ECHO Overview

Matteo Merialdo
Project Implementation Coordinator

RHEA Group

31 January 2020

Funded by the European Union’s Horizon 2020
Research and Innovation Programme, under Grant Agreement no 830943

The EU cybersecurity challenge

from *“fragmented in diversity”* to *“united in diversity”*

Cybersecurity Gaps for EU

ECHO consortium identified gaps in current cybersecurity technologies and operations in EU:

1. Lack of effective means to assess multi-sector technology requirements across security disciplines
2. Lack of effective means to assess dependencies between different industrial sectors
3. Lack of realistic simulation environments for technology research and development, or efficient security test and certification
4. Lack of an up-to-date cyberskills framework as a foundation for cybersecurity education and training
5. Lack of effective means to share knowledge and situational awareness in a secure way with trusted partners

These gaps **are particularly relevant for EU**

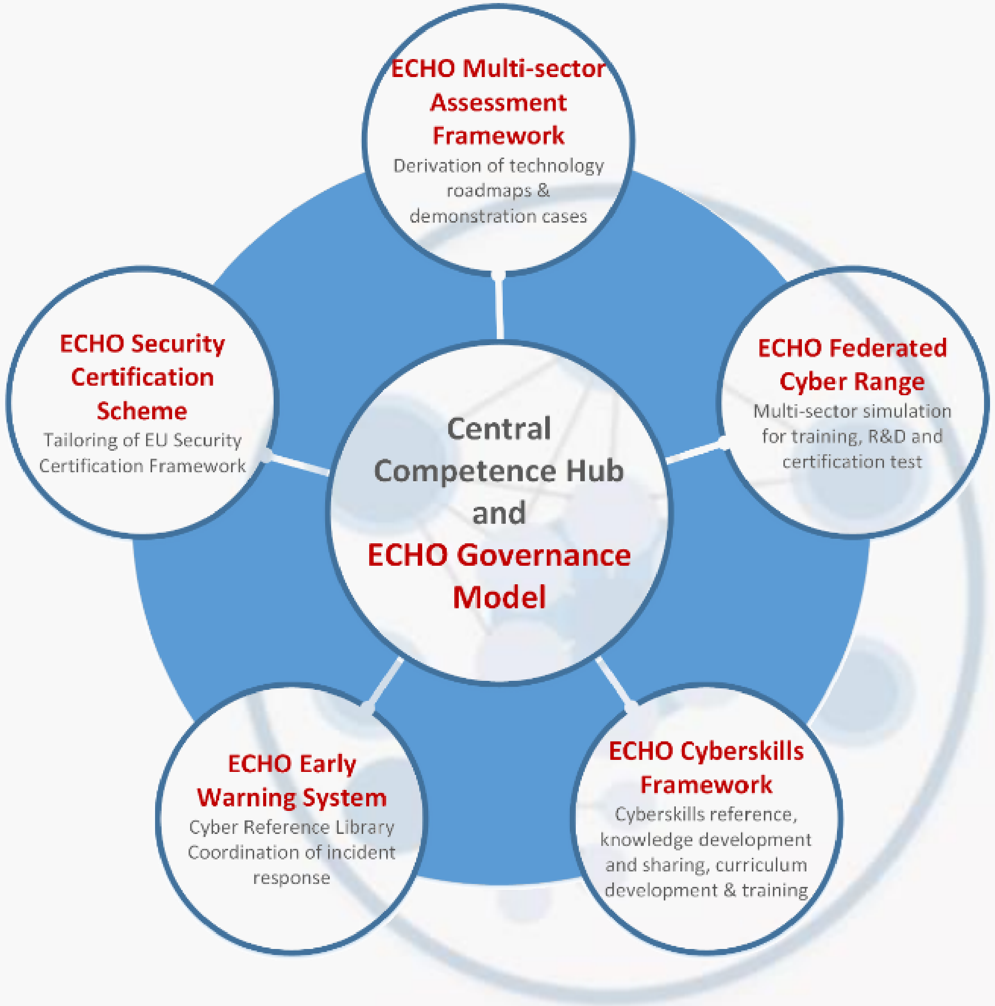
Partners

Key summary

- Project Coordinator: **Royal Military Academy of Belgium (Wim Mees)**
- Project Management: **RHEA System S.A. (Matteo Merialdo)**
- 16 Millions budget (1.7 for RHEA)
- 4 years (started Feb 2019)
- 30 partners
- 15 new partner engagements
- 13 existing competence centres
- 16 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

European network of Cybersecurity centres and competence Hub for innovation and Operations

- Main concepts:
  - ECHO Governance Model:
    - Management of direction and engagement of partners (current and future)
  - ECHO Multi-sector assessment framework:
    - Transverse and inter-sector needs assessment and technology R&D roadmaps
  - ECHO Cyberskills Framework and training curriculum
    - Cyberskills reference model and associated curriculum
  - ECHO Security Certification Scheme
    - Development of sector specific security certification needs within EU Cybersecurity Certification Framework
  - ECHO Federated Cyber Range
    - Advanced cyber simulation environment supporting training, R&D and certification
  - ECHO Early Warning System
    - Secured collaborative information sharing of cyber-relevant information



Central Competence Hub and ECHO Governance Model

ECHO Multi-sector Assessment Framework
Derivation of technology roadmaps & demonstration cases

ECHO Federated Cyber Range
Multi-sector simulation for training, R&D and certification test

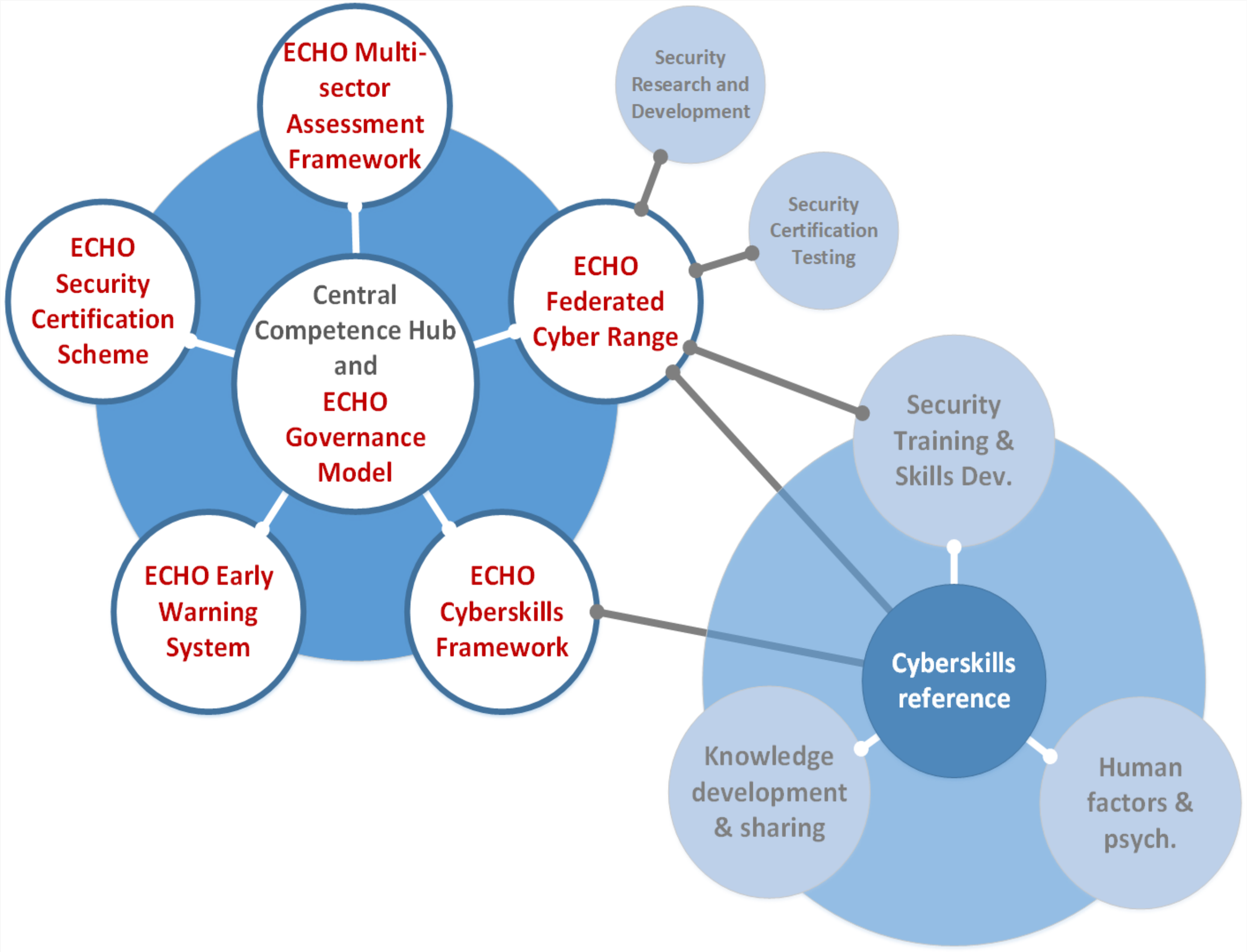
ECHO Cyberskills Framework
Cyberskills reference, knowledge development and sharing, curriculum development & training

ECHO Early Warning System
Cyber Reference Library Coordination of incident response

ECHO Security Certification Scheme
Tailoring of EU Security Certification Framework

ECHO Cyberskills and curricula

- ECHO Cyberskills framework
  - Mechanism to improve the **human capacity** of cybersecurity across Europe
- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome based curricula**
- **Hands-on skills development** opportunities through realistic simulation (ECHO Federated Cyber Range)
- Lessons learned feed **knowledge sharing** (ECHO Early Warning System)

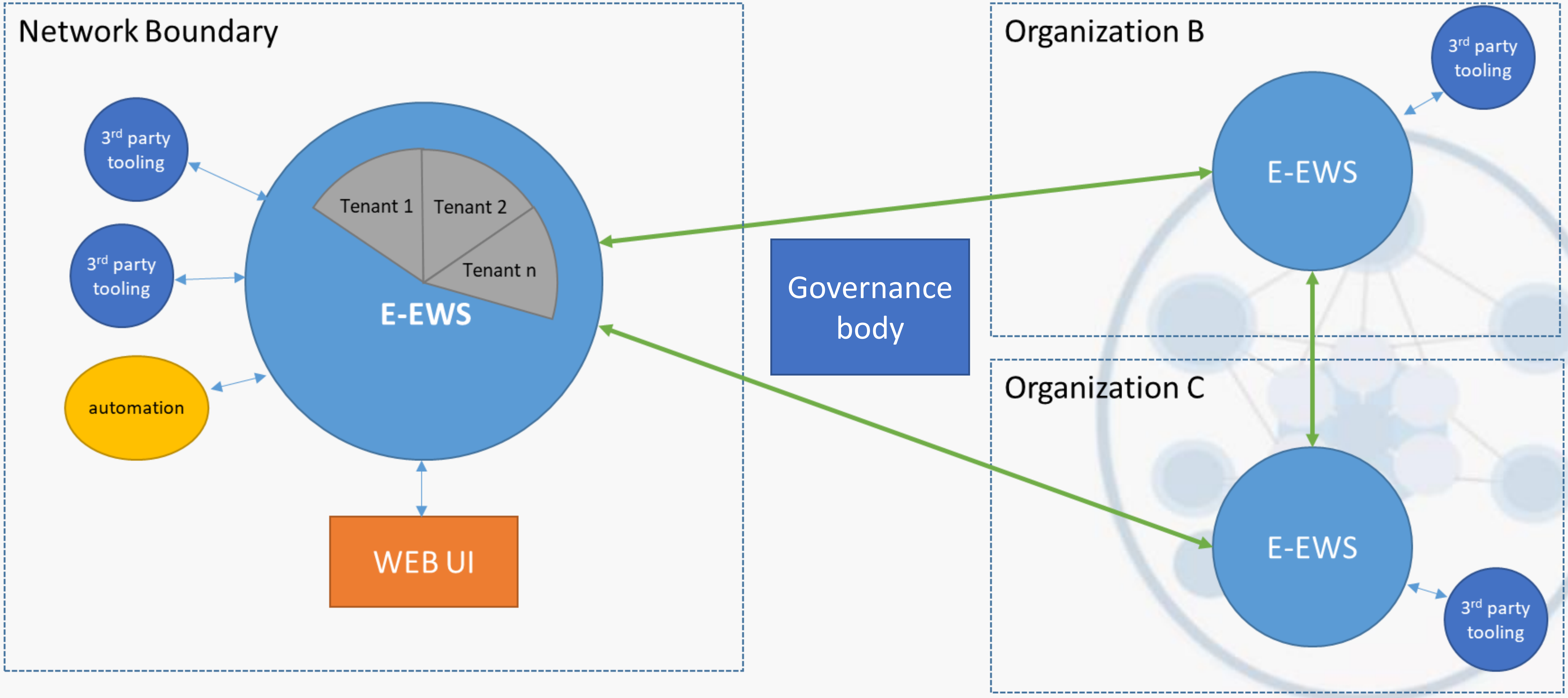


ECHO Multi-sector Assessment Framework
ECHO Security Certification Scheme
Central Competence Hub and ECHO Governance Model
ECHO Federated Cyber Range
ECHO Early Warning System
ECHO Cyberskills Framework
Security Research and Development
Security Certification Testing
Security Training & Skills Dev.
Cyberskills reference
Knowledge development & sharing
Human factors & psych.

ECHO Technology roadmap: E-EWS

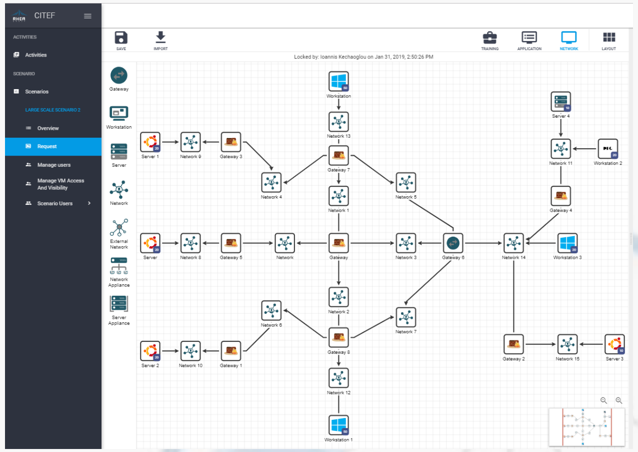
- ECHO Early Warning System
  - **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
  - Secure information sharing **between organizations**; across organizational boundaries and national borders
  - Coordination of **incident management workflows**
  - Retain **independent management and control of cyber-sensitive** information
  - Account for **sector specific needs** and protection of **personal information protection** (GDPR compliant)
  - Includes sharing of **reference library** information and **incident management** coordination
  - Target **Technology Readiness Level: 9**
  - Governance and Sharing Models in development
  - **Potentially, it could serve all the network of centres of competeces!**

E-EWS concepts - distribution

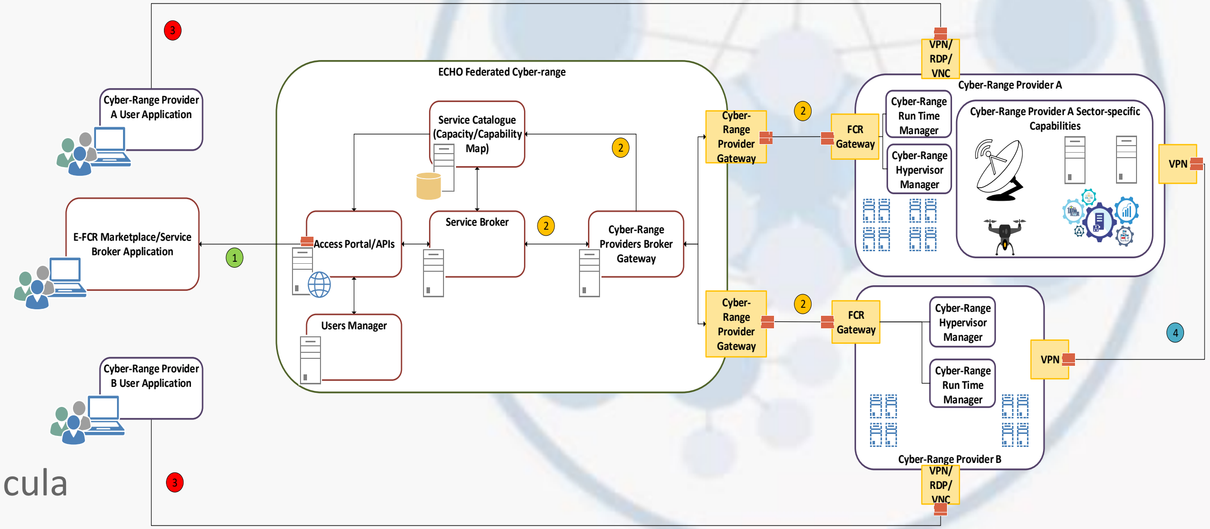


Technology roadmap: E-FCR

- ECHO Federated Cyber Range (FCR)
    - Interconnect existing and new cyber range capabilities through a convenient portal
    - Portal operates as a **broker** among cyber ranges
    - A **marketplace** enable content providers to sell cyber range contents to a wider market
    - Enables access to emulations of **sector specific and unique technologies**
    - Target **Technology Readiness Level: 8**
    - Governance Model in development
- Cyber Range is a multipurpose **virtualization environment** supporting **“security-by-design”** needs
    - Safe environment for **hands-on cyberskills** development
    - Realistic simulation for **improved system assurance** in development
    - Comprehensive means for **security test and certification** evaluation
- To be used as virtual environment for:
    - Development and demonstration of **technology roadmaps**
    - Delivery of specific instances of the **cyberskills training** curricula

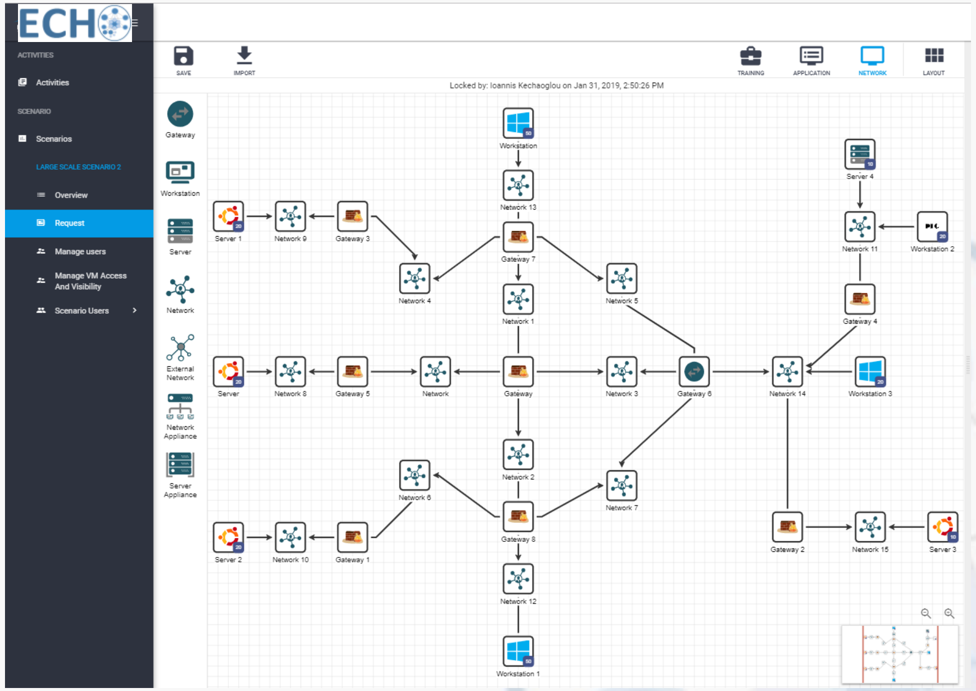


Locked by: Ioannis Kechaoglou on Jan 31, 2019, 2:50:26 PM


ECHO Federated Cyber-range
Cyber-Range Provider A User Application
E-FCR Marketplace/Service Broker Application
Cyber-Range Provider B User Application
Service Catalogue (Capacity/Capability Map)
Access Portal/APIs
Service Broker
Cyber-Range Providers Broker Gateway
Users Manager
Cyber-Range Provider Gateway
Cyber-Range Provider Gateway
FCR Gateway
FCR Gateway
Cyber-Range Provider A
Cyber-Range Run Time Manager
Cyber-Range Hypervisor Manager
Cyber-Range Provider A Sector-specific Capabilities
Cyber-Range Hypervisor Manager
Cyber-Range Run Time Manager
Cyber-Range Provider B
VPN/ RDP/ VNC
VPN/ RDP/ VNC
VPN
VPN
1
2
2
2
2
2
3
3
4

E-FCR concept

- Customers will have access to
  - **Service Designer** -> concept already in progress (develop new scenarios leveraging on single or multiple ranges)
  - **Marketplace** (content providers can upload contents/scenarios for a wider market)



Locked by: Ioannis Kechaoglou on Jan 31, 2019, 2:50:26 PM

Critical Sectors
EC-JRC taxonomy

Audiovisual and media	Defence	Digital infrastructure	Energy	Financial
Government and public authorities	Health	Maritime	Nuclear	Public safety
Tourism	Transportation	Smart ecosystems	Space	Supply chain

Outcomes

- ECHO targets practical use of outcomes to offer technologies and services having increased cyber-resilience by sector and among inter-dependent partners
  - Use of E-FCR for experimental simulation of cyber-attack scenarios, pre-production testing, product evaluations, training
  - Combined use of E-FCR and E-Cybersecurity Certification Scheme (E-CCS) for certified qualification testing of potential technologies required to meet customer specification
  - Use of E-CCS as benchmark of cybersecurity certification to be obtained as a market differentiator
  - Use of E-EWS to share early warning of cybersecurity related issues (e.g., vulnerabilities, malware, etc..), potentially at EU level
  - Promotion of improved cyberskills through leveraging diverse education and training options made available by the E-Cybersecurity Skills Framework, particularly as it relates to security-by-design best practices
- Although not clear what will be the future of the 4 Pilot projects, it is expected the most relevant outcomes will be merged to create the **future EU cybersecurity competence centres network**

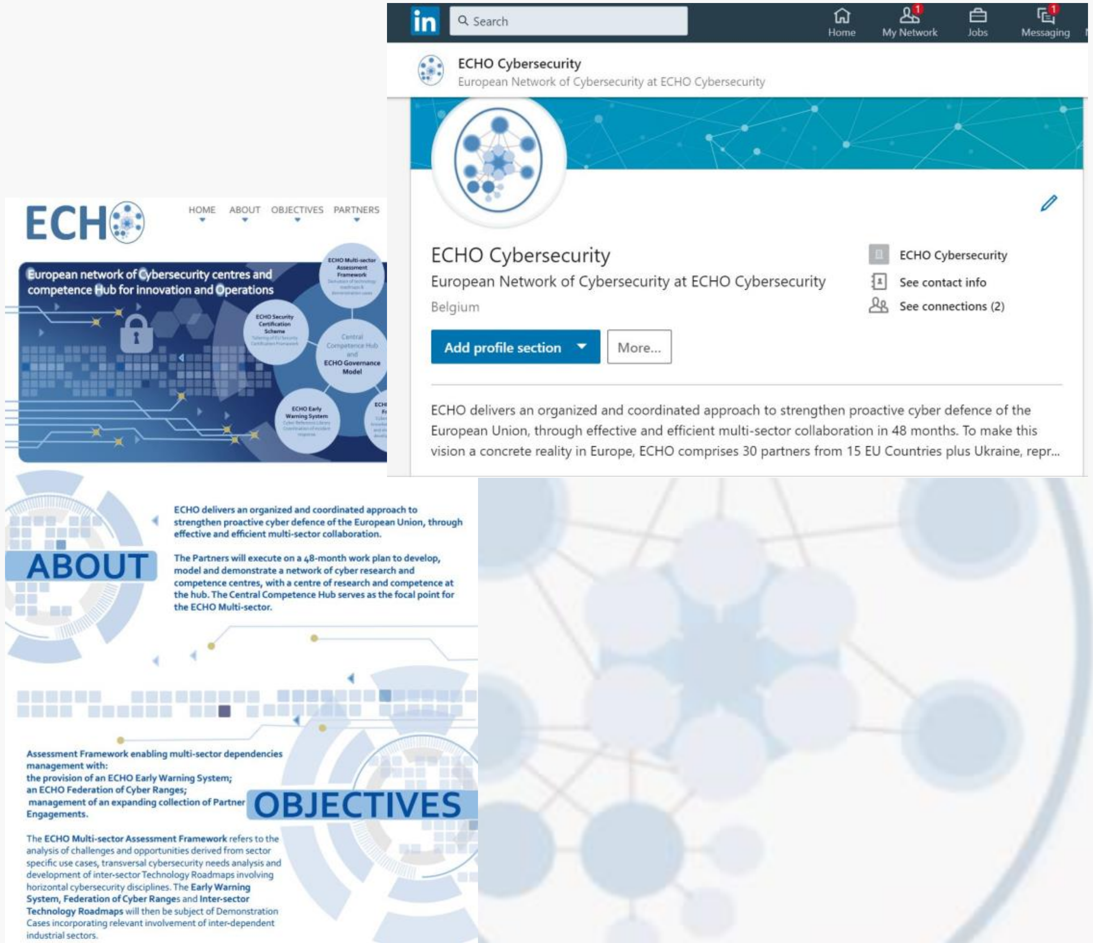
A European Competence Network of Cybersecurity Centres of Excellence

The first 2 years

- ECHO schedule for the first 2 years is quite tight
  - First technical **review successfully passed**
  - **E-EWS** and **E-FCR TRL 6** prototypes to be developed for **mid 2021 – ongoing**
    - **First version of E-EWS** already **active**! Searching for tenants!
  - Governance Models (and related transition from the current model) for the network will be ready for **mid 2021**
  - Preliminary models for **sustainability** of the network, the E-EWS and the E-FCR
  - Goal is to immediately deploy E-EWS (**already operational**) and E-FCR and start using them within the ECHO **enlarged partners** (beneficiaries + stakeholders) – **new tenants** for the E-EWS and **new cyber ranges** for the E-FCR (many with **RHEA CITEF Technology**!)
  - Training packages will be ready for **mid 2021** and in delivery, leveraging on E-EWS and E-FCR prototypes
  - **Healthcare**, **Maritime**, **Energy** sectors demonstrations in development (including dependencies with space and water sectors, likely)
  - Other 2 technology innovations (at least) from the technology roadmaps will be in development

Social Media

- For information: info@echonetwork.eu
- ECHO website: www.echonetwork.eu
- Twitter: **@ECHOcybersec**
- Linkedin: ECHO cybersecurity


HOME
ABOUT
OBJECTIVES
PARTNERS
European network of Cybersecurity centres and competence Hub for innovation and Operations
ECHO Multi-sector Assessment Framework
ECHO Security Certification Scheme
Central Competence Hub and ECHO Governance Model
ECHO Early Warning System
ABOUT
OBJECTIVES
Search
Home
My Network
Jobs
Messaging
Add profile section
More...
See contact info
See connections (2)

ECHO delivers an organized and coordinated approach to strengthen proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration.

The Partners will execute on a 48-month work plan to develop, model and demonstrate a network of cyber research and competence centres, with a centre of research and competence at the hub. The Central Competence Hub serves as the focal point for the ECHO Multi-sector.

Assessment Framework enabling multi-sector dependencies management with:
the provision of an ECHO Early Warning System;
an ECHO Federation of Cyber Ranges;
management of an expanding collection of Partner Engagements.

The **ECHO Multi-sector Assessment Framework** refers to the analysis of challenges and opportunities derived from sector specific use cases, transversal cybersecurity needs analysis and development of inter-sector Technology Roadmaps involving horizontal cybersecurity disciplines. The **Early Warning System, Federation of Cyber Ranges** and **Inter-sector Technology Roadmaps** will then be subject of Demonstration Cases incorporating relevant involvement of inter-dependent industrial sectors.

ECHO Cybersecurity
European Network of Cybersecurity at ECHO Cybersecurity

ECHO Cybersecurity
European Network of Cybersecurity at ECHO Cybersecurity
Belgium

ECHO Cybersecurity

ECHO delivers an organized and coordinated approach to strengthen proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration in 48 months. To make this vision a concrete reality in Europe, ECHO comprises 30 partners from 15 EU Countries plus Ukraine, repr...

- Youtube: https://www.youtube.com/channel/UCDQBXrQhoLJ2lnf38x1X6Uw