ECS
EUROPEAN CYBER SECURITY ORGANISATION

JUNE EDITION
AWARENESS CALENDAR

Cybersecurity for verticals

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?

- This month's topic "Cybersecurity for verticals" focuses on all vertical application sectors which help ensure the cyber resilience of our economy, infrastructure and services, such as energy, transport, health and digital infrastructure.

- On the 13th May 2022, the Council and the European Parliament agreed on measures for a high common level of cybersecurity across the European Union ("NIS2"), to further improve the resilience and incident response capacities of both the public and private sector. It sets the baseline for cybersecurity risk management across all sectors and lays down mechanisms for effective cooperation. READ MORE.

- ECSO built a Community of Verticals (CoV) providing an open forum of exchange to facilitate the dialogue between Users (operators, companies, governments) and Suppliers/Providers of cybersecurity solutions to understand cyber threats and needs, envisage possible solutions, and support implementation of trusted and resilient solutions for key verticals. READ MORE.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

Offers several options for Cybersecurity Verticals

(ISC)² offers security briefing webinars specific to cybersecurity verticals. One sector on which (ISC)² has several focused educational and informative webinars is the healthcare industry. These (ISC)² Security Briefings last 1 hour and provide an opportunity for attendees to take a "deep dive" into a specific topic related to cybersecurity. Webinars are available free of charge to (ISC)² members only. Members can immerse themselves in a topic and learn from industry experts as topics are addressed.

A Persistent Cyber Target for Threat Actors: Health Care
Darktrace #1: Cyber-Threats Facing Global Healthcare
Cybersecurity Roundtable In the Bullseye: Healthcare and Email Threat Actors
Additionally, (ISC)² offers a webinar on the topic of Third-Party Risk in the financial sector:
Continuous Monitoring for Third-Party Risk: A Customer Journey

A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures

Project FISHY delivers a coordinated framework for cyber resilience provisioning intended to guarantee trusted ICT systems supporting the supply chains, built upon distributed, dynamic, potentially insecure and heterogeneous ICT infrastructures. READ MORE.

Public Sector and Identity as the New Perimeter

Identity Management and Authentication (IAM) works together, you can't login if you don't exist!With a strong authentication and a verified identity, you can build trust in the digital world. However, it is key to keep the active directory in good shape and to be able to verify trust in the identity before we allow it into our access perimeter. Automated provisioning, delegated management and a degree of user self-service are keys to success. Public administrations, municipalities and healthcare sectors work with highly private, sensitive data where guarding this perimeter is of utmost importance. These public sector organisations need a unified digital strategy that puts identity into centre and enables citizens to access public services fast but safely. Secured digital identities tightly coupled with application-controlled network access enables an IT environment where the responsible manager can with certainty say who accesses what data, when and from where. This provides individualised security policies down to the access level, providing zero-trust network access control. READ MORE.

CitySCAPE

City-level Cyber-Secure Multimodal Transport Ecosystem

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

CitySCAPE will explore all different cybersecurity dimensions of multimodal transport. These dimensions will drive a characterisation of the cyber-threats in the ICT multimodal transport, extended to the close-by power and financial sector. Innovative software tools will be introduced to estimate the cyber-threats propagation in the system.

CitySCAPE introduces innovative risk analysis techniques and orchestrates a number of software solutions to realise an interoperable toolkit that seamlessly integrates to any multimodal transport system. More specifically, the CitySCAPE software toolkit will:

- Detect suspicious traffic-data values and identify persistent threats
- Evaluate an attack’s impact in both technical and financial terms
- Combine external knowledge and internally-observed activities to enhance the predictability of zero-day attacks
- Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

The solution will be tested in 2 use cases: Tallinn, Estonia & Genova, Italy. READ MORE.

CyberSEAS

Cyber Securing Energy dAta Services

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

CyberSEAS aims to improve the overall resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions, the extended involvement models of stakeholders and consumers as channels for complex cyber-attacks, the presence of legacy systems and the increasing connectivity of energy infrastructures, data stores and services retailers.

There are three strategic objectives: 1.Countering the cyber risks related to highest impact attacks against EPES; 2.Protecting consumers against personal data breaches and attacks; 3.Increasing the security of the Energy Common Data Space.

There is one open and extendable ecosystem of 30 customisable security solutions: 1.risk assessment; 2.interaction with end devices; 3.secure development and deployment; 4.real-time security monitoring; 5.skills improvement and awareness; 6.certification, governance and cooperation. Solutions are validated through experimental campaigns consisting of 100+ attack scenarios, tested in three labs before moving out to one of six piloting infrastructures across six European countries. READ MORE.

How 5G security can be your industrial virtual airbag

ERICSSON

Safety-related systems in industries aim to provide protection to critical assets including human life. Yet, as more industries become connected to the outside world, safety functions themselves need protection from intentional malicious attacks. This blog post looks into on how 5G security can fill the needs of security for safety, acting as a virtual airbag to help ensure correct and timely deployment of safety systems to prevent harm to people and critical assets. READ MORE.

Cybersecurity for verticals: Threats and Solutions

Cybersecurity can be considered for verticals as there is evidence of the rise of new cyber threats. Vertical Structures are tasked with understanding their current level of security information and data security. Cybersecurity for verticals includes penetration testing, information security, cybersecurity awareness and more. Any organisation, regardless of vertical, must protect its data. Targeted threats can generally be traced back to cyber adversaries that specialise on a particular industry in a particular area. A common factor among them is the large number of people with critical data so that cyber attacks can require significant money. In fact, Exprivia Cybersecurity Observatory through its Threat Intelligence analyses that cybercriminals focus mainly on stealing data and money. Exprivia Cybersecurity develops its own business processes and technology competencies suited to meet the needs emerging from this evolution, understanding the specific requirements of the vertical industry. READ MORE.

Verticals everywhere

For SMEs: The use of technology in organisations depends largely on their activity and how they do business in their specific verticals. At SECtoriza2, and also with the Itinerarios short videos, we provide specific guidelines and recommendations to anticipate the particular threats of each sector and avoid the possible negative impacts of incidents on your finances and reputation. Find your SECtoriza2 and Itinerario!

For children and educators: See this awareness campaign on cybersecurity and personal data treatment aimed at teachers. The set of resources includes articles, infographics, videos, tests and tips about the application of security measures, account protection, malware and online fraud prevention and the use of encrypt methods to keep students' personal information safe. READ MORE.

At home: “Senior Experience” is dedicated to all those who are experts in life, but aren't digital natives, to help them to enjoy Internet and technology safely. READ MORE.

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Self Sovereign Identity for Industry 4.0

In the Industry 4.0 ecosystem we find different types of entities that are related to each other and need to trust the information provided by third parties: companies, products and key assets in the processes, production resources like machines that must meet certain requirements, and even workers with specific skills to perform certain operations.

The SSI (Self Sovereign Identity) technology helps us to build the concept of interoperable digital identity in Industry 4.0 for production resources and industrial products. It contributes to create new models of relationships and exchange of credentials and attributes of products, components and assets in this ecosystem, as well as their information throughout their life cycle, from their conception to their operation. With SSI we built a system in which the statements made about the fulfilment of requirements in products and industrial resources can be reliably verified by third parties. READ MORE.

Cybersecurity for Autonomous Vehicle Systems

Security-critical applications, systems and services require standardised and certified products, systems and practices. This is also stated in the directives and regulations of the European Union. For example automotive directives and regulations impose requirements for third-party approval. The VTT Technical Research Centre of Finland is exploring and evaluating security threat modelling methods and testing tools for autonomous vehicles. VTT utilises its “War Room” laboratory, which is used for attacking the security wired and wireless interfaces of the devices under study. Test methods include service enumeration, penetration testing, DoS-testing, vulnerability scanning and protocol fuzzing which are customised for autonomous vehicle target systems. As a case study we are doing penetration testing on VTT’s driverless bus that is operated in the Tampere region. The attack surface extends also to the smart charging communication protocols used by charging stations of electric vehicles, as well as the web services used to control the charging process. READ MORE.

RESOURCES FROM THE COMMUNITY

High Priority IoT Firmware Cybersecurity for Telecom, Healthcare & Aviation/Avionics/Aerospace Organizations

IoT devices have become an attractive target for cyberattacks as they quite often lack security at their core (firmware). The large and rapid increase of IoT devices adopted by various organisations looking for improved efficiency also adds to the problem of IoT security. Telecom companies, healthcare & aviation/avionics/aerospace organisations are a tempting target for IoT cyberattacks since they operate a myriad of IoT devices in their networks and have access to the most sensitive data. READ MORE.

The first step to securing your OT environment

When it comes to cyberattacks targeting OT environments, the disruption can lead to devastating consequences, affecting the flow of goods and services that are essential to keep modern society going on. Sometimes, non-compliance with regulations can be fatal in this respect. Find out how a security assessment can help you improve your business security posture. READ MORE

THANK YOU

for your time!

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

in company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu