CYBER RANGE FEATURES CHECKLIST

& LIST OF EUROPEAN PROVIDERS

ECS
EUROPEAN CYBER SECURITY ORGANISATION
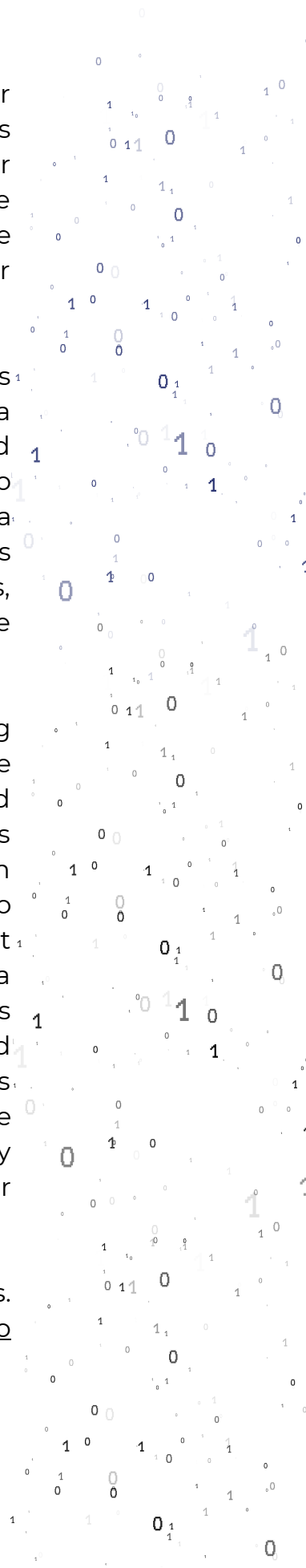
PREPARED BY: ECSO WG5

2022 EDITION

SUMMARY

In 2021, ECSO launched a Call to Action to identify and bring together European cyber range providers and end users. The aim of this initiative was to consolidate the approaches of European cyber range-enabled services and concepts, promote and support the development of best practices and guidelines that define the "European Cyber Range" and its uptake, and help shape the further development of European cyber range platforms & solutions.

To promote and support the best practices and develop guidelines that define cyber ranges, ECSO has identified the key features of a cyber range platform, presented in the form of a checklist for end users and groups. This checklist can be leveraged by end users to define their cyber range requirements and subsequent award criteria for electronic tenders for procurement purposes. ECSO, through its Call to Action, has also identified European cyber range providers, providing for the first time a central point and repository of these providers.

This document provides value to end users and groups by providing them with a better understanding of the European cyber range market and providers, open-source alternatives, and web-based penetration tools. It assists end users in identifying the main features of a cyber range platform so they can easily identify and distinguish between platform offerings. This document also provides a guide to end users and groups on the main features and requirements that could potentially form part of the award criteria when selecting a cyber range provider. From the cyber range provider perspective, this document is an opportunity to showcase the range, depth and breadth of platform offerings at a European level, raising awareness of the benefits of cyber range platforms and further promoting the market. It develops a common set of features and terminology around cyber range platforms and services, thereby allowing deeper engagement with end users and groups.

This document also includes a Glossary and foundational elements. from the ECSO paper "Understanding Cyber Ranges: From Hype to Reality" that was published in 2020 [1].
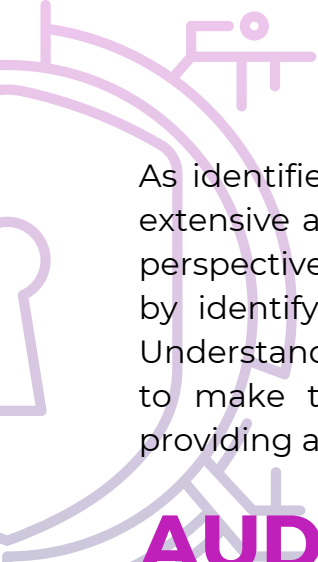
CYBER RANGE OVERVIEW

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

A cyber range not only enables advanced R&I in cybersecurity, but it also allows public and private sector organisations to test, in a secure sand-boxed environment, the cyber resilience of their digital systems against cyber-attacks, allowing weaknesses to be identified and remedied before cybercriminals can exploit them. Cyber ranges also support interdisciplinary research into understanding the psycho-social engineering tactics of cybersecurity attacks, supporting the development of combined human factors and technology solutions to mitigate those attacks. Cyber ranges also support the training of advanced cybersecurity skills for both academic and work-based learners who will be able to hone their skills in the highly realistic training environments that cyber ranges can offer.

Cyber ranges are used by many diverse user groups such as academia, research centres, industry, government agencies, enabling, developing and enhancing a range of advanced cybersecurity services and supporting a broad number of use cases. Cyber range platforms include commercial offerings with many inbuilt cybersecurity scenarios and content, allowing for a more immediate impact for key users or groups. Open-source platforms have also recently emerged, generally with less well-developed scenarios and in-built features and support, but offered to user groups at a reduced or with no licensing cost.

PROBLEM

Searching for a cyber range provider is a difficult task but selecting a European cyber range is even more difficult as currently there is no single catalogue offering of European cyber range providers. This document provides a list of European cyber range providers, to support end users/groups in identifying providers that best support their requirements.

As identified in Annex I, the range of cyber range providers across Europe is extensive and selecting the most suitable platform from an end user or group perspective can be a challenging task. This document assists end users/groups by identifying the key features that cyber range platforms generally offer. Understanding these requirements and features will allow the key users/groups to make the most suitable investment in technologies and platforms by providing assistance on identifying their own requirements.
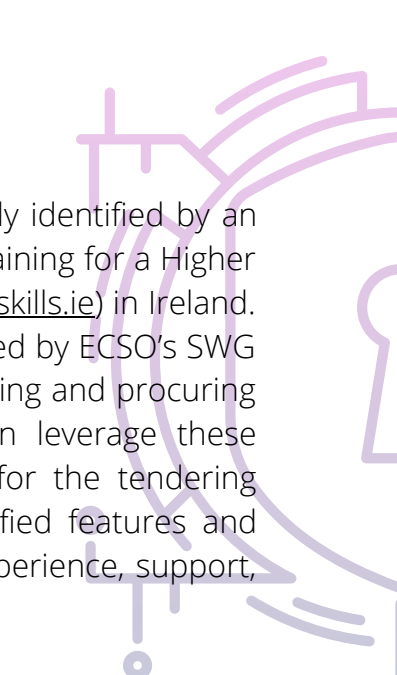
AUDIENCE

This document is intended for anyone looking to invest in a cyber range platform solution, with a focus on European cyber range providers. The intended end users/groups include academia, research centres, government agencies and industry stakeholders looking to enable, develop or enhance their products, services or activities through a cyber range platform.

CYBER RANGE FEATURES CHECKLIST

The use case requirements and cyber range features below were initially identified by an end user looking to procure a cyber range platform for education and training for a Higher Education Authority (HEA) funded initiative called Cyber Skills (www.cyberskills.ie) in Ireland. These features and requirements were subsequently reviewed and refined by ECSO's SWG 5.1 'cyber range' chairs and WG members to support end users in selecting and procuring a cyber range platform for their identified use case. End users can leverage these requirements and features as part of their identified award criteria for the tendering process, but award criteria should not be limited to just these identified features and should include items such as cost, course/scenario catalogue, sector experience, support, training and maintenance etc.

The cyber range features below are presented as a series of features, items and checkboxes. If end users are leveraging these features and this checkbox list as part of their award criteria then it is advised to instruct cyber range providers to complete this table, clearly indicating their response and providing additional answers/evidence if necessary.

The features and format below extend upon and refine the cyber range checklist previously provided by NIST [2] outlining the key features and considerations that end users/groups could potentially consider when evaluating and selecting a cyber range provider.

Use Cases supported by the Cyber Range	The Cyber Range is focused on the following audiences and/or use cases (more than one selection is possible):
☐	**Cybersecurity education** - Educators seeking to implement basic and advanced cyber security courses and curricula.
☐	**Cybersecurity training** - Organisations or individuals seeking training for security operations, analysis, and forensic specialists.
☐	**Security Testing** - Organisations seeking "situation operations" testing for new products, software releases and organisational restructuring.
☐	**Competence Assessment -** Organisations or individuals seeking cybersecurity skills validaion to evaluate candidates for cybersecurity positions.
☐	**Cybersecurity research** - Academic institutions and researchers to research new attack detection and mitigation methods etc.
☐	**Cyber Resilience** – Academic institutions, organisations ability to response and to be able to sustain a security incident or cyber-attack while maintaining its ability to deliver its core business function.
☐	**Cyber Capabilities** – assists in developing the capabilities of security professionals, research and development of cyber tools and other assets and for the continuous delivery of cyber exercise to test cyber capabilities.
☐	**Crisis Management for SOCs** – Ability to reproduce effects of cyber threats / malware to study propagation and impact.
☐	**Hybrid Scenarios** - Ability to integrate with cyber physical platforms for exchanging cyber effect events with other sectors' simulations.
☐	**Cyber Protection by Deception** - Ability to emulate entire portions of fake devulnerabilised enterprises to allow the analysis and study of ongoing threats.

Location of the Cyber Range	The Cyber Range can be located (more than one selection is possible):
☐	**On Premise (fixed or limited users)**
☐	**On Premise (with cloud capability)**
☐	**Cloud based (remote)**
☐	**Hybrid (blend of on premise and cloud based)**

Scalability and Elasticity	The Cyber Range can support:
☐	**Limited number of users for a limited time period.**
☐	**Limited number of users for an unlimited time period.**
☐	**Unlimited number of users for a limited time period.**
☐	**Unlimited number of users for an unlimited time period.**
☐	**Interoperability with remote orchestrators, scenarios. Possibility to federate with other scenarios.**

Reliability	The Cyber Range must provide specific minimum availability requirements:
☐	**Not important**
☐	**>95%**
☐	**>99%**

Virtualisation Platform	
☐	OpenStack
☐	OpenNebula
☐	VMWare vCenter
☐	VMWare vCloud
☐	Kubernetes
☐	AWS Cloud Provider
☐	MS Azure Cloud Provider
☐	Other

Ease of use	The Cyber Range allows learners to:
☐	**Save and resume scenarios.**
☐	**Save and resume single (or groups) of virtual machines in a scenario.**
☐	**Record and replay events on the scenarios.**

Realism of the emulation	The Cyber Range allows:
☐	**Stateful traffic generation.**
☐	**Stateless traffic injection.**
☐	**Human behaviour simulation.**
☐	**Cyber Defence automation.**
☐	**Scenario Network L2 stretching over VPN.**
☐	**Scenario Network L2 stretching over vVLANs.**
☐	**Scenario Network L2 stretching over physical VLANs.**

Internet Connection	The Cyber Range scenario allows individual VM/Containers etc to connect to the Internet to download and install packages (even temporarily):
☐	**Yes**
☐	**No**
☐	**Should be configurable for each scenario**

Customisation	The scenarios of the Cyber Range are::
☐	**Pre-packaged (no customisation)**
☐	**Pre-packaged with options for some customisation.**
☐	**Full and significant customisation** **New scenarios (developed from scratch) can be requested**

Learning Management System (LMS) Integration	The Cyber Range can export student performance data to an external Learning Management System (LMS) eLearning platform through:
☐	**eXperience API (xAPI) integration**
☐	**Shareable Content Object Reference Model (SCORM)**
☐	**No integration**
☐	**Other (please specify)**

Learning Outcomes & Standard Alignment	The Cyber Range provides tooling and/or supporting services that aligns with the following frameworks:
☐	**NIST Framework**
☐	**NICE Framework**
☐	**MITRE ATT&CK**
☐	**MITRE CAPEC**
☐	**NSA/DHS National Centres for Academic Excellence Knowledge Units**
☐	**Allows alignment to custom framework.**
☐	**Other (please specify)**

Assessment	The Cyber Range can support assessments allowing educators to (more than one selection is possible):
☐	**Schedule a cyber exercise on a particular date and time.**
☐	**Individual / asynchronous training and exercises.**
☐	**Set a password for an active/scheduled cyber exercise.**
☐	**Monitor the participant's progress on a live cyber exercise.**
☐	**Review actions of learners participating in a cyber exercise through record/replay features.**
☐	**Facilitate feedback to learners by assigning them a mark and comments on their performance.**
☐	**Other (please specify)**

Participants	The Cyber Range can support the following users with different roles (more than one selection is possible):
☐	**Red –** member can play the role of attacker, pentester, and ethical hackers.
☐	**Blue –** member can play the role of a defensive team member that allows improving and learning about different attack techniques.
☐	**White -** created for instructor, moderators and administrators; it allows content management, monitoring of the learners and overall evaluations.
☐	**Green –** support and technical monitoring of the cyber range infrastructure.
☐	**Purple –** ethical hacking aimed at increasing protection of skills.
☐	**Grey –** reference, support, coordination, scoring, process and supervision.

Training & Support	The Cyber Range provider provides:
☐	**Initial Support and Training**
☐	**Periodic Support and Training**
☐	**On-Call Support and Training**
☐	**On-Call Support to develop new scenarios and/or cyber exercise**

Licenced/Open Source Security Tools	The Cyber Range can support the following commercial tools:
☐	**Splunk**
☐	**ArcSight**
☐	**Alien Vault**
☐	**IBM QRadar**
☐	**MISP**
☐	**Wireshark**
☐	**Metasploit**
☐	**Nmap**
☐	**Next Gen Firewalls (please specify)**
☐	**CTI Platforms (please specify)**
☐	**Other COTS (please specify)**

Capture The Flag (CTF)	The Cyber Range can host CTF events supporting:
☐	**Single users**
☐	**Multiple users**
☐	**Red teams (simulated or live)**
☐	**Blue teams**
☐	**Live scoring and leader board**

Attack Simulation	The Cyber Range can simulate/has the capacity to run:
☐	**Real benign traffic**
☐	**Malicious traffic**
☐	**Collection of IoCs**

Operational Technology	The Cyber Range can support the Operational Technology (OT) in addition to Information Technology (IT) systems:
☐	**Yes**
☐	**No**

Industrial Communications (complete if you answered yes to previous question)	The Cyber Range can support the following industrial communication protocols:
☐	**Modbus**
☐	**Profibus**
☐	**UMAS**
☐	**S7**
☐	**Ethernet**
☐	**IEC 61850**
☐	**IEC 104**
☐	**DNP3**
☐	**OPC**
☐	**I2C**
☐	**Avionic/MIL Buses (MIL-STD-1553, etc...)**
☐	**Space protocols (CCSDS, etc..)**
☐	**Other (please specify)**

Scenarios & Workflows	The Cyber Range allows users with sufficient permissions to:
☐	**Create new scenarios.**
☐	**Modify an existing scenario**
☐	**Clone existing scenarios**
☐	**Modify a live scenario**
☐	**Export existing scenario**
☐	**Import scenario from a compatible source**
☐	**Map scenarios and labs to competency framework**
☐	**Automatically discover a real network and (partially) reconstruct its emulation within a cyber range scenarios**
☐	**Run multiple scenario instances in parallel**

Scenarios & Workflows	The Cyber Range provides an existing catalogue of scenarios or labs:
☐	**Yes**
☐	**No**
	If yes, specify which scenarios are available:
	If yes, specify how many scenarios can be stored in the cyber range:

Testing Capabilities	The Cyber Range supports scenarios to test single assets or combination of assets:
☐	**Yes, with specific features such as test timelines, configuration of the Security Targets, traceability to security requirements, reporting, etc..**
☐	**Yes, without specific features**
☐	**No**

Hardware Requirements	The provider must provide details of the underlying platform required to install the platform, in addition to the number of concurrent VM/hosts it can support.

Providers	The provider:
☐	**Offers a maintenance and support package with subscription**
☐	**Provides SLAs**
☐	**Can also procure the HW for an on-prem deployment**
☐	**None of the above**

Assets Library	The cyber range is provided with an asset library of virtual templates to be used to create or customise scenarios:
☐	**Yes**
☐	**No**
	If Yes, the Asset Library:
☐	**Can be further expanded**
☐	**Includes a variety of different assets licensed and/or open source (include a list of the available assets)**
☐	**Each asset can be contextualised and configured on cyber range scenarios via scripting language (for example, Ansible)**

Assessment for training scenarios	
☐	**Automated or semi-automated trainee performance assessments**
☐	**Manual trainee performance assessment**
☐	**Reports generation**
☐	**Customisable questionnaires**

GLOSSARY

Capture the Flag (CTF) – In the context of computer security, a CTF is a type of cyber war game which can be played either in teams or as individuals. A popular type of CTF is attack and defence where participants compete to compromise other participants' systems while at the same time trying to defend their own.

Competence – Competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks.

Computer Network Operations (CNO) Units – These are units located within a state's military structure that are tasked to engage in operations involving computer networks.

Cyber Capabilities – Cyber capabilities are the resources and assets available to a state to resist or project influence through cyberspace.

Cyber Defence Exercises – Also more commonly referred to as CDX, a cyber defence exercise is a special type of cyber exercise focused on assessing cyber defence capabilities.

Cyber Exercise – A cyber exercise is a planned event during which an organisation simulates cyber-attacks or information security incidents or other types of disruptions in order to test the organisation's cyber capabilities, from being able to detect a security incident to the ability to respond appropriately and minimise any related impact. A cyber exercise may be use one or more cyber range scenarios.

Cyber Resilience – Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources.

Orchestration – Orchestration is the automated configuration, coordination, and management of computer systems and software.

Hypervisor – A hypervisor is the software layer between the hardware and the virtual machines (VMs). It coordinates the VMs ensuring they don't interfere with each other and that each has access to the physical resources it needs to execute.

Platform – A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed.

Annex I - European Cyber Ranges

Commercial off the Shelf (COTS)

Platform	Company	Description
Airbus CyberRange	**Airbus Cybersecurity**	Airbus CyberRange is a multi-role cyber simulation platform. It has been developed to model IT / OT systems composed of tens to hundreds virtual component and play realistic scenarios including real cyber-attacks. As a system integrator, Airbus CyberSecurity designed its CyberRange as a sustainable industrial product, tackling the following objectives: Customizable (IT/OT), easy to operate (VMWare ESX and Docker). Provide Training, Testing (HW/SW), Crisis management. https://www.cyber.airbus.com/cyberrange/
AIT Cyber Range	**AIT**	AIT's Cyber Range is a virtual environment for flexible simulation of critical IT and OT systems with complex networks, different system components and users. It provides a secure and realistic environment for analysing and testing incidents in various scalable scenarios without using real production systems. This allows different security processes to be rehearsed for live operation and special incident response processes for cyber incidents to be tested in order to meet the highest security requirements for system architectures and operating processes. The AIT Cyber Range training courses and exercises address the cyber security needs of staff, IT professionals, CERTs/CSIRTs, management and advisory boards in industry, research and government. https://cyberrange.at/
AMOSSYS Cyber Range		The AMOSSYS Cyber Range Platform focuses on dataset generation through Cyber Range capabilities (attack simulation, user simulation and software/data provisioning). Based on the AMOSSYS Cyber Range Platform, an honeypot/honeynet use case is also developed. All AMOSSYS Cyber Range Platform components are managed through REST API, thus allowing end users for integration into larger ecosystems. The AMOSSYS Cyber Range Platform also provides normalized formats to allow interoperability with other platforms (Cyber Range, Cyber Products, ...). https://www.amossys.fr/
CDEX		Customisable cyber range platform based on OpenStack. Medium amount of available scenarios. https://cdex.cloud/

Commercial off the Shelf (COTS)

Platform	Company	Description
Paideusis	**CINI**	PAIDEUSIS is a cyber-range mainly oriented to cybersecurity education, training and research; it is also used to host CTF competitions. PAIDEUSIS provides users with scenarios to address both hardware security issues, such as side-channel attacks and hardware trojans, and software security topics. Scenarios are built mixing emulation and real devices, so that users can be involved in hardware security activities that cannot be done by means of simulation. The cyber range is fully accessible remotely, allowing to reach a much larger pool of users that would be otherwise impossible to involve given the physical nature of hardware security topics. Future development includes the introduction of scenarios concerning OT environments. It is also possible to get in touch with CINI to cooperate in the design and implementation of fully customized scenarios.
CITEF	**RHEA**	CITEF is RHEA's proprietary cyber range solution. The platform's flexibility allows for the creation of totally customizable cyber ranges scenarios to meet different client needs, including training to anticipate and mitigate cyber attacks, testing infrastructure updates (e.g patches, updates) compliance (e.g. product testing) and R&D activities. The platform allows the creation and customization of virtual and hybrid scenarios. A large, vendor agnostic library of assets enables users to create environments that truly reflect their own infrastructure, a first step to create digital twins. New assets can be added and customized easily. The already available, rich, scenarios library and related training curricula (with different levels of difficulty) is in constant expansion. Train-the-trainer, custom scenarios and other ad-hoc professional services options are always available and give clients the freedom to build the cyber range configuration to best meet their needs. CITEF is available on-prem or as-a-service. CITEF's technology and RHEA's strong expertise on cyber range solutions were key to being selected by the European Space Agency to build their Space Cyber Centre of Excellence. https://www.rheagroup.com/services-solutions/security/cybersecurity/cyber-range/

Commercial off the Shelf (COTS)

Platform	Company	Description
Coliseum	**Talgen/ Nortal**	Talgen Cybersecurity is a Nortal Group's arm focused at a bespoke cybersecurity solutions. Talgen has designed, developed and holds a license for the next-generation NATO Cyber Range platform, a flexible, operationally relevant and representative Digital Twin automation environment that allows integrated simulation, training and collaboration for a wide variety of blue and red team cyber mission exercise areas, enabling practitioners the ability to securely collaborate and refine their tools and tactics on-premise or remote. https://www.talgen.com/
CYS4 - SOC CyberRange	**CYS4**	CYS4 has created a unique Cyber Range platform that helps SOC analysts to recognise and understand SIEM alerts & attack chains upon real-world scenarios. Our cutting-edge exercises teach different methods to detect and immediately catch any possible cyber threats. The experience gained in our labs will take you to the next level. The learning paths are based on the MITRE ATT&CK® Framework. We keep pace with the latest world incidents, carefully analyzing & simulating the attacks, to finally develop the most advanced training content. Students are also allowed to shape their tailor-made growth paths. Our education experience embraces the continuous learning model. Labs & documentation are accessible at any time. The platform fosters the students' engagement with its Gamification approach; it assigns points, trophies, and certifications, inspiring users to keep learning and stimulating a competitive atmosphere. SOC analysts can benchmark their performance & expertise through in-depth analytics, endlessly improving their knowledge. https://www.cys4.com/

Commercial off the Shelf (COTS)

Platform	Company	Description
CybExer Cyber Range Platform	**CybExer Technologies**	CybExer Technologies' NATO-awarded Cyber Range Platform provides realistic environments for exercises, trainings, security/technology testing and other simulations. This highly scalable, flexible and high availability cyber range platform gives the client maximum flexibility for the use of the cyber range. There are no limitations to the number of users, scenario configurations, or number of iterations. The only limitation is the computing power of the underlying infrastructure. Alarge portion of a range's functionality comes from the content (either virtual or actual hardware-based) it can create, deploy, and manage. CybExer's platform includes a large target library and features that enable integration of special systems or creating custom scenarios. The platform consists of three key software components for orchestration, automation, and visualisation. • ISA – Provides situational awareness on the environments that are deployed on the cyber range. That includes granular visuals on each individual environment, instant updates on their status, detailed timeline view of activities. The solution provides near real-time visualisation and comparison of exercise data. • vLM – Handles the deployment and management of game scenarios. It is also used as the development tool for preparing and creating new targets. • vLM-UP – Enables the trainees to have access to the virtual machine consoles and perform virtual machine operations like revert to snapshot, reset, power on etc. CybExer's solution has been tested out and used by many demanding clients such as the NATO, EDA, and various defence forces and ministries. The platform has flexible service models keeping in mind the needs of the client (e.g., SaaS, on-premise hosting, cloud hosting). https://cybexer.com/products/cyber-range/
CYBER RANGES	**Silensec**	CYBER RANGES platform delivers the ability to create, share and deliver, realistic hands-on scenario training. The platform can serve both individuals and thousands of simultaneous users, either as a cloud-based application, or an on-premise solution. CYBER RANGES is currently equipped with many of realistic hands-on scenarios, of varying difficulty levels (from novice to complex enterprise setups), and the scenario library is being updated constantly. https://www.cyberranges.com/

Commercial off the Shelf (COTS)

Platform	Company	Description
Cyber Range Laboratory	**Tecnalia**	Pioneering facilities in Europe, dedicated to training personnel and research, and developing and validating new cybersecurity technologies in a virtual environment (cyber range). New cyber-range infrastructures are advancing to include real industrial control systems that allow the execution of more realistic cyber-range exercises. This is the case of TECNALIA´s cyber-range laboratory (https://www.tecnalia.com/en/infrastructure/cyber-range-laboratory) integrated with the electrical grid cybersecurity laboratory (https://www.tecnalia.com/en/infrastructure/electrical-grid-cybersecurity-laboratory) for the energy domain, which are part of the Cybersecurity Node of the Basque Digital Innovation Hub (BDIH) (https://basqueindustry.spri.eus/en/basque-digital-innovation-hub/).
Cyber Trainer	**Leonardo**	Cyber Range is a multifunctional on premise operating environment with the aim of creating realistic training scenarios using advanced virtualization techniques. The goal is to test new attack and defense techniques, as well as verify the tools and processes used to protect technological systems. It also supports cooperative, competitive and technology evaluation processes based on the integration with external virtual and physical environments. It can be used to implement a "digital twin" of real infrastructure/system with the possibility to integrate real physical environment also. Cyber Trainer is a platform designed to provide educational contents and training sessions on topics in the Cyber Security field addressed to a heterogeneous audience. It supports users throughout the whole training process: from the identification of training needs, to formal learning, from the practical application of acquired knowledge (through "virtual lab" functionality), to the certification of skills, offering social tools that allow each user to keep up to date on the topics of greatest interest in a continuous and autonomous way. The combination of the above solutions enables the delivery of a range of simulation & training services for a broad range of use cases (Cyber IT and cyber Physical/OT) with different level of complexity. https://cybersecurity.leonardo.com/en/home

Commercial off the Shelf (COTS)

Platform	Company	Description
Diateam HNS	**Diateam**	Creator of the HNS Platform since 2008. (use the HNS-Platform) (Associated also with THALES "Thales CYBER RANGE powered by DIATEAM"). The platform seems to be flexible and the service is mainly marketed for custom private ranges. The company also operates professional training centers in Paris and is now partner with Thales, opening traning centers in Belgium and building a Range for Dutch MOD. https://www.diateam.net/
hackrocks	**hackrocks**	hackrocks is a Cyber Security Training platform with laboratories, challenges, competitions Capture The Flag (CTF) and much more. hackrocks is focused on the training of technical profiles through hands-on scenarios like Attack vs Defense or Jeopardy competitions. With a unique method, hackrocks can provide a white label platform with different scenarios or even create custom ones on demand. Website: https://hackrocks.com Demo: https://hackrocks.com/ctf/demo
NCR (Norwegian Cyber Range)	**NTNU (Norwegian University of Science and Technology)**	The Norwegian Cyber Range (NCR) is an arena for testing, training, and practicing cyber security. In NCR, users and systems are exposed to realistic events in a safe environment. The NCR offers training and testing across various levels of abstractions, from strategic decision-making perspective into low-level operational training. https://www.ntnu.edu/ccis/center-for-cyber-and-information-security

Commercial off the Shelf (COTS)

Platform	Company	Description
Realistic Global Cyber Environment (RGCE)	**JYVSECTEC**	Realistic Global Cyber Environment (later RGCE) is a fully functional live cyber range. RGCE brings together a realistic global world and real organization environments in an isolated sandbox which utilizes modern ways to combine virtualization techniques, physical devices, and business specific systems. The cyber range provides realistic Internet, corporate environments, threat actors' attack campaigns, automated user simulation, and tools and technologies for training and exercise purposes as well as research and development. It is also possible to create tailored environments for organization's specific training, exercise, or research and development needs. https://jyvsectec.fi/cyber-range/overview/
WithSecure Playground	**WithSecure**	WithSecure™ Playground is a global, on-demand SaaS platform for hands-on cybersecurity training, research and Capture The Flag exercises. Its versatile labs and curated courses canbe used to train both offensive and defensive teams, such as developers, pen-testers, and threat hunters, from novice to advanced. Playground labs are on-demand, dedicated sandboxed training environments. For example, Attack Detection Lab is built for attack detection and security operation personnel and offers a full corporate environment with an Active Directory forest, workstations and servers, where the learners are guided through simulating attackers' TTPs and analysing the evidence left to hunt for attack traces. Playground training content is organised into learning pathways. Users can progress through different levels of our standard pathways – application security, attack detection, and penetration testing – developing confidence and competence along the way. Custom pathways can be designed for specific needs, with support of experienced WithSecure consultants. https://www.withsecure.com/en/solutions/security-training/withsecure-playground

Open Source

Platform	Description
DETER/DeterLab	Built with emulab it provides a state-of-the-art scientific computing facility for cybersecurity researchers engaged in research, development, discovery, experimentation, and testing of innovative cyber-security technology. To date, DeterLab-based projects have included behaviour analysis and defensive technologies including DDoS attacks, worm and botnet attacks, encryption, pattern detection, and intrusion-tolerant storage protocols. Did not seem like an active project. https://deter-project.org/about_deterlab
EDU Range	This range is very appropriate for cybersecurity education market. They provide the code via github and you can host the range on your own server on the cloud or laptop. http://www.edurange.org/
KYPO Cyber Range	CONCORDIA H2020 released the KYPO Cyber Range platform as open sources. Very focused on education as well, removing the high cost of most cyber range solutions. You need open stack and openID connect provider to install platform. https://crp.kypo.muni.cz/
UNIGE CRACK Multidomain CyberRange (CRACK MCR)	UNIGE CR is the Cyber Range developed and hosted by the Computer Security Laboratory (CSECLab - https://www.csec.it/) at the University of Genoa. CRACK MCR fosters education, training, and testing by providing multi-domain scenarios that integrate, among others, complex IT/OT infrastructures, a simulated Cloud Computing environment, mobile devices, and Security Operation Centers (SOC) facilities. It also focuses on maritime cybersecurity by interfacing with the ShIL-Ship-In-the-Loop research infrastructure (https://shil.diten.unige.it/) to simulate microgrids and port assets and provide an accurate ship digital twin through a realistic full bridge simulator. To create, deploy, and refine such rich and heterogeneous scenarios, CRACK MCR relies on open-source frameworks exploiting automation, verification, and testing capabilities, e.g., CRACK - Cyber Range Automated Construction Kit (https://github.com/enricorusso/CRACK) and LiDiTe-Lightweight Digital Twin Environment (https://github.com/CSecLab/LiDiTE/). CRACK MCR also offers the infrastructure components to manage the scoring and the situational awareness dashboards and automates some of the yellow team activities. It operates for hands-on activities during institutional courses and for hosting Capture-The-Flag competitions and Cyber Defence exercises. Lastly, it is extensively used for testing in the field of maritime cyber security with the involvement of seafarer operators as well. Such an activity made it possible to discover novel cyberattack techniques against ships' sensors and equipment and develop effective countermeasures.

Open Source

Platform	Description
UNINA Docker Security Playground	The Docker Security Playground is a framework that allows for the creation of container-based interactive scenarios based on complex network infrastructures. It can be leveraged for hands-on training in the cybersecurity field. Docker is the adopted container technology, which is lightweight and allows to: (i) reproduce real-world networking scenarios; (ii) build ad-hoc network playgrounds involving vulnerable nodes/services and malicious users/tools; (iii) provide lab participants with low-cost, COTS-based, easily reproducible networking tools. The platform is available at: • https://github.com/giper45/DockerSecurityPlayground.git It is also shipped with a list of interactive laboratories that cover a variety of security related topics, each one to be explored with a hands-on, offensive approach: • https://github.com/NS-unina/DSP_Repo • https://github.com/giper45/DSP_Projects The former repository contains labs that cover the basics for aspiring penetration testers, such as Scanning and Enumeration techniques, useful tools as well as exploitation techniques. The latter is made up of hacking labs and Capture The Flag challenges, such as those presented at Arsenal Black Hat 2018 (Las Vegas) and 2019 (London).

Open Source

Platform	Description
Vigrid	Vigrid(1) is an extension of the GNS3(2) (Graphical Network Simulator) tool adding industrialization for massive usage. Over an ergonomic and easy to use GUI (web or heavy client), anyone can use gns3 to create projects hosting virtual machines over Qemu or docker. Each project works on its private network but can bind to real interfaces to communicate with the real world if needed. GNS3 also includes features such as network link control (disturbance, bpf filtering...), console access to VM with mouse & clean keyboard control. Vigrid combines available best open source technologies to open GNS3 to a new universe. On the network side, Vigrid extends GNS3 to a Cyber Range Blue/Red Team design with various network configuration mixing user and admin LANs. Network layers are ready for new features : load balancing, new LANs for other uses... About emulation, Vigrid also adds capabilities to emulate mostly any CPU (x86/amd64 but also ARM, PowerPC etc), offering new virtual machines such as Android, Pi, IoT. This also includes shared GPU access for VM. This includes the power to emulate commercial hardware from many vendors. For more industrial usages, Vigrid provides its own NAS technology able to support thousands of running projects/VM at a time with snapshot and massive diskless cost cloning features. Over this design, it becomes possible to use an unlimited heterogenous bare-metal servers to host GNS3 project clones. Organized as a library, projects can also be stored for a later usage or sharing. Through a simple WWW GUI, Vigrid will permit clientless console access to VM, project/node/links control and all functions related to snaping shot & cloning. Permanently evolving, GNS3 & Vigrid will soon offer RBAC (currently tested in alpha version) which is a strong need requested by its many users. Other parallel projects also benefit to Vigrid are ongoing, such as 'Puppet Master', a framework using Caldera to scenarize actions of discrete agents hidden into Vigrid projects. Vigrid is opensource, free and its only purpose is to help as many as possible. Many new ideas have been technically validated and all contributors are welcome to join the adventure. Vigrid is already used in multiple different usages: presales demos, tests, trainings, engineering, forensics/audits, events, etc. As host of Orange Group "Capture The Flag" events, Vigrid permits each team on the hundreds to work on its own private network and virtual machines to face more complex challenges than usual with equal chances. (1) https://github.com/llevier/vigrid (2) https://github.com/GNS3

REFERENCES

[1] European Cyber Security Organisation (2020), Understanding Cyber Ranges: From Hype to Reality, https://www.ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[2] The Cyber Range : A guide – Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training, https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf

ECS

EUROPEAN CYBER SECURITY ORGANISATION

www.ecs-org.eu

company/ecso-cyber-security

@ecso_eu