ECHO
EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

Newsletter

TOWARDS THE ECHO DEMO CASES

Written by Matteo Merialdo
Project Implementation Coordinator, RHEA Group

The ECHO team travelled for 30 months to develop technologies, frameworks and relations strong enough to dare the final endeavour, complex Demonstration Cases which aim is to validate multiple technologies and teams together in real-life usage situations.
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.

ECHO Cyber Ranges to support Demonstration Cases

To support E-FCR demonstration cases, a set of cyber ranges will be available, each with several training, testing and R&D scenarios. Read more about ECHO Demonstration Cases and sector-specific cyber ranges here!

READ MORE

IMPACT PRODUCT

WP4 INTER-SECTOR TECHNOLOGY ROADMAPS

D4.2 Inter-sector technical cybersecurity challenges report

Lead Author: Notis Mengidis (CERTH)

One of the main objectives of ECHO project is the development of cybersecurity technology roadmaps as a result of analysis related to current and emerging cybersecurity challenges and associated technologies. These roadmaps will create the foundations for new industrial capabilities, and assist towards the development of innovative technologies that will aim to address these cybersecurity challenges. To this end, early prototypes research and development which will target specific, high-priority opportunities identified in these roadmaps will be performed.

To achieve these objectives, the roadmaps will be developed in accordance to the challenges identified in the analysis performed in the work: “Detailed analysis of transversal technical cybersecurity challenges” and its associated deliverables. This document is the first version of one of the two deliverables that discuss and analyse a range of inter-sector technical cybersecurity challenges, i.e., technical cybersecurity challenges that are sector-related, but span across more than one sectors.

The analysis resulted in the identification of a total of 83 technical cybersecurity challenges: 57 transversal challenges (reviewed in D4.1) and 26 inter-sector challenges (reviewed in this deliverable). Each of the identified challenges is broadly presented across three dimensions: (i) the detailed description of each specific challenge, (ii) the mitigation techniques currently existing either as a commercially available product or as the state-of-the-art on a research level, and (iii) the opportunities that can be derived based on the availability of mitigation techniques and solutions. Based on these three pillars and also on the number of research and technological domains that each challenge covers, we performed an initial qualitative prioritisation in order to highlight the challenges with higher criticality that would need to be analysed by T4.2 “Inter-sector technology roadmap development”.

The next steps include conducting dedicated workshops to receive feedback from cybersecurity experts, as well as collect input through questionnaires. For this purpose, a list of recipients has already been collected and the plan is to use it in the next version of the deliverable. Also, the report collection process is ongoing in order to keep up to date with all emerging cybersecurity challenges. Finally, the ECHO Multi-sector Assessment Framework will be used in order to prioritise the challenges in a quantitative manner.

ECHO NEWS

WP4.2 AI CISO Ideathon

On April 13th, ECHO hosted an ideathon on how to support the Chief Information Security Officer with AI! 28 participants from different countries, took part in it and many great ideas have been shared!

READ MORE

Welcome the new participants at ECHO

By joining ECHO, new project participants help us improve the quality of our inputs, identify new and exciting opportunities, improve the products we create and help Europe in its mission to strengthen its cybersecurity posture.

READ MORE

CYBER INDUSTRY NEWS

Irish cyber-attack: Hackers bail out Irish health service for free

The Irish Department of Health was attacked in May, 2021, and the Conti ransomware group is threatening to publish data.

Source: https://www.bbc.com/news/world-europe-57197688

What the cyber-attack on the US oil and gas pipeline means and how to increase security?

The recent cyber-attack on the US major oil and gas pipeline could become one of the most expensive attacks to an economy.

80% of senior cybersecurity leaders see ransomware as a dangerous growing threat that is threatening our public safety.

Here are six principles to improve the cybersecurity of critical infrastructure.

Source:

https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/

Meet ECHO's expert - ANA MARIA MATEJIC

Security Services Manager, RHEA Group
Brussels

How would you introduce yourself and your role within the ECHO Project?
I have recently joined ECHO through Rhea's active membership. I am managing the cybersecurity services team within Rhea so through this position i am following closely and contributing to ECHO's initiatives.

Why do you think cybersecurity is important nowadays?
I believe cybersecurity has gained importance in time. Because it became a topic on the C-level agenda only recently it actually created a "gap" along the years between having a (good) cyber-response strategy and hackers' sophistication. Today, there is no business that can survive and develop on the long-term without a clear strategy for cyber. That is because any cyber-weakness can be exploited to their loss by various parties.

How are you and your organization contributing to the project?
Rhea is an active supportive member of ECHO and drives several initiatives within ECHO.

What surprised you the most about working in ECHO?
I was pleasantly surprised to meet very knowledgeable professionals that are willing to go the "extra-mile" (in this case to allocate extra time and effort) in order to move the initiatives ECHO drives into the business world thus contributing to the steps towards improving cyber-defense.

What was the biggest challenge you were facing?
Time :)

In your opinion, what will be the biggest lesson of the Covid-19 epidemic in terms of cyber security?
An important lesson that Covid-19 emphasized faster and more obvious: you can never foresee all scenarios that can affect the "business as usual" and therefore the cyber-strategy. This means that "be ready for the worst case scenario" is a good premise to start from when building cyber-strategies.

EVENTS

The CS4CA (Cyber Security For Critical Assets) Summit virtual cybersecurity conference was held on May 6th with more than 600 participants. ECHO supported the event and was represented by Matteo Merialdo,

Upcoming

DIGILIENCE 2021

Third International Scientific Conference "Digital Transformation, Cyber Security and Resilience"

29 September -1 October, 2021
Veliko Tarnovo, Bulgaria

READ MORE

2021 IEEE International Conference

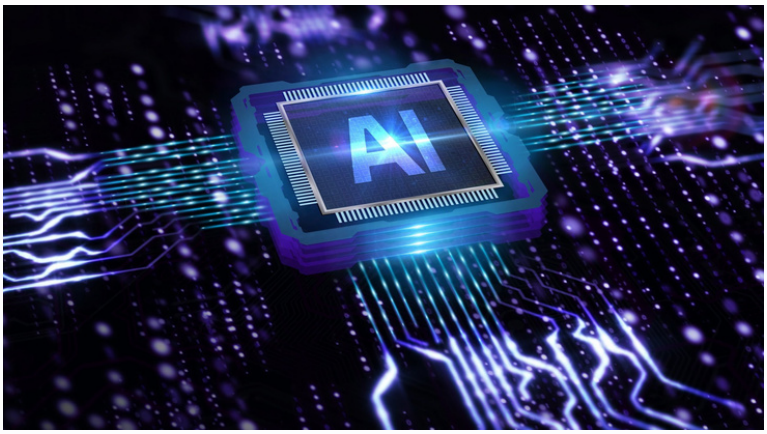
on Cyber Security and Resilience

26-28 July, 2021
Virtual Conference

READ MORE

THE LIGHTER SIDE

Quiz: How much do you know about artificial intelligence?



Artificial Intelligence (AI) is a super in-demand area right now.
But how much do you actually know about it? Put your skills to the test with this fun quiz!
Source:
https://careerswithstem.com.au/artificial-intelligence-trivia/
.

VISIT OUR WEBSITE:
https://www.echonetwork.eu