Leveraging Cyber ranges for Prototyping, Certification and Training: The ECHO case

Notis Mengidis
CERTH-ITI
Thessaloniki, Greece
nmengidis@iti.gr

Maya Bozhilova
Bulgarian Defense Institute
Sofia, Bulgaria
m.bozhilova@di.mod.bg

Cyril Ceresola
Naval Group
Paris, France
cyril.ceresola@naval-group.com

Consuelo Colabuono
Security Services, RHEA Group
Frascati, Italy
c.colabuono@rheagroup.com

Michael Cooke
Maynooth University
Maynooth, Ireland
michael.cooke@mu.ie

Gregory Depaix
Naval Group
Paris, France
gregory.depaix@naval-group.com

Angel Genchev
Bulgarian Defense Institute
Sofia Bulgaria
a.genchev@di.mod.bg

Georgi Koykov
ESI CEE
Sofia, Bulgaria
georgi.koykov@esicenter.bg

Wim Mees
Cyber Defence Lab, Royal Military Academy
Brusells, Belgium
w.mees@cylab.be

Matteo Merialdo
Security Services, RHEA Group
Redu, Belgium
m.merialdo@rheagroup.com

Antonis Voulgaridis
CERTH-ITI
Thessaloniki, Greece
antonismv@iti.gr

Theodora Tsikrika
CERTH-ITI
Thessaloniki, Greece
theodora.tsikrika@iti.gr

Konstantinos Votis
CERTH-ITI
Thessaloniki, Greece
kvotis@iti.gr

Stefanos Vrochidis
CERTH-ITI
Thessaloniki, Greece
stefanos@iti.gr

***Abstract*—Security needs and demands are nowadays constantly increasing for cybersecurity professionals and organisations in general. A cyber range provides a multipurpose virtual environment, which organisations can utilise for training, prototyping and certification of new technologies and create security testing environments that would otherwise be impossible to create. Being the equivalent of classic shooting ranges, cyber ranges are closed and controlled testbeds that contain all the necessary tools, networks and user simulations that are required for all intended security purposes. Within the scope of the ECHO project, a federation of interconnected cyber ranges form the foundation of the ECHO demonstration cases, providing the host environment in which three demonstration cases will be executed and demonstrate the added value that cyber ranges bring in the development of technology roadmaps, cyberskills development as well as certification testing.**

Keywords—cyber range, training, federated, simulation, cybersecurity, prototyping, certification

I. Introduction

The main goal of the ECHO project[1] is to organize and optimize currently fragmented cybersecurity efforts across the EU. Following this objective, a series of assets, modalities and tools are currently being developed by partners in the ECHO consortium, including the ECHO Federation of Cyber Ranges (E-FCR) [1], the ECHO Cyberskills Framework (E-CSF), the ECHO Cybersecurity Certification Scheme (E-CCS), and the ECHO Early Prototypes.

Work-package 8 (WP8) of the ECHO project, which commenced in January 2021, is tasked with understanding and assessing the usefulness, stability, completeness, adaptability, and general operation of these various assets through a series of demonstration cases. In this instance, a ‘Demonstration Case’ is defined as a particular kind of use case that demonstrates the functionality, performance characteristics, and value of a product or tool, as well as the operational conditions under which it achieves the promised outcomes. These operational conditions include management, human factors/resources, financial considerations, and legal/regulatory frameworks.

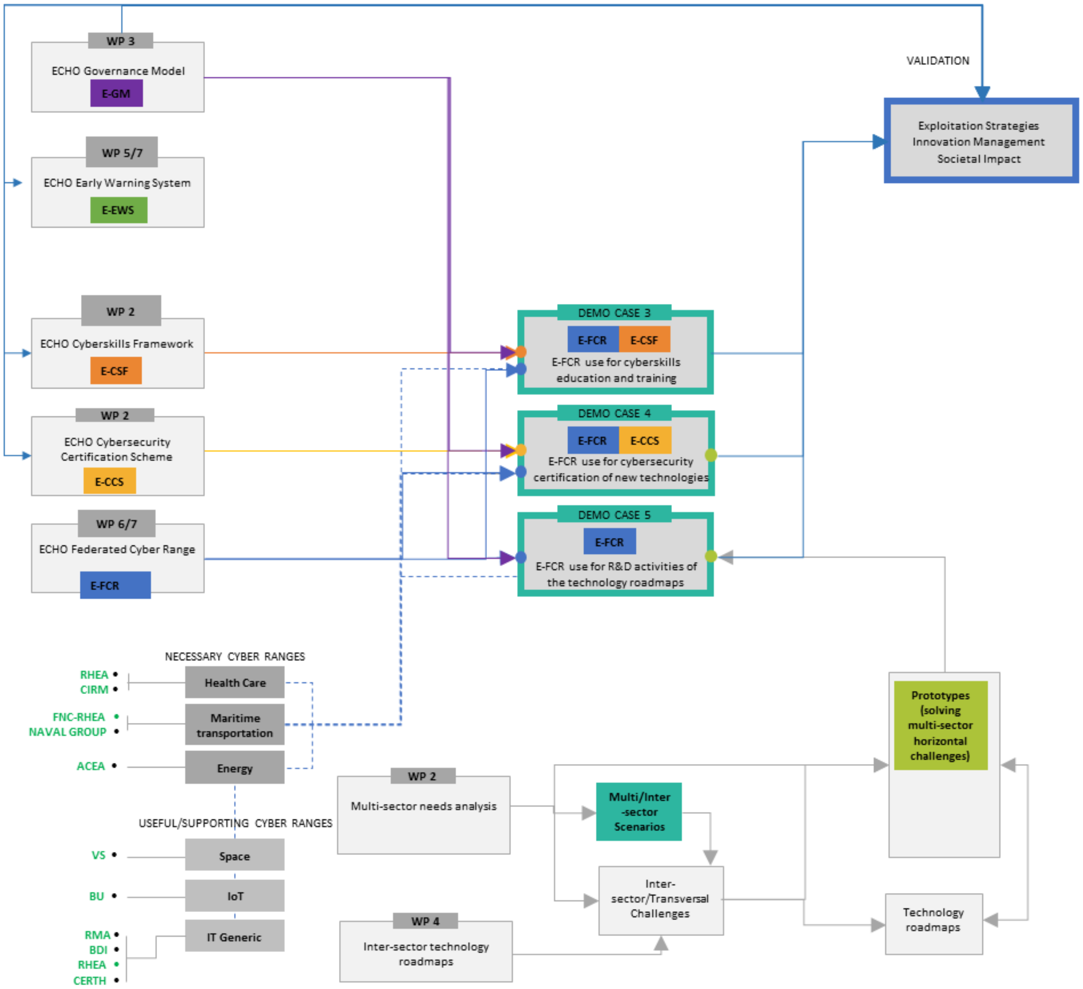
Crucially, a demonstration case requires all the following components to be operated effectively:

- Defined end-users and stakeholders and their operational objectives (and means of measuring same)
- Clear description of the asset
- Specified set of functions and their intended outcomes (respective organizational logic and means of measuring same)

[1] https://echonetwork.eu/

- A description of the organizational structure and process flows demonstrating critical inputs, outputs and dependencies
- Resource requirements
- A timeframe sufficient to allow the measurement and demonstration of the operational benefits of tool deployment approximating a real-world situation
- E-FCR use for R&D activities of the technology roadmaps

Generally, relationships between the different activities in ECHO drive towards the Demonstration Cases. In Figure 1, a diagram showing these relationships is provided: this constitutes the foundation of current and upcoming ECHO activities bringing the full integration of the outputs of the project.



WP 3
ECHO Governance Model
E-GM
WP 5/7
ECHO Early Warning System
E-EWS
WP 2
ECHO Cyberskills Framework
E-CSF
WP 2
ECHO Cybersecurity Certification Scheme
E-CCS
WP 6/7
ECHO Federated Cyber Range
E-FCR
VALIDATION
Exploitation Strategies
Innovation Management
Societal Impact
DEMO CASE 3
E-FCR
E-CSF
E-FCR use for cyberskills education and training
DEMO CASE 4
E-FCR
E-CCS
E-FCR use for cybersecurity certification of new technologies
DEMO CASE 5
E-FCR
E-FCR use for R&D activities of the technology roadmaps
NECESSARY CYBER RANGES
RHEA
CIRM
Health Care
FNC-RHEA
NAVAL GROUP
Maritime transportation
ACEA
Energy
USEFUL/SUPPORTING CYBER RANGES
VS
Space
BU
IoT
RMA
BDI
RHEA
CERTH
IT Generic
WP 2
Multi-sector needs analysis
WP 4
Inter-sector technology roadmaps
Multi/Inter -sector Scenarios
Inter-sector/Transversal Challenges
Prototypes (solving multi-sector horizontal challenges)
Technology roadmaps

Figure 1: ECHO Demonstration Cases and WPs relationship

The ECHO Demonstration Cases are structured in a way to force the interaction and the combined work of multiple Tasks and Work Packages within the project. The team actively started working on the Demonstration Cases since they are key to validate most of the ECHO Assets and their combination.

Five Demonstration Cases are foreseen, combined in a way to cover all the important ECHO assets, albeit E-FCR is used in three of them and more specifically :

- E-FCR use for cyber-skills education and training
- E-FCR use for cybersecurity certification of new technologies

II. E-FCR FOR CYBERSKILLS EDUCATION AND TRAINING – DEMONSTRATION CASE 3

The design, development and deployment of cyber range scenarios for hands-on training exercises on detection of, response to and recovery from cyber incidents is an essential part of the ECHO project and demonstration and validation cases. The leveraging of the E-FCR platform in training and educational scenarios has been discussed from the beginning of the project implementation and considered in the design and development of the ECHO use cases and scenarios.

A. *Technical status and key functions*

The main objective of the Demonstration Case 3 is to explore the connections between the theoretical and fundamental training content with practical learning with real-world scenarios (cyber-attacks and incidents) and its impacts on a better acquisition of skills and knowledge. The Federation itself allows building of complex and distributed scenarios where the participants can apply their knowledge in offensive and defensive roles. The significance and complementarity of fundamental and practical education should be balanced and transferable. It is important to provide opportunities for improving the synergies between higher education and professional training, considering the specific nature of both.

The theoretical content designed and delivered through instructional methods (lectures, e-learning) complemented with cyber range scenarios deployed and delivered within cyber range infrastructures not only improve the learners' skills in cybersecurity but support the realistic assessment of their preparedness and form the paths of their future professional development. The assessment methods created within WP2 of the project enlarge the simple evaluation "satisfactory" and "poorly" with the additional information about possible need of adjusting the scenarios and/or increasing their complexity according to the proficiency level of the participants.

The creation of more flexible methods for the design of short-term trainings in operational environments to develop purpose-based acquisition of critical skills is also a part of the validation. The prioritization of tasks in the scenario design is a tough and time-consuming task. The ECHO project demonstrates the created conditions and infrastructure to support the timely identification of gaps and methods to fill those gaps continuously with combining information sharing and incident detection tool with a platform for team play on incident response and recovery. The latter facilitates collaboration and knowledge sharing between professionals and industries.

The key functions of the E-FCR platform for demonstration of its capabilities in training and education are:

- Flexible design of a training scenario in the context of the theoretical content and according to the proficiency level and experience of the participants;
- Building and deployment of infrastructure that can be easily re-used and/or transferred to third party for maintenance and tutoring;
- The participants should be able to connect to and/or monitor more than one cyber ranges;
- The participants should have at least 3 independent channels for interaction – one or two for playing the scenario and a third and or more, for communication. The detailed technical requirements will be developed after considering the particular scenarios.

III. E-FCR USE FOR CYBERSECURITY CERTIFICATION OF NEW TECHNOLOGIES – DEMONSTRATION CASE 4

While developing the certification for new technology can be an interesting way to highlight the overall quality and security of an IT product, it can be a long and complex process spanning from the connection between the developers of a product and the certification team to contracting and prototype provision. Consequently, leveraging this process through the medium of cyber-ranges can make things easier.

Demonstration Case 4 aims to demonstrate the suitable use of the E-FCR during the conformity assessment of new technologies that need to receive a security certification. According to the assurance level to be reached in the certification, different assessment activities are foreseen aspiring to also use penetration tests and cyber-attack simulation to check the resilience against a certain potential attack of a malicious actor with a certain level of skill.

In the following paragraphs, we present the roles and methodology of the certification approach adopted by the E-CCS the technical status and readiness of the E-FCR with respect to the aforementioned technologies.

A. *Stakeholders and methodology*

The potential customer of a product and the owners of a product would like to have enough confidence that their product has sufficient and correct countermeasures to minimize the identified risks of the product itself. The product is a general or sector-specific asset: named Target of Evaluation (TOE). The main stakeholders involved in the certification and evaluation process are the following:

1) *Consumers*

Consumers can use the results of evaluations to help decide whether a TOE fulfils their security needs. ISO/IEC 15408 [2][3][4] gives consumers, especially in consumer groups and communities of interest, an implementation-independent structure, termed the Protection Profile (PP), in which they are able to express their security requirements in an unambiguous manner.

2) *Developers*

ISO/IEC 15408 is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST).

3) *Evaluators*

Evaluation is based on Common Criteria and related standards: ISO/IEC 15408 – 1, 2, 3 and ISO/IEC 18045 [5].

ISO/IEC 15408 is only suitable for assessing the correctness of IT countermeasures. Therefore, the non-IT countermeasures (e.g. human security guards, procedures) are always in the Operational Environment, the environment in which the TOE is operated.

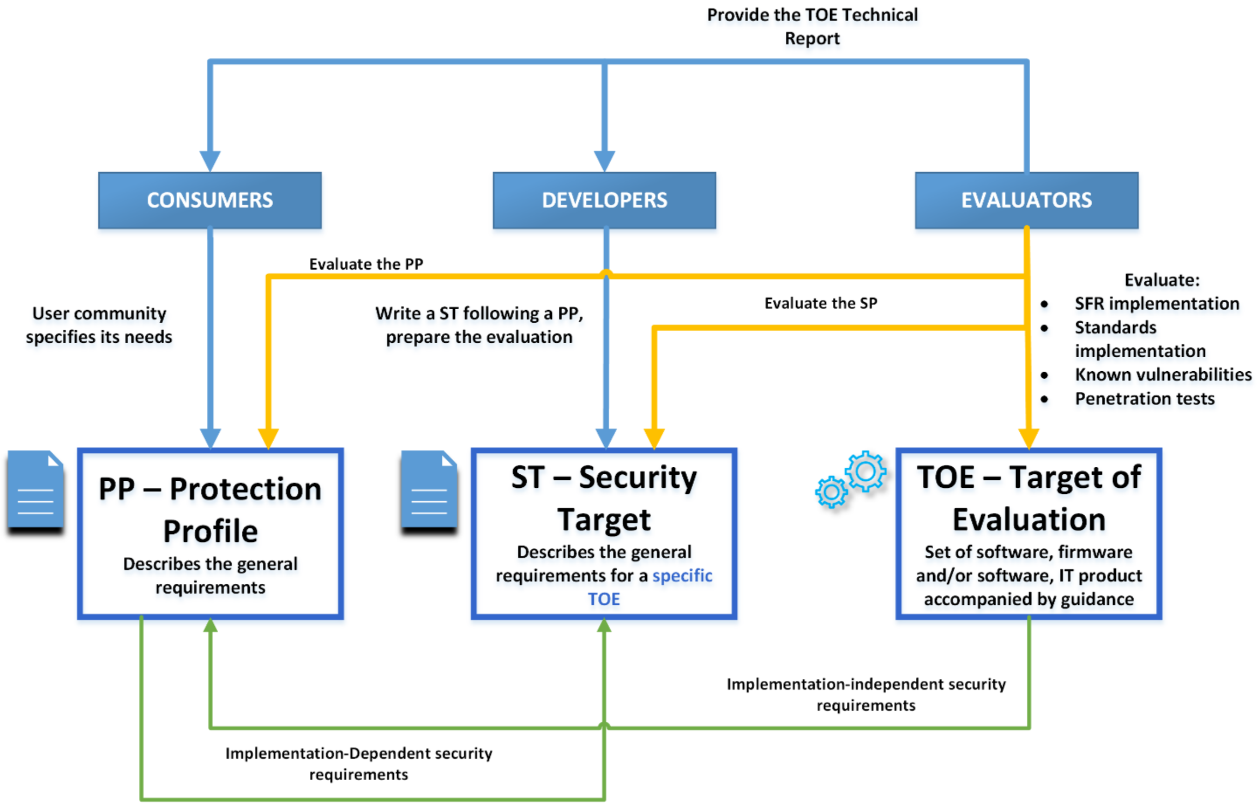

Provide the TOE Technical Report
CONSUMERS
DEVELOPERS
EVALUATORS
Evaluate the PP
User community specifies its needs
Write a ST following a PP, prepare the evaluation
Evaluate the SP
Evaluate:
SFR implementation
Standards implementation
Known vulnerabilities
Penetration tests
PP – Protection Profile
Describes the general requirements
ST – Security Target
Describes the general requirements for a specific TOE
TOE – Target of Evaluation
Set of software, firmware and/or software, IT product accompanied by guidance
Implementation-independent security requirements
Implementation-Dependent security requirements

Figure 2: Overview of the certification framework

The purpose of the PP is to state a Security Problem (SP) for a given system or product category and specify security requirements to solve that problem. The SP is a formal statement defining the nature and scope of the security that the TOE is intended to address. This statement consists of a combination of:

- threats to be countered by the TOE;
- the Organisational Security Policies (OSPs) enforced by the TOE;
- the assumptions that are upheld for the TOE and its Operational Environment (OE).

Security Objectives (SO) are statements of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions. ISO 15408 provides a common set of requirements for the security functionality (SFR) of IT products and for assurance measures (SAR) applied to these IT products during a security evaluation. A set of assurance components (SARs) has been chosen for each Evaluation Assurance Level (EAL). These EALs consist of an appropriate combination of assurance components.

In general, when estimating assurance level needed, it makes sense to consider breaking down the risk equation into its impact and likelihood factors:

- Impact derives from maximum injury in case of failure. For EN, HC, MT sectors, the injury table is very high since there is potential loss of life (individual or group) in all cases. This may be adjusted downward depending on the nature of the Target of Evaluation, but we assume the impact factor to be very high.
- Likelihood can be taken as a function of vulnerability: more vulnerabilities will generate a higher likelihood of an impact due to compromise.

In this demonstration case, the E-FCR will provide the necessary service to perform the security tests aiming to validate the E-CCS, applied to two of the prototypes developed in the project. The selected technologies are a SIEM tool for the MT sector (CyMS) and an information sharing platform for the HC sector (SISP). The selected certification scheme used for the certification is the E-CCS ideated within ECHO and based on the EUCC scheme of ENISA [6]. Finally, a second goal for this demonstration case is to validate the maturity of the E-CCS as a framework to develop tailored security certification schema for sector-specific products.

IV. E-FCR USE FOR R&D ACTIVITIES OF THE TECHNOLOGY ROADMAPS – DEMONSTRATION CASE 5

R&D activities often need wide access to various sources of information, technologies and skills. Some pre-design studies can be greatly facilitated if certain technologies, tools or environments can be made available quickly. Demonstration Case 5 aims to demonstrate the suitable use of the E-FCR and its connected cyber ranges throughout R&D projects. The selected technologies are a SIEM tool for the Maritime sector CyMS), a Penetration Testing tool for attack simulation and detection of vulnerabilities, and a service/device monitoring system (MonSys).

A. *CyMS*

CyMS is a software produced by Naval Group and it is a cyber-threat monitoring and an alert tool: it is a kind of Security Information and Event Management systems. SIEMs are tools designed and developed to gather logs from multiple sources.

Based upon third-parties and Naval Group's own components, the CyMS aims to foster the Cyber Defence of IT/OT infrastructure onboard ships. With its two main functionalities: cyber supervision and administration, it enables operator's awareness of relevant cyber threats and suggest mitigation actions to contain the attack. It collects logs from heterogeneous distributed sensors, processes datasets, raises value-added alarms and manages cyber incidents.

Human Machine Interface (HMI), which is being developed as a prototype under the scope of the ECHO project, is dedicated to respond to the challenge of the presentation of a complex situation to crew members who are not cyber experts. The E-FCR will contribute efficiently to the development of CyMS by providing network emulation environments where the CyMS can undergo functional tests: this will generally be of assistance to the CyMS developers, able to constantly test their software on a realistic network environment.

The E-FCR is envisioned to allow the owner of the CyMS prototype to:

- search for a network architecture provider (a cyber range provider able to instantiate a network emulation environment where to deploy CyMS and test it on a realistic situation)
- contract with the cyber range provider easily
- design and build a testbed network in the provider's cyber range, following the specification of the customer
- during the development activities, test the CyMS inside the emulated network

B. *Penetration Testing Tool*

The penetration testing tool is a software platform specifically designed to assess system security and identify attack vectors. These tools are generally used to simulate real-world attack scenarios in order to discover and exploit security gaps in software and services. Penetration testing tools are also crucial during the software development process, especially for R&D departments that have to test services and software reachable through the web or external computers. Finally, system maintenance is also a domain that can greatly benefit from using such tools as deprecated services can be identified and updated.

Expanding on the above, the central goal of the penetration testing tool, developed by CERTH is to semi-automate a number of time-consuming and complex tasks and assist in the reconnaissance and exploitation phase of a network/host service infrastructure. The penetration testing tool has five functionalities:

- Scanning a target network and identifying active hosts
- Scanning a target host to identify open ports and known service vulnerabilities
- Enumerating the services running on these open ports to identify possible security vulnerabilities on the system
- Performing automated attacks on the services by using the information discovered by the previous steps
- Presenting the results to the user in a friendly Web Interface.

The E-FCR will contribute efficiently to the development of the tool by providing network emulation environments where it can undergo functional test; this will generally be of assistance to the developers, since they will be able to constantly test their software on a realistic network environment.

The E-FCR will allow the owner of the tool to:

- search for a network architecture provider (a cyber range provider able to instantiate a network emulation environment where to deploy the tool and test it on a realistic situation)
- contract with the cyber range provider easily
- design and build a testbed network in the provider's cyber range, following the specification of the customer
- during the development activities, test the tool inside the emulated network

C. *MonSys Bridge*

The MonSys Bridge prototype provides connectivity between different types of Early Warning Systems, Intrusion Detection Systems, Intrusion Prevention Systems and Situational Awareness tools with the ECHO-Early Warning System (E-EWS). The bridge integrates the alerts, signals and warnings (related to abnormal behaviour and disruption) generated by those systems with the library and resources of the E-EWS in a ticket format. The functionality of the prototype has been successfully tested within several E-EWS table-top exercises with the monitoring system MonSys developed by the Cybersecurity Lab and ESI CEE's team as well as Zabbix - open-source system. The dissemination of the notifications generated within the E-EWS complies with the communication and sharing rules of the latter.

In brief, the MonSys platform is a distributed real-time monitoring tool operating in public and private cloud. It is capable to monitor a large amount of services and/or devices, to run basic and custom tests. The platform notifies the user when some of the monitored services is down or disrupted according to pre-defined rules. It maintains several notifying channels as the bridge ensures mainly the connectivity with the E-EWS system.

Main capabilities:

- Real-time monitoring and notifications of the E-EWS tenants.
- Setting custom checks and rules.

- Long-term large amount of data storage.
- Custom availability checks and logic.
- Several notification channels.
- Data normalization

In the context of Demonstration Case 5 the bridge could be used to generate and send to interested parties an alert and subsequent sanitized ticket through the E-EWS about discovered relevant service disruptions or anomalies. A third-party customer developing a service using the same or similar infrastructure could use this intelligence to request a cyber range to test the applicability of this information within the context of their service. The cyber range providers compile the related infrastructure and testing tools and rent it out to the customer. Such a scenario demonstrates the capability of the MonSys Bridge through the

E-EWS and E-FCR to contribute to the secure software development of applications for various industries and use cases across Europe.

The E-FCR must allow the owner of the tool to:

1) Decentralized approach:

- The bridge is deployed and configured leveraging the use of E-EWS with an external monitoring system.
- Different type of solutions monitor different services integrating alerts/warnings into the E-EWS through the MonSys Bridge.
- The E-EWS system notifies the interested parties via tickets/warnings.
- Those interested parties request a test bed infrastructure through E-FCR for testing specific services and applications against received intelligence.
- Combination with other prototypes is optional, i.e. penetration testing tool for automation of some pen tests.

2) Add-on approach:

- The bridge is connected with a monitoring solution installed in the customer's premises.
- The customer's monitoring system sends a sanitized ticket to the E-EWS notifying related partners/ suppliers of the customer or other interested parties about found disruption or vulnerability in a specific service or infrastructure.
- The third-party organizations request a sandbox to simulate their similarly connected operational and IT infrastructure and analyze the information from the ticket.

V. Conclusions

The complexity and scale of the cybersecurity threat landscape create a constantly increasing strain in an organisation's defences and cyber ranges have become a valuable tool moving towards more realistic and competitive scenarios that can help the users receive focused experiential cybersecurity training. However, the interest in cyber ranges in applications other that education, has increased in the last few years. In this paper, we presented how a cyber range can be used for certification and prototyping purposes besides being used as a traditional educational platform.

In this paper we presented how the ECHO project plans to use a federation of cyber ranges to demonstrate the functionality, performance characteristics, and value of the products and tools, as well as the operational conditions under which it achieves the promised outcomes. In this context, we presented each demonstration case individually, as well as the methodological approaches which will be adopted during the undertaking and evaluation of these demonstration cases. Finally, we displayed a more in-depth view on how the E-FCR will provide the necessary services towards the successful demonstration cases.

Acknowledgment

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

[1] N. Oikonomou,, et al. "ECHO Federated Cyber Range: Towards Next-Generation Scalable Cyber Ranges." 2021 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2021.

[2] ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security, Part 1: Introduction and general model (2009)

[3] ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security, Part 2: Security functional components

[4] ISO/IEC 15408-1:2009, Informational technology – Security techniques – Evaluation criteria for IT security, Part 3: Security assurance requirement (2008)

[5] ISO/IEC 18045:2008, Informational technology – Security techniques – Methodology for it security evaluation (2008)

[6] European Union Agency for Cybersecurity (ENISA),"Cybersecurity certification: EUCC candidate scheme" 02-Jul-2020. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

[7] "IEEE Guide for Information Technology - System definition - Concept of Operations (ConOps) document," in IEEE Std 1362-1998 , vol., no., pp.1-24, 22 Dec. 1998, doi: 10.1109/IEEESTD.1998.8942