing context around information structure and information management, which is a mix of platform functionalities and procedures.

We identified further distinctions between supplier-driven (where data sharing is encouraged from supply to demand side of cybersecurity), demand-driven (where consumer requests and drives data sharing) and facilitator-driven data sharing (where participants are prosumers and co-creation happens from both sides equally). In this respect CONCORDIA objective, in the long run, is to create a mixed model with cross-sectorial data sharing which would probably be a hybrid type that combines different community types.

Supply-side driven and private communities (including SOC – security operation centers) are left out of scope in this report. According to one stakeholder from the financial sector, some of these communities are trying to incentivize participation by a possibility "to combine a top-down approach arising from regulations and market trends, with a

[1] https://ec.europa.eu/digital-single-market/en/news/eu-isacs-conference-2020

collaborative one based on real experience and best practices" and in this way reduce the burden of reporting.

Closer to CONCORDIA pilots and exploitable results, threat intelligence sharing communities are focused on information that might help an organization protect itself against a threat or detect the activities of an actor. Data and information shared or exchanged include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.

In MISP Open Communities[1], for example, it is mentioned that each TI community might have specific rules to join them. Some of these existing public communities might be interconnected and some might be in an island mode. In MISP Information Sharing Maturity Model[2], there is a focus on understanding the maturity and capabilities of an organization and to have incentives to contribute more. Another incentive-oriented effort is gamification through MISP-Dashboard, an experimental feature upon which organizations compete by contributing intel within their sharing group. MISP-Dashboard is currently in alpha stage[3].

We have also reviewed several EU and non-EU initiatives that look more closely at motivational factors when it comes to the context of data sharing. This includes DISIEM, X-ISAC, PISEX projects, as well as publicly available articles or surveys ([4], [5], [6], [7], [8], [9]). They all contain some ideas on how to modify the behavior of actors to improve voluntary sharing. One of the key issues that emerges is expectation management. Among expectation parameters are reciprocity, value, institutional design and reputation. Discussion on quality and quantity of data and information that has been shared, and it should influence the trust score is one of the frequent topics.

NIST Special Publication 800-150 [10] is segregating incentives per phase of data sharing: engaging in ongoing communication, consuming and responding to security alerts, automation, consumption and use indicators, organization and storage of indicators and finally production and publishing of indicators.

Finally, we reviewed another line of research, dedicated to gamification and similar user interface-oriented approaches. Systematic study on human-computer interaction in data sharing has been done in paper [11], which also makes a distinction between incentives for junior and senior security analysts. Senior-level interviewees perceived lack of adequate sharing policies as the major obstacle for effective sharing, while less experienced analysts welcomed their incentives, such as badges or awards for sharing but may not always fully understand what they are sharing. They explored cross-organizational aspects of badges and user profiles, so it might be an interesting direction for CONCORDIA as well, with the ambition to become cross-sectorial threat intelligence sharing platform.

After the analysis of findings from the literature, that includes external suggestions and experiments, we suggested several clusters with relevant issues that should be further explored and compared to internal project findings:

1) Expectations:
- Sharing will be reciprocated,
- Information received from the transaction partner will be valuable,
- Sharing will be facilitated by an effective tool, procedures and policies
- Sharing will be beneficial for the reputation of the organization and the person

2) Trust:
- Background of community members
- Transparent scope and objectives of sharing

[1] https://www.misp-project.org/communities/
[2] https://www.misp-project.org/2017/01/16/Information-Sharing-Maturity-Model.html
[3] https://vvx7.io/posts/2019/07/misp-gamification-in-cyber-threat-intelligence/

- Privacy and data protection
- Use of trusted broker or similar intermediator

3) Platform and working methods
- Communication and data sharing policies or rules
- Tool usability
- Tool effectiveness
- Tool performance and security
- Support services, including administration, maintenance etc

4) Governance and operation
- Internal staff of platform operator
- Legal provisions
- Financial model, incl fee for participation in the community
- Topology of community (hub and spoke, source-subscribe, separated circles of trust, distributed vs central etc)
- Built-in explicit incentives (e.g. skill-based digital seal, community contributions award, scoring system with table, label or tag)

Internal inputs and discussions

In the first year of CONCORDIA project several data and information sharing related efforts have been done, foremost in T3.1 and T3.2. In T3.1, for example, an open-source MISP (Malware Information and threat Sharing Platform) instance has been deployed at DFN-CERT (managed cooperatively by Siemens AG and DFN-CERT) and was made available for CONCORDIA participants that started testing in Nov 2019 prior to official roll-out phase in 2020. Although this testing focus was not on incentives for data sharing, using specific "sharing groups" (e.g., info visibility only to telcos, banks, etc.) was also scheduled. Task T3.2 produced draft data sharing agreement for pilot phase 1. In this data sharing pilot, which is the part of the wider concept of "anti-DDoS coalition", some lessons learned on motivation and incentives were already available in the first year. Early in the second-year demos for the EC review have been prepared with an update of the cookbook, written in a series of blogs[1].

The concept of the Dutch Anti-DDoS Coalition and the status of one of its pillars, the DDoS clearing house is described, together with lessons learned. One input for motivational factors and incentive scheme is **trust scaling**.

Clearing house started with ten partners and this small facilitated the development of mutual trust, for instance through frequent face-to-face meetings. Group opted for unanimous decision-making in their initial "**governance model**", which was formalized as part of the data-sharing agreement - DSA). This DSA was also posted on CONCORDIA internal website and due to its simplicity can be considered as one of "incentives" to join this community.

Other motivational factors and incentives are likely to be needed, in order to scale up trust (impersonal trust). This also needs to cover scaling of DSA, that besides a basic outline of legal aspects (e.g., liability, security, treatment of personal data and governance), might include more information and evolve for subsequent pilot iterations.

CONCORDIA aims at enhancing approaches to threat intelligence sharing, and different **enhancement services**, like supplementary services in task T3.2, could be considered as motivational factors, as they increase automation or replace tedious manual checks on data. One example is the framework of security metrics in order to provide quality feedback and situational awareness to the user groups, while another one is IoC (indicators of

[1] https://www.nomoreddos.org/en/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward/

compromise) enrichment, developed in a pilot in T2.1. Demo v2.2 from task T3.2 showed working basic version of supplementary services, such as a ranking mechanism to prioritize attacking hosts that are more harmful, based on their traffic delivery power.

Participation in standardization, such as the one considered in "course of actions" (or "playbooks"), that can be easily interpreted and shared within the cybersecurity community, is also considered as a motivational factor. Available standards such as the "Open Command and Control" Language (OpenC2) and newly proposed ones such as the "Collaborative Automated Course of Action Operations" (CACAO) are examples from task T3.1.

In a survey done among CONCORDIA participants, we received several additional explanations or suggestions on why to share data in general, or cybersecurity threat intelligence in particular:

- Save time: the objective would be to have near real-time information sharing
- Threat understanding e.g. identify affected platforms or systems, implement protective measures etc
- Knowledge aggregation: enhancing existing indicators, correlation etc
- Increase agility
- Awareness about other defense capabilities
- Establishing trust: it is interesting here that trust is mentioned not only as an enabler, but also as the objective of the data sharing
- Go beyond sharing, for example, in T3.2 the members of the Dutch Anti-DDoS Coalition spotted the opportunity to collaboratively simulate network and application-level DDoS attacks and practice responding to them.

During the discussion of taskforce members, it became clear that the main problem is how to efficiently achieve labeling or tagging when valuable data is shared (e.g. data that helped prevent incident) and how to assure that this eventually leads to community recognition.

When it comes to trust scaling, iterative addition of community members was experimented in task T3.2, while the use of "trusted introducer" in T3.1 was also discussed as an approach to enlarge the community. The "trusted Introducer" and ad-hoc "terms of access" refer to a couple of possibilities ICH/CCH envisioned for accessing the CONCORDIA Threat Intelligence Platform and the related services. However, this is not fully implemented yet and DFN-CERT is the only one that currently uses those to grant access to the Incident Clearing House.

The link between trust and topology of community and data sharing mechanism has been discussed. Clearing house model adopts hub and spoke model, so the role of central hub or trusted introducer is much more important than in peer to peer topology. While the formalized exchange is often based on an agreement, such as a non-disclosure agreement, legal contract, or a membership agreement, the clearance-based exchange could be considered as a special case of a formalized exchange. Trust-based groups, for example, are similar, but even more restricted and limited to closed groups of like-minded actors who inform one another on an ad hoc basis.

The publish-subscribe method for sharing threat intelligence consists of a producer who publishes information on a regular or irregular basis, and whose publications are individually subscribed by one or more community members, which is rather common in supply-driven communities. Aggregation, on the other hand, occurs when members collectively contribute to a discussion thread, for example an automated cyber threat sharing repository, to transform or create new value. One example could be the statistics framework from DFN-CERT.

When it comes to the scaling of trust, it could be worth mentioning that there is also work on the formalization of trust. The trusted introducer does this by using the "SIM3 Security Incident Management Maturity Model", built on three basic elements:
1) Maturity Parameters
2) Maturity Quadrants
3) Maturity Levels
The Parameters are the quantities that are measured in regard maturity – some forty exist and they belong to one of four categories of Parameters: O – Organisation, H – Human, T – Tools and P – Processes.
In the case of e-Health pilot of CONCORDIA, participants sent additional considerations that apply to sharing of sensitive data (patient ID data, emergency case data, patient data coming from medical equipment...). Besides trustful service providers and trust in the technology (including communication protocols, servers, 3rd party software providers...), they have to rely on trust in data related to measurements from devices, external patient identification data or trust in real-time data (emergency cases).
When it comes to data sharing policies and agreements, requirements and recommendations come from different sources. What is less clear is whether some neutral authority should be able to audit these.
In CONCORDIA task T3.1 there is a clearly established limitation, namely "Project", defined as "the collaboration between the Parties in the context of the pilot organised for the purpose described in Article 3, with a duration of six months starting from the date that this Agreement is signed, to be tacitly extended by successive periods of three months until the Project Group determines that the Project is to end". It outlines the purpose of the project, responsibilities, liability, confidentiality and access, as well as protection of personal and other data.
One of the most interesting parts of DSA deals with a governance model, which is very simple. It states that "the Parties shall hold regular governance meetings with the other Project Group members. At the governance meetings, all developments relating to the Project shall be discussed".
Voting is by unanimity, but if unanimity cannot be secured, a motion may be carried by a majority vote. At the same time, a simple majority shall be insufficient to carry a motion to amend the data-sharing agreement. While this works fine at a small scale, it is likely not enough for EU wide scale. In the future, one recommendation to the legal task in CONCORDIA or future EU cybersecurity competence center would be to study legal perspective of EU-wide data sharing, having mind experiences and models from tasks T3.1 and T3.2.
During T2.1-WP1 Workshop (virtual meeting), which was held on 27th of May 2020, several participants talked about enrichment services, such as to improve the quality and usability of the IoCs (Indicator of Compromise) by implementing an automated validation and ranking of the IoCs (pilot by TIM). Most of the time, data-sharing community participants do not have the malware sample and need to establish which are the fields that are absolutely needed for specific purposes or give clear guidelines on how to use them to store the information.
To summarize, in task T3.5 we have been looking at external sources as well as preliminary inputs from the other tasks, in order to feed the discussion on motivation and incentives for data sharing. Thanks to the collaboration between partners from different work packages and tasks, we have clustered motivational issues around the following issues:

- Trust, with a special emphasis on trust scaling
- Governance model, including data sharing agreement – DSA, legal issues etc

- Platform and its functionality, including both supplementary services (e.g. ranking, statistics from task T3.1) or enhancement services (e.g. automation, enrichment of IoC in WP2)

Other related issues, such as standardization, incentive approaches (e.g. gamification), typology of community or cultural issues have also been discussed, but the further work will focus on the above mentioned topics and will hopefully provide useful feedback to tasks that are implementing data sharing pilots.

References:

[1] ENISA, Incentives and Barriers to Information Sharing, 2010 report, accessible at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing
[2] ENISA report, Information sharing and analysis centre cooperative models, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models
[3] ECSO position paper, https://ecs-org.eu/publications
[4] W. Tounsi, What is Cyber Threat Intelligence and How is it Evolving?, Cyber-Vigilance and Digital Trust (pp.1-49), 2020 Edition: https://media.wiley.com/product_data/excerpt/81/17863044/1786304481-46.pdf
[5] Ponemon Institute LLC, Exchanging Cyber Treat Intelligence, There Has to Be a Better Way, https://www.ponemon.org/news-updates/blog/security/the-second-annual-study-on-exchanging-cyber-threat-intelligence-there-has-to-be-a-better-way.html
[6] 2020 SANS Cyber Threat Intelligence survey, https://www.sans.org/reading-room/whitepapers/threats/paper/39395
[7] A.Mermoud, S. Gernhauti, M.Matias, D. Percia, Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection, CRITIS 2016 proceedings: page 150-162
[8] A.Mermoud, S. Gernhauti, M.Matias, D. Percia, Incentives for Human Agents to Share Security Information: a Model and an Empirical Test, June 2018 Conference: 17th Workshop on the Economics of Information Security (WEIS)
[9] T. D. Wagner, E.Palomar, K. Mahbub, and A. E. Abdallah: A Novel Trust Taxonomy for Shared Cyber Threat Intelligence, June 2018, Security and Communication Networks 2018(1):1-11
[10] NIST publication, Guide to Cyber Threat Information Sharing, October 2016, https://csrc.nist.gov/publications/detail/sp/800-150/final
[11] T.Sanders and B.Hein, Usability and Incentives for Threat Information Sharing Technology, 28th Annual FIRST Conference, Seoul, Korea, June 14, 2016

Annex F: Quarterly newsletter for PECS-UP Community (T3.5)

"Pan-European Cybersecurity Start-Up Community" (PECS-UP) is a community established in task T3.5 of CONCORDIA project with a vision of bringing together different stakeholders in the cybersecurity start-up ecosystem. In 2019, before this community was formally established and specific mailing list has been enabled, Quarterly Newsletter for start-ups was distributed to all CONCORDIA partners, in order to spread further information, diffusion of best practices and matchmaking news. In 2020 this newsletter received a more formal look and feel and was distributed only to subscribers of PECS-UP community, both project partners and external entities.
While the original goal was to stay up to date with latest news, events and the future initiatives, and was implemented as a one-way communication channel, over time this quarterly newsletter was transformed into a kind of discussion forum, where many stakeholders can participate and express their opinion, publish articles or share contents.
In this annex we include the content of the last edition of Quarterly Newsletter, published on November 30th 2020, and adapted to the format of this annex.

Meet Community Members: Collider

In this newsletter, we present you the Collider, an innovation programme of Mobile World Capital Barcelona, that bridges the gap between science and market to create disruptive technology-based start-ups. They foster an entrepreneurial attitude in universities and uses the researcher – entrepreneur formula to create new high-value companies. On the other hand, Collider also actively encourage corporations to take part in the programme as well. They conduct innovation sessions to identify the main sectorial challenges and look for technologies in the local research ecosystem that can potentially help corporations. Later, they bring on board entrepreneurs that together with scientists build deep tech start-ups and launch pilots with corporate partners.
Check further details, portfolio and funding opportunities at: https://thecollider.tech/
If you want to get in touch with Collider or MWC directly please let us know.

Guest Article: Bug Hunting for and by start-ups

Bug bounty is the name given to a kind of offering given by websites, organizations and software developers by which bug hunters can receive recognition and compensation for discovering, reporting or resolving bugs before the general public is aware of them. It used to be something reserved to larger organisations, but recently there are also bug bounty programmes or platforms specialised for start-ups. RISE, for example, is a managed bug bounty program designed specifically for start-up companies and is connecting start-ups to hundreds of security researchers. RISE belongs to Safehats company, based in India, but with offices in Germany. Secuna, headquartered in Philippines, is yet another non-EU company that specialises in bug bounty for start-ups. However, many European companies are also entering bug bounty business, although they target mainly larger organisations.
The American leader HackerOne was founded in 2012 by two Dutch hackers and the ex-Head of Product Security at Facebook. It uses a network of freelance hackers who are paid from 1000 to 100.000 euros. The company is now headquartered in the U.S. where the majority of its business comes from (Verizon Media, Paypal, Airbnb, Twitter, the U.S. Department of Defence) but it is growing in Europe and Asia. Bugcrowd is another American Bug Bounty platform with a very similar model.

In Europe, the start-ups are plenty and divided by their business model : private bug bounty programs (bug hunters are selected and the program is secret) or public ones (to the whole community of bug hunters).
The Belgian Intigriti has recently announced raising €4.1 million in their Series A round, led by European based venture capital firm ETF partners. Intigriti was founded in 2016 and uses a network of 15.000 ethical hackers that serve more than 75 customers. A similar number of hackers is also used by YesWeHack platform. Launched in 2013 and raised the same amount as Intigriti two years ago they also claim to be the leader among bug bounty platforms in Europe (offices in Paris, Germany and Switzerland), they start growing in Asia with an office opened in Singapore in the last year. Their last innovation is using blockchain to improve smartly the Coordinated Vulnerability Disclosure (CVD). In January 2020, YesWeHack wrote a white paper about this topic for the European Union context. They are also using students who are trained with another bug bounty platform.
Yogosha, another French company that raised 2 million in January, is specialized in private Bug Bounty (500 shortlisted bug hunters) in Europe. They recently increased their offer in all of Europe, especially in Germany and Spain.
The Dutch Zerocopter is another European bug bounty platform with 3 000 hackers. Among newcomers, we can mention Hackrate from Hungary, which is listed in EU start-up directory and is looking for the investment to further develop their platform. CazHack is an example of new platform active in Spain.
Hype or not, bug bounties program are an interesting option to complement the internal testing process, while incentivizing ethical hackers to report bugs and issues and get paid for their work. Crowdsourcing of pen testing is considered as a long-term innovation in the existing cybersecurity processes.
This article has been co-written with Louise Bautista.

After the first experience in Capgemini consulting group, Louise Bautista worked as an account executive for YesWeHack, the European Bug Bounty platform. She is working now for VPN client software company, TheGreenBow. She is also Secretary general of the non-profit organization: the French club of Cryptocurrency and founder of its delegation in Malta. Louise wrote many articles about cybersecurity, blockchain and innovation for Cryptonaute, Harvard Business Review France, Security and Defence magazine. Louise will be also speaking at CONCORDIA Woman in Cybersecurity webinar dedicated to entrepreneurship, scheduled for December 14th at 16.30. More details in EVENTS section.

Event Report: From COD to COD

The CONCORDIA project runs an annual event called CONCORDIA Open Door (COD) that is used as an enabler of an open and constructive dialogue about the whole spectrum of cybersecurity, from research to technology, from legal to business, but also to collect important feedback about what can the community expect and offers to the future European Cybersecurity Competence Centre. This dialogue conclusions and the feedback that is received is then used to align CONCORDIA activities with the needs of a wider cybersecurity community.

COD2019 was held at Hotel Parc Alvisse, Luxembourg on the 16th and 17th of October 2019 with around 100 participants. During this first edition of COD event, ID Quantique, one of the members of PECS-UP community, presented their work on quantum key distribution (QKD) systems, quantum-safe network encryption, and hardware random number generators. This Swiss company, founded as a spin-off of the Group of Applied Physics at the University of Geneva, also gave insights in best practice collaboration between small and large enterprises.
For those that are interested in this topic, we recommend recently published white paper on "How quantum technologies are helping to secure our digital future".
Link: https://www.idquantique.com/landing-page/the-quantum-revolution/
This year, CONCORDIA Open Door event 2020 was a virtual event due to the circumstances related to COVID-19. It was held on 28th and 29th of October 2020 and included two-panel sessions related to start-ups and SMEs, namely "Startups, SMEs, and the future European Cybersecurity Competence Center and Network" and "Big vs Small Industries: Approach to Cybersecurity".
Before the first panel session, there was a keynote presentation from Maria Lundquist, from the European Investment Bank (EIB), about the ecosystem provided by EIB in the context of cybersecurity. This institution is helping start-ups and SMEs to overcome barriers and funding gaps that correspond to "valleys of death", as they are known in innovation management and growth strategies. Maria also presented Cybersecurity Related Investment Estimation method, a kind of methodology to estimate values of investment that go into cybersecurity, when it is difficult to separate it from the other IT investments. Finally, she also briefly mentioned InnovFin funds, such as AI and Blockchain fund, and several projects that they selected for financing.
Panel session started with an introduction about pooling Europe's Cybersecurity expertise and implementing European Cybersecurity Competence Centre and Network. The first panellist Jean Diederich (Wavestone) gave an overview of the current cybersecurity start-up landscape and mentioned that there are segments, such as cloud security, which not currently addressed by start-ups. José Ruiz Gualda from jtsec and CONCORDIA PECS-UP start-up community was stressing the importance to choose the best solution in EU, overcoming fragmentation and support of "national start-up champions". Victoria Villanyi from ELTE addressed entrepreneurship gap, and made a link to the cultural factors, while Danilo D´Elia from ECSO presented several new initiatives started in this organisation, such as cybersecurity start-up award and letter of intent to start a dialogue on creation of Pan-European cybersecurity specific investment fund.
The challenge is, all panellists agree, on how to coordinate what is useful for EU in emerging start-up landscape (e.g. which are strategic segments), how to move from proof of concept to the next stage that involves real operational deployment, as well as how to keep start-ups in Europe, after the initial success. The conclusion of the panel is that, besides addressing already mentioned and well-known gaps (funding, growth, territorial and educational differences), EU needs also to foster quality and not quantity in the cybersecurity start-up ecosystem.

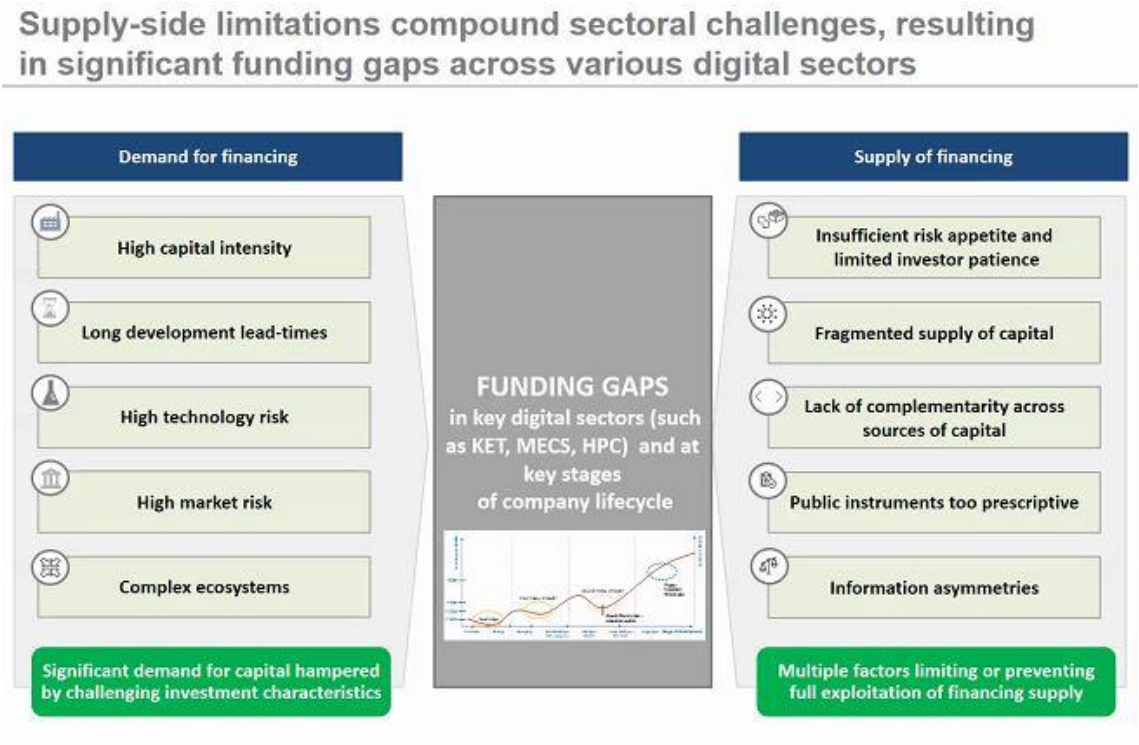


Figure 1: Gaps in start-ups financing (from EIB presentation at COD 2020 event)

The second start-up and SME panel was named "Big vs Small Industries: Approach to Cybersecurity" and it was focusing on a better understanding of how the European start-ups, SMEs and large enterprises are approaching the cybersecurity challenges. Despite a growing interest in cybersecurity, in 2020, a vast majority of start-ups and SMEs stakeholders are not aware of the impact of cyber breaches and threats on their businesses. This was confirmed by independent statistics as brought forward by the panel guests Georgiana Ghiciuc from Beaglecat and Christopher Richard from United Biometrics. Panellists also mentioned some other challenges, such as low cybersecurity budgets. The SMEs decision-makers are considering cybersecurity as an IT issue rather than an organisational governance issue and consequently they are setting-up smaller budgets compared with the real needs. These challenges are also encountered by the large corporations, but at a different scale as the representative of a large enterprise, Frank Schubert from Airbus, confirmed.
The second panel concluded that there is still a strong need to further encourage the actions and impact of joint cybersecurity initiatives such as CONCORDIA project, where different stakeholder, small and big, work together.

Featured Article: How does large organisation relate to start-ups?

Wait! Before going to "how" we should explain "why". Large organisations sometimes have problems in reorientation, transformation or revitalization of its product and service portfolio. Investing in or collaborating with a start-up company, that executes parts of the strategy not possible to execute in the large firm, could be a viable option, used by many large organisations.
Besides this motivation that can be described as "one strategy, different tactics", there is also more traditional motivation, such as staying ahead of competition, even if this is done through adjacent start-up. Operational level activities include start-up scouting, monitoring of windows of opportunity etc.

Mind the Bridge, together with Nesta, annually elaborates the "Europe's Corporate Start-up Stars", a ranking of more 'start-up-friendly' corporates in Europe. Telefonica, for example, which is one of CONCORDIA partners, was praised for inversion in cybersecurity, among other into companies such as Countercraft and Imbox. While Telefonica is famous for its Wayra innovation hub and accelerator, there are other ways to invest or collaborate with start-ups, including direct or indirect corporate venture. Sapphire, for example, was formerly known as SAP Ventures but rebranded as Sapphire in 2014, to reinforce its status as a firm independent from the German corporation. BBVA Ventures was transformed into a separate entity, Propel Ventures, while Banco Santander did something similar when transforming InnoVentures into Mouro Capital. Siemens has also set up a separate venture capital unit called Next47, to foster disruptive ideas. Some companies from Next 47 portfolio entered Atos Scaler programme, where 15 start-ups are selected to develop their projects according to specific customer interests, and to contribute to enriching Atos offerings. One of these companies (United Biometrics) was recently present at CONCORDIA Open Door event (COD2020) exhibition space.
In summary, there are different ways to achieve win-win situation between large organisations and start-ups and CONCORDIA ecosystem, with more than 50 partners, from which are more than 20 large organisations, is one opportunity to explore these links.

Dual Purpose Vehicle: Telefonica Tech Ventures

On October 22nd, 2020 Telefónica introduced Telefónica Tech Ventures, its investment vehicle specialized in cybersecurity. It is promoted by ElevenPaths, Telefónica Tech's cybersecurity company, and by Telefónica Innovation Ventures, Telefónica's Corporate Venture Capital, it starts with a portfolio of nine invested startups and investment plans for up to fifteen more over the next three years.
This new vehicle serves a dual purpose: to develop Telefónica Tech's own investment capabilities in the highly dynamic cybersecurity sector, and secondly, to detect the most disruptive innovation in this field. More details on : https://techventures.telefonica.com/

Should I stay or should I go: Bitdefender experience

In 2001, Florin Talpes started the company in Romania that over time would become the role model for start-ups everywhere in the world. Bitdefender, a partner of CONCORDIA, started in an antivirus business, but is now doing also other cyber security products and services. It grew to more than 1600 employees worldwide.
During all these years, the company preserved its headquarters in Romania. In one interview, Florin, who is CEO now, mentions the major milestone when the company started to employee abroad, first in Germany and then in US. This "nuclear explosion" moment, as he calls it, happened when Bitdefender decided to have a double HQ, partly in Romania and partly in the US.

EU Cybersecurity Investment Platform: ECSO initiative

European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016 with more than 250 European cybersecurity stakeholders. ECSO Working Group 2, dedicated to Investment and Market deployment, organises a regular technical workshop with private investors to discuss challenges and opportunities to invests in European companies. ECSO WG2, with the support of the European private investors, drafted a letter of intent to initiate a dialogue with the EU Institutions for the creation of a European cybersecurity investment platform (fund-of-funds) of at least €1 billion investment, with the duration up to 5 years.

In this letter, ECSO and investors identified several key challenges for the European cybersecurity companies to scale up in Europe and also outline objectives such as to stimulate the emergence of new pan-European cybersecurity specialised funds, or to encourage the creation of a pan-European "Cybersecurity Accelerator" as a network of regional ecosystems specialised in cybersecurity.
If you want to support ECSO in this initiative, please let us know.

More Letters Have Been Signed: EIT and EIC

Another Letter of Intent has been signed, this time between the European Innovation Council (EIC) and the first wave Knowledge and Innovation Communities (KICs), including EIT DIGITAL, one of CONCORDIA partners. European Institute of Innovation and Technology (EIT) is a European Union body, established in 2008, with designated Knowledge and Innovation Communities (EIT KICs), each set up as independent entities. EIT Digital has two main instruments for venture creation. The first one is Innovation Factory, that brings together organisations from all over Europe to launch deep tech ventures, while the second is the Venture Program that supports teams of entrepreneurs from the so-called RIS (regional innovation scheme) countries to launch their Minimum Viable Product. EIT Digital is also running Digital Challenge that in 2020 has established a new record: 403 scaleups from 32 countries applied to the 7th edition of Europe's flagship deep tech competition in digital, a 44% growth with respect to 2019. The 20 best companies are invited to an exclusive event to pitch in front of a jury of high-profile corporates and investors. Among them, the jury will select 5 winners that will receive prizes totalling €350,000 to boost their international growth.
On the other hand, the European Innovation Council (EIC), to be fully implemented from 2021 under Horizon Europe, was introduced to support the commercialization of high-risk, high-impact technologies in the European Union. Enhanced European Innovation Council (EIC) pilot has been launched since 2018 at the request of the European Council. While EIC Pathfinder is providing grants to high-risk cutting-edge R&D projects implemented by consortia exploring new territories aiming at developing radical and innovative technologies, the EIC Accelerator is providing support to single start-ups or SMEs dealing with innovation which is still too risky to attract private investments.
Link: https://ec.europa.eu/research/eic/pdf/ec_eic_letter-of-intent-eic-eit.pdf

Past Events

We have been participating in Horizon Cyber event on October 2nd, 2020, co-organised by ECSO, SPARTA pilot project, ENISA and others, where several start-ups (mainly French) presented themselves. In addition, we participated in the South Summit event and sessions dedicated to cybersecurity on October 7th, 2020. South Summit was created by IE Business School in 2012 and is currently the largest start-up gathering event in Spain and one of the most important in Europe. As a part of cybersecurity start-up scouting efforts to enlarge PECS-UP community, we also attended a virtual event called Impact Week, more specifically dedicated session on start-ups that are working on key topics such as DLT and blockchain.

Future events

This year, in relation to its recently launched start-up award, ECSO was very active in co-organisation the local competitions, such as Cybersecurity Luxembourg Start-up Pathway on 15-16 September (Luxembourg), Horizon Cyber on 2 October (France), or European Cyber Week on 18 November in Rennes (France). The 8th edition of the ECSO Cyber

Investor Days is organised together with eurobits e.V. on Nov 30th and Dec 1st . Here is the link for registration: https://www.eventbrite.com/e/8th-cyber-investor-days-tickets-119427455735

CONVERGENCE is the new name for the joint annual event of pilot projects for the European Cybersecurity Competence Centre, Network and Community. CyberSec4Europe, SPARTA, CONCORDIA and ECHO announced a two-day concertation event from 9-11 December to be hosted online. Registration is free of charge and you can find the agenda here: https://cybercompetencenetwork.eu/convergence/

CONCORDIA will provide a series of webinars focusing on topics related to gender balance. The purpose of the webinar is to provide insights from relevant speakers and facilitate networking with the audience, to help women potentially interested in starting a new career path to be in touch with relevant speakers/organizations. The webinars are organized on two moments: first, a panel with relevant speakers (about 45 min) and second mentoring activity, implemented as private calls between people from the audience and a speaker (45 mins). We are happy to announce that the first webinar will be on women entrepreneurship, with Louise Bautista, Paola Bonomo and Sara Colnago. Registration is required, at the following link: https://hopin.com/events/dc-women-entrepreneurship

Cybersecurity Ventures is an International Acceleration Programme for cybersecurity start-ups, which emerged from the initiative of the National Institute of Cybersecurity (INCIBE) in Spain. Cybersecurity start-ups can sign up to the programme until 1 March 2021. More about benefits and other details at this link: https://www.incibe.es/ventures

Feedback needed: How did COVID impacted your business?

The World Economic Forum found that cyber-attacks and data fraud ranked third amongst COVID-related business concerns. It's a challenge for many organisations — but also an opportunity for start-ups. According to the LORCA Report 2020, investment into UK cybersecurity startups in 2020 has increased by 940%, compared to the same quarter in 2019 (which had already reached an all-time high of £521m). New cyber startups are springing up all the time, too; a new cyber business is registered every week in the UK, while vacancies for cybersecurity jobs climbed by 22% year-on-year in 2019. How did COVID impact your business? Do you have a story to share?

Let us know and we will publish your story in the next newsletter.