ECS

EUROPEAN CYBER SECURITY ORGANISATION

MAY EDITION

AWARENESS CALENDAR

Cyber ranges & range-enabled services

Awareness Calendar **CYBERSECURITY**

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO Members' and Partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2022 are planned as follows:

- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management

DID YOU KNOW?

- 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. READ MORE.

- In 2021, ECSO launched a Call to Action to kick start an initiative to identify and bring together European cyber range providers and end users. The aim is to consolidate the approaches of European cyber range-enabled services' exercise methodologies 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 solutions. READ MORE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

Accenture Cyber Ranges- May 2022

Industrial process control networks remain vulnerable to cyber-attacks, as traditional IT equipment must now integrate reliably and securely with aging field systems, while fending off sophisticated attacks. This is where cyber ranges come into play, as they offer companies the ability to test and stage the responses of industrial process controls against sophisticated attacks in a risk-free setting. They enable clients to better orchestrate changes to their OT environment, including threat response exercises to train their teams to more effectively recognise, mitigate and repel attacks. Accenture has expanded its cybersecurity capabilities with three cyber ranges to help industrial companies.

- "Accenture Expands Cybersecurity Capabilities with Network of "Cyber Ranges"
- "Tradition meets Innovation-Essen Industry X Innovation centre".
- Learn about Accenture's ICS Cyber Range in Houston – YouTube
- Cyber Defense I Accenture

CyberRange by AIRBUS Cybersecurity

The CyberRange of Airbus CyberSecurity is an integration and simulation platform for IT & OT systems that allows you to build and run complex simulations tailored to your needs:

Design: design of real or representative IT & OT systems, integration of existing equipment or from your own system, light client accessible from a web browser, configuration management of your component library, import and export capability to exchange your designs and hybrid modelling by coupling physical and virtual systems.
Realistic simulation: replicate activities representative of your operations and conduct penetration tests in an isolated environment, create and orchestrate complex scenarios of realistic actions, take advantage of a comprehensive library of customisable actions (Cyber-attacks, Traffic generators, Tests) and take advantage of the ready-to-use IT and OT libraries and scenario examples.
Collaboration: multi-site collaborative teamwork, management of multiple and isolated workspaces, with access rights per user and community portal for resource sharing (VMs, Topologies, Scenarios). READ MORE.

CYS4 Cyber Range for SOC Analysts

CYS4 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 analysing & 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. READ MORE.

Cyber Range Courses Available with (ISC)²

(ISC)² offers lab courses designed to help build necessary technical skills in cyber security. Lab courses include a NEW Introduction to Image File Forensics and File Allocation and Tracking in MTFS, as well as Follow Allocation and Tracking in FAT32 and Accessing Application Security.

Participants will use real tools, real attacks and realistic scenarios to hone their skills in a virtual space. Each Lab begins with an instructional video to guide learners through the relevant content and reviews background information needed to complete the Lab assignment. Participants who successfully complete all Lab activities, submit a course evaluation and score 70% or higher on the final assessment can earn continuing professional education (CPE) credits to support their (ISC)² certifications. Courses are free for (ISC)² members and available for purchase for non-members.

READ MORE about the courses currently being offered with (ISC)².

Realistic cyber-range for Operation Technologies

tecnalia

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Nowadays, the role of workers is essential to ensure cybersecurity in any company and, for that reason, there is a clear need for workers in any sector to have the necessary knowledge to try to prevent, detect and respond to cyber-attacks. For this purpose, new training tools, such as cyber-range, become very relevant. However, traditional cyber-range infrastructures, mainly based on virtualised elements, have realism limitations, especially when considering Operation Technologies. Therefore, there is a need to move forward and develop new infrastructures that include “real elements” with “real responses” in “real time”. In this sense, 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 integrated with the electrical grid cybersecurity laboratory for the energy domain, which are part of the Cybersecurity Node of the Basque Digital Innovation Hub (BDIH).

WITH SECURE™ Playground

A Platform for Developing Cybersecurity Skills

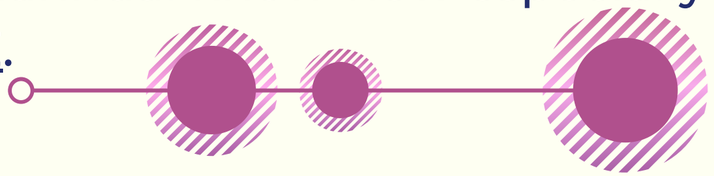
WithSecure™ Playground is a global, on-demand SaaS platform for hands-on cybersecurity training, research and Capture The Flag exercises. Its versatile labs and curated courses can be used to train both offensive and defensive teams, such as developers, pen-testers, and threat hunters, from novice to 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.

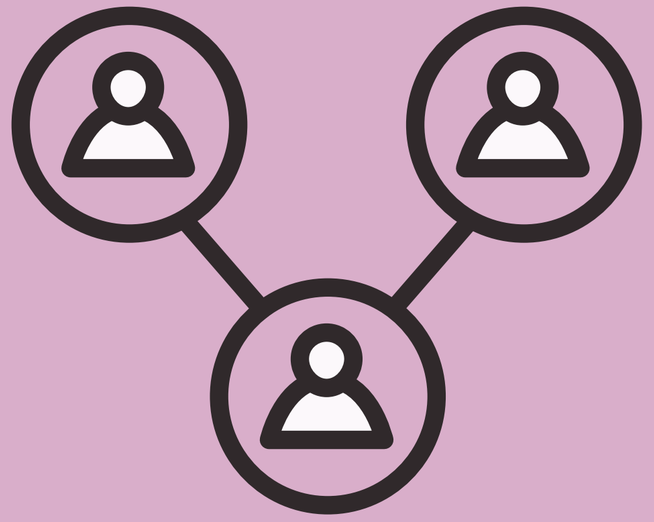
Playground training content is organised into learning pathways. Users can progress through different levels of our standard pathways – application security, attack detection, and penetration testing – developing confidence and competence along the way. Custom pathways can be designed for specific needs, with support of experienced WithSecure consultants. READ MORE.

Zanasi & Partners
Security Research and Advisory

The Capacity Capability Map of the ECHO Federated Cyber Range

Within the scope of the EC-funded project ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations), Z&P took part to the development of the ECHO Federated Cyber Range, a marketplace of multi-sector services coming from multiple cyber ranges to be applied in several areas (e.g. Healthcare). In particular, Z&P focused on the implementation of the Capacity Capability Map, an essential microservice that manages all the capabilities and capacities of the interconnected cyber ranges and that is able to reserve resources for a certain customer, in order to allow him to perform the requested service. Zanasi & Partners is a company leader in Europe in the field of security/defence research and advisory services. Incorporated in Italy with a foothold in France and active internationally, the company can rely on multiannual know-how especially in artificial intelligence, cyber and physical security. READ MORE.





RESOURCES FROM THE COMMUNITY

How to design your hands-on cybersecurity training? CONCORDIA will help you!

Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA H2020 project released an open-source KYPO Cyber Range Platform (KYPO CRP). It is an impactful tool; however, we decided to help our community even more. We have prepared educational content, new powerful tools and webinars in May, which will show everyone how to design their hands-on cybersecurity training. READ MORE.

Cyber Ranges for Hands-on Training

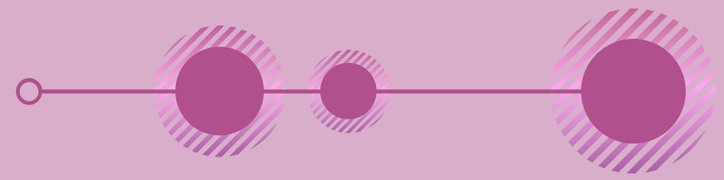
Sababa Security

With cybercrime on the rise, it is no longer a matter of whether a company will be attacked, but when it will happen. The threat landscape is becoming increasingly complex, while enterprises are struggling to hire and keep cybersecurity experts. Find out how cyber ranges can improve your overall security posture. READ MORE.

SPIDER
5G CYBER RANGE

a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

SPIDER H2020 project delivers a novel 5G CyberRange-as-a-Service platform which targets 5G deployment and will assist security professionals of various levels to enhance their skills being trained under realistic conditions. SPIDER Cyber Range offers a synthetic and sophisticated war-gaming environment. Main features include advanced simulation and emulation tools, novel training methods towards active learning, as well as generation of improved risk analysis and econometric models based on emulation of modern cyber-attacks.



THANK YOU

for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu