ECS
EUROPEAN CYBER SECURITY ORGANISATION

# Cybersecurity Awareness Calendar

# CYBERSECURITY EXERCISES

July 2021

# 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 2021 are planned as follows:

- January – Phishing
- February – Internet of Things
- March – Cloud Security
- April – Malware
- May – Ransomware
- June – Cybersecurity Skills
- July – Cyber Exercises
- August – Cybersecurity Summer School
- September – Mobile Devices & Bring Your Own Device (BYOD)
- October - Gender Diversity in Cyber
- November – Safe User Authentication & Password Hygiene
- December – Cybersecurity Trends 2022

# DID YOU KNOW?

## About Cybersecurity Exercises

- Cyber exercises can be divided into 'Capture The Flag' (CTF) and live-fire exercises. CTF are usually organised in attack and defence style where individuals or teams have to find and fix vulnerabilities in their own systems while simultaneously attacking systems that belong to other participants. Live-fire cyber exercises enable teams to train cyber professionals to detect and mitigate large-scale cyber-attacks while being constantly attacked by a "red team" of hackers. ECSO Paper "Understanding Cyber Ranges: From Hype to Reality"
- ENISA manages a programme of pan-European exercises named Cyber Europe which is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate to become cyber crises.
- A cyber range is a simulation environment or platform that can be used for a variety of purposes, including to run cyber exercises and competitions. ECSO recently launched a Call to Action to gather the cyber range community and consolidate the European cyber range market and services.

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

# RESOURCES FROM ECSO MEMBERS

accenturesecurity

# ACCENTURE CYBER RANGES

- “Why Security Teams turn to Cyber Range technology as online threats grow”
- “Tradition meets Innovation-Essen Industry X Innovation centre”
- (2) Learn about Accenture's ICS Cyber Range in Houston - YouTube
- Cyber Defense I Accenture
- “Accenture opens three “cyber ranges” to improve the security posture of industrial organizations”

Industrial process control networks remain quite vulnerable to cyber-attacks, traditional IT equipment must now integrate reliably and securely, aging field systems while fending off increasingly sophisticated attacks. Challenge lies in the fact these increasingly sophisticated attacks are aimed against remote, difficult-to-protect IoT systems that are so critical to daily life that taking them offline to test against cyberthreats is virtually unfeasible.

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. In addition, the Cyber Range enables clients to better orchestrate changes to their Operational Technology (OT) environment, including threat response exercises to train their teams to more effectively recognise, mitigate and repel attacks. The need to simulate highly individualised systems means having every possible tool on the metaphorical shelf, including programmable logic controllers, distributed control systems, SCADA systems, remote terminal units, human-machine interfaces and more. This level of customisation gives ability to ability to simulate uniquely configured industrial control systems and run any number of tests to find weak points.

# TEST YOUR ORGANISATION'S CAPACITIES AND DEVELOP YOUR CYBER RESILIENCE THROUGH CRISIS MANAGEMENT

AIRBUS

Crisis Management Exercise is a set of techniques and means that enable an organisation to prepare, manage and resolve a cyber crisis. The objective is to improve the structure, procedures, communication and coordination of an organisation through lessons learned.

CYBERSECURITY

Crisis Management

CyberSecurity

## Test your organisation's capacities and develop your CyberResilience through Crisis Management

- Customisable scenarios tailored to your business
- Cyber-attacks based on real-life cases
- A simulated crisis involving all of your services
- Animation by our cyber experts
- Feedback and complete report on lessons learned

## The objectives and benefits of Crisis Management training

Meeting legal requirements

Reassuring and/or engaging its ecosystem

Raising awareness internally

Training and/or coaching staff

Testing the cyber crisis management system

CRISIS MANAGEMENT

- Cyber crisis management does not only involve technical functions, but the entire organisation
- Training and education are necessary to prepare for effective crisis management
- Conducting cyber crisis management exercises requires expertise
- Airbus CyberSecurity is an experienced partner capable of supporting you in this process

## Airbus CyberSecurity

A leading European provider protecting EU institutions

An end-1-end integrator for IT and OT industrial cyber security

A trusted partner for Airbus, Governments and Critical Industries

Unique experience with platform security and embedded systems

AIRBUS

More here

Région
BRETAGNE

PÔLE D'EXCELLENCE
CYBER

eurobits
Europäisches Kompetenzzentrum für IT–Sicherheit • Bochum

BASQUE CYBERSECURITY CENTRE

EUSKADI
BASQUE COUNTRY

tecnalia Inspiring Business

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

CYBEXER TECHNOLOGIES

# FEDERATED CYBER RANGE

## First application of Cyber Range for the Healthcare sector

The Federated Cyber Range project concept is issued from the output of the "Cyber Pilot Action program" led by Brittany and 4 other Regions in 2018-19. There are two priority sectors: Healthcare and Energy.

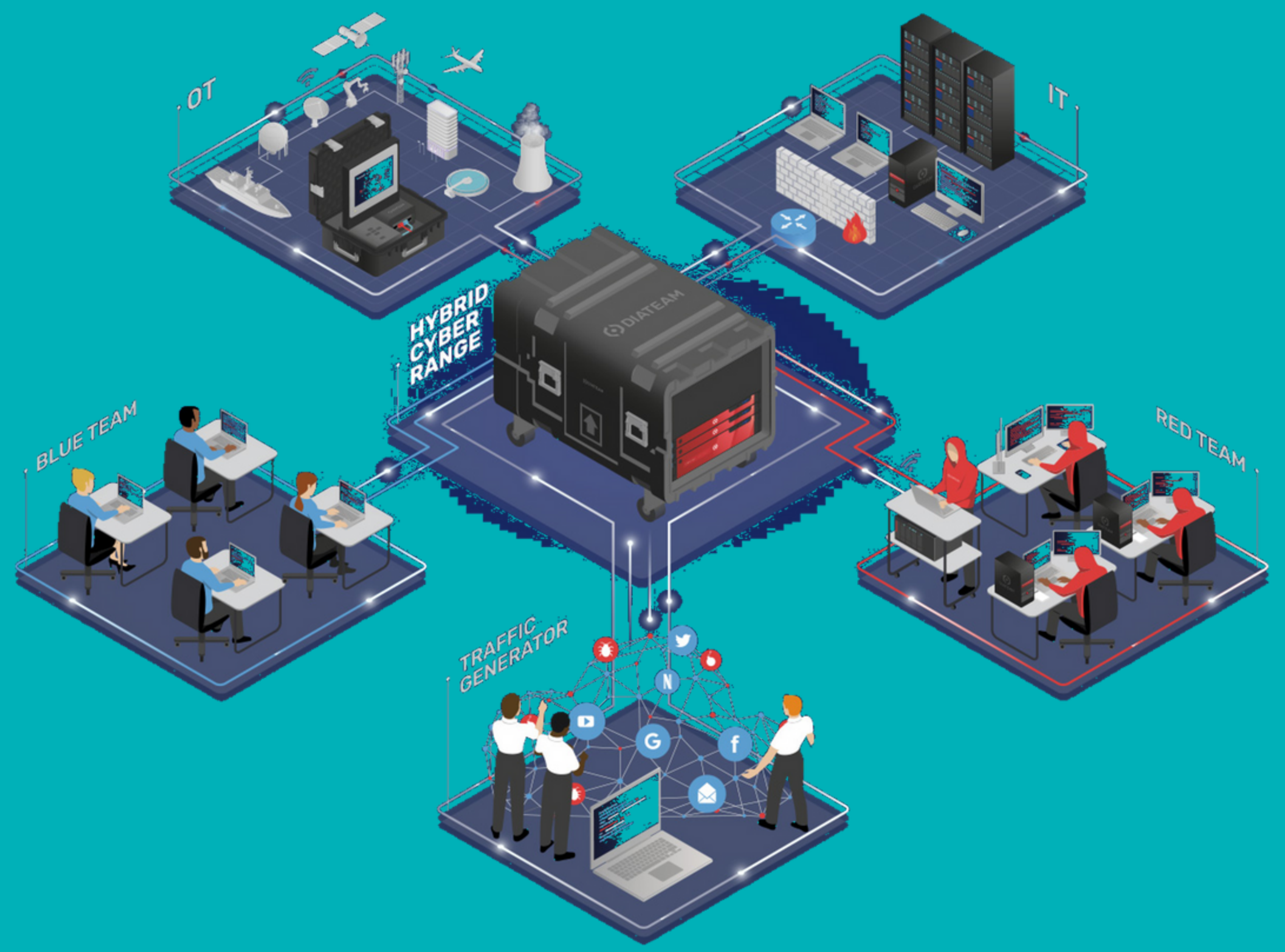
The idea is to leverage the Cyber Range facility as a simulation platform to test existing and innovative security solutions of complete IT/OT systems.

The project was supported by the Technical Assistance Facility (TAF) from the S3P-Industry platform to work on a market study methodology, a business plan, and a governance note with business experts.

*Latest news: A first* implementation will be rolled out under a collaborative project between SMEs and two hospitals in Brittany. Two use cases will be studied : monitoring patient and patient journey chain. The next step will be to interoperate with two Cyber ranges.

DIATEAM

# HANDS-ON CYBER TRAINING THROUGH IMMERSIVE HYBRID CYBER RANGE



**Founded in 2002, DIATEAM is the French historical creator of cyber range and hybrid simulation systems for cyber defence.**
**A cyber range is a virtual environment that enables organisations to simulate cyber combat training, system/network development, testing and benchmarking.**

**The DIATEAM cyber range offers a complete simulation environment to:**

- **empower customers' cyber skills;**
- **train operational teams;**
- **improve responsive capacity in case of a cyber crisis;**
- **connect any network equipment for testing and prototyping.**

**Learn more at www.diateam.net**

HERMESBAY
enhanced awareness

# CYBER EXERCISES FOR CYBER AWARENESS

More here

The incidence of the human factor is a crucial element in information security management.
Hermes Bay supports the development of cyber-awareness through the deployment of conventional and unconventional training techniques. Each technique is selected following a thorough analysis of the internal and external factors impacting the organization. The analysis is composed of two macro-phases:

- Cyber Threat Intelligence: aimed at identifying the awareness theme that best suits the organization
- Context Analysis: analysis of the structure and processes of the organisation and adaptation of the case studies to the given context.

In relation to the corporate roles involved in the exercises, Hermes Bay proposes:

- Passive techniques: this category includes passive role-plays and seminars. In the former scenario, role-plays, the target audience attends an event run by a group of non-professional actors who stage the management of a security event in a company. The latter scenario, seminars, involves the presentation by operators of "life experiences" lived during a critical event/emergency. Passive techniques are mostly addressed to the company's Top Management and are aimed at conveying experience through identification.
- Active Techniques: this category involves tabletob simulations and operating simulations. This type of simulation is based on the use of dynamic story telling techniques that allow to adapt the development of the scenarios presented in relation to the operational choices of the participants. Active techniques are aimed primarily at operational staff and middle management, promoting methods of learning by doing.

# PRACTICE MAKES THE MASTER

incibe_

SPANISH NATIONAL CYBERSECURITY INSTITUTE

Exercising is the best way to become stronger. This is also true in cyberspace. To make it hard for cybercriminals to hack us, repeat this routine until you became expert. These are a set of cybersecurity exercises from The Spanish National Cybersecurity Institute (INCIBE):

- For children and educators: Test exercise for parents to check knowledge of risk situations for children and young people on the Internet. Available here.
- For anyone at home: Do you know as much about cybersecurity as you think? Test yourself here.
- For those who want to be CS professional: Participate with your friends in these cybersecurity challenge trainings. We will launch a new call shortly. Start building your team! Available here.
- For SME's: There is a new section 'TemáTICa – Incident response management' that gathers resources to help employees and business owners to strengthen their cyber resilience capabilities. Available here
  NOTE: All resources in Spanish.

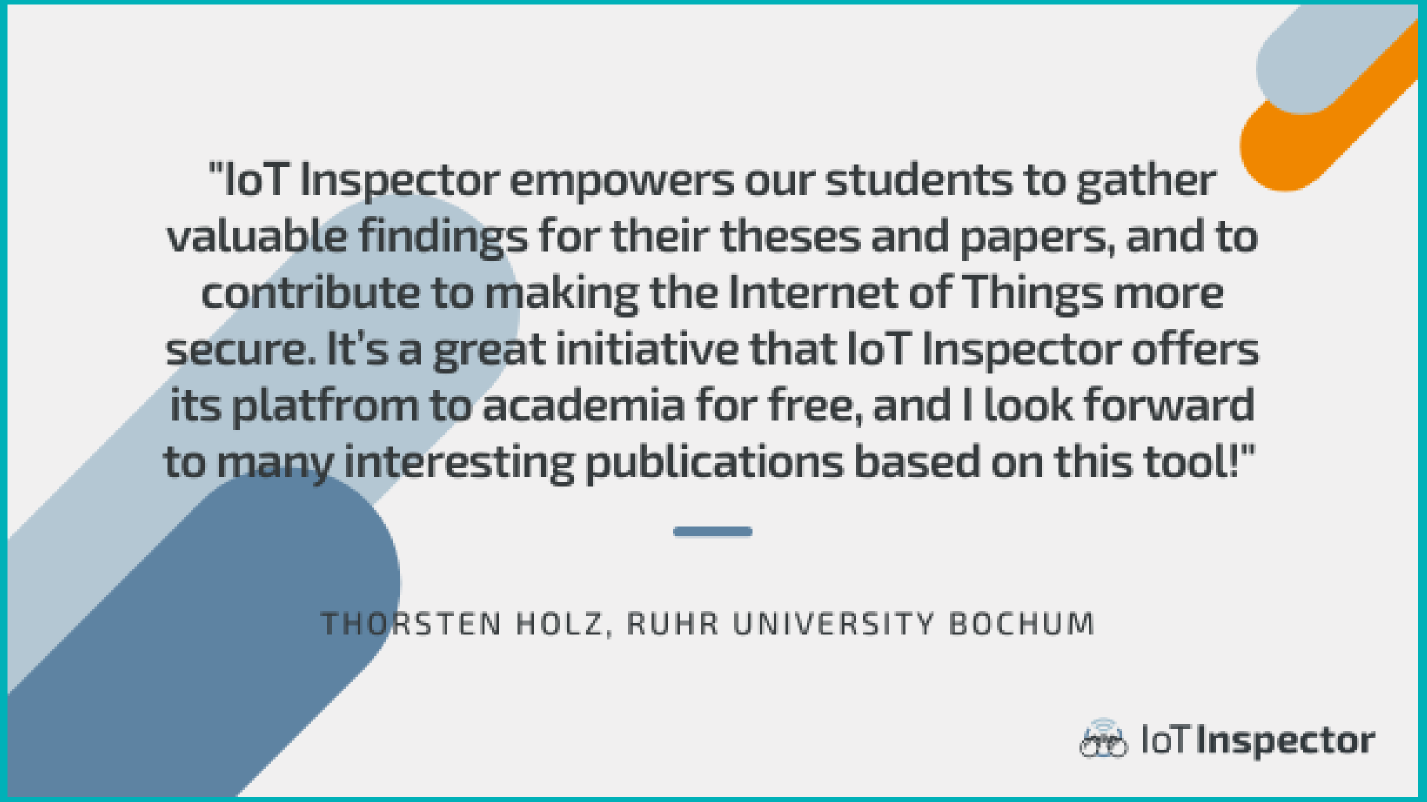
IoT Inspector

# A RANGE OF CYBERSECURITY LEARNING OPPORTUNITIES AVAILABLE

**IoT Inspector is the leading European platform for automated security analyses of IoT firmware. It is the easiest way to examine the device's firmware for vulnerabilities and its compliance with international security standards.**

**Due to enormous interest from research and academia in our security analysis platform IoT Inspector, we decided to make it available to students, teachers, and academic researchers – totally free of charge. We hope that many curious minds will benefit from our IoT firmware analysis platform for their university projects or personal research, and join us in our mission to #makeIoTsecure.**

**LinkedIn / Twitter**



"IoT Inspector empowers our students to gather valuable findings for their theses and papers, and to contribute to making the Internet of Things more secure. It's a great initiative that IoT Inspector offers its platfrom to academia for free, and I look forward to many interesting publications based on this tool!"

THORSTEN HOLZ, RUHR UNIVERSITY BOCHUM

IoT Inspector

**#makeIoTsecure**

# CYBERDRILLS @ RABOBANK

Rabobank employs a Cybersecurity Crisis Organisation.
For the most critical incidents that cannot be resolved as part of normal operations, special teams are started.
In order to train these teams, we employ training sessions. In these sessions, the incident responders are trained based upon common attack scenario's. These trainings help responders to get used to the process. It also provides opportunities to improve the process.

# LUXEMBOURG IS ABOUT TO LAUNCH ITS CYBER RANGE IN OCTOBER 2021

SECURITY MADEIN.LU

circl.lu cases.lu c-3.lu

*"You can compare it with a flight simulator where you can simulate and train different scenarios of attacks in a realistic environment"*, Ben Fetler, Cyber Defence Principal Advisor at the Luxembourg Directorate of Defence

Luxembourg decided to create a Cyber Range so that cyber experts can train in a virtualised but realistic environment. But not only cyber experts from Luxembourg. Luxembourg wants to create a competence center with it, in order to offer it to other nations, critical infrastructures and operators of essential services. The objective is to make sure that experts get to know each other and are able to efficiently work together in the event of a major crisis.

The Luxembourg Cyber Range includes various aspects:

- training: extending knowledge in a specific domain, identifying gaps
- exercising: trying skills and collaboration in exercises such as Locked Shields
- security testing: testing new solutions

More here

SIEMENS
energy

# SIEMENS ENERGY SUPPORTS HIGH LEVEL CYBER DEFENSE EXERCISE

Siemens Energy was one of a few companies to support the "Locked Shields" high-level cyber defense exercise conducted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in April 2021. Experts from SE CYS simulated, among other things, an attack on key energy infrastructure facilities.

The international "Locked Shields" cyber defense exercise has been conducted annually by the CCDCOE since 2010 and is considered to be the most complex technical live-fire challenge in the world. The aim of the participating countries is to enable cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks.

The exercise focused on power generation and distribution facilities, 4G and 5G communication systems, maritime surveillance, water purification plants, and other critical infrastructure components.

## Proven cooperation

Siemens has been supporting Locked Shields since 2017, and in the past has also provided power distribution control technology from the Spectrum Power portfolio for exercise purposes. In June 2020, Siemens Smart Infrastructure and the NATO CCDCOE announced the signing of a Memorandum of Understanding to continue cooperation in the field of cybersecurity for critical infrastructure.

As part of Locked Shields, Siemens Energy is cooperating closely with Siemens Smart Infrastructure to share lessons learned and, where appropriate, identify security gaps.

# RESOURCES FROM THE COMMUNITY

## TEST YOUR DEFENSES WITH THE PENETRATION TESTING

HWG
A Cyber Security Company

Penetration testing consists of an attack simulation, in which the security experts play the role of the hackers, attempting to breach a system using the tools and methods commonly used by cyber attackers. The aim is to identify any cybersecurity vulnerabilities the organisation may have before an actual attack happens.
MORE HERE (in Italian)

itrainsec
Learn from the best

## APPLICATION SECURITY ESSENTIALS LABS: COMMON AND CRITICAL VULNERABILITIES

To properly implement a product maturity program, organisations need to embed and grow security expertise. Cultivation of application security champions requires the right pivot point in the following topic: application bug hunting and mitigation strategy. ENROLL for itrainsec workshop in collaboration with HITB conference!

## IT IS TIME TO HARDEN ACTIVE DIRECTORY

Active Directory (AD) is used by large companies to automate multiple tasks and integrate assets. However, as an organisation develops, its AD structure becomes more complex and less transparent. Learn why and how to assess and harden AD.

More HERE.

## "CYBERSECURITY EXERCISES": IS YOUR IDENTITY AND ACCESS MANAGEMENT READY FOR SECURE DIGITAL TRANSFORMATION?

Are you currently managing your company's Digital Transformation? Are you unsure if you and your IT team have done all you can to prevent connected cybersecurity incidents? These 3 exercises will leave you with a clear path forward to ensure your company is able to identify and optimize key factors regarding the protection of your data from hacking and malfeasance connected to Identity and Access Management. More HERE.

THRIVE WITH EQ

# REAL-LIFE INSPIRED SCENARIOS TO EXERCISE THE HUMAN FACTOR OF CYBER SECURITY

Everything humankind does exists in polarity, as does the criminal mind. We may never eradicate cyber crime, but we must think faster and act prepared so we can recover and thrive quicker than before. Thrive with EQ's tabletop exercises help you build human readiness in the digital age.

More HERE.

# THANK YOU!

## for your time

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

www.ecs-org.eu

secretariat@ecs-org.eu

/company/ecso-cyber-security/

@ecso_eu