Strengthening EU cyber defence through effective and efficient multi-sector collaboration

Pilots for the European Cybersecurity Competence Networks: how can your SME benefit?

Matteo Merialdo (Project Implementation Coordinator)

RHEA Group

Cyberwatching.eu, 02 April 2019

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

Current challenges

ECHO consortium identified following challenges 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

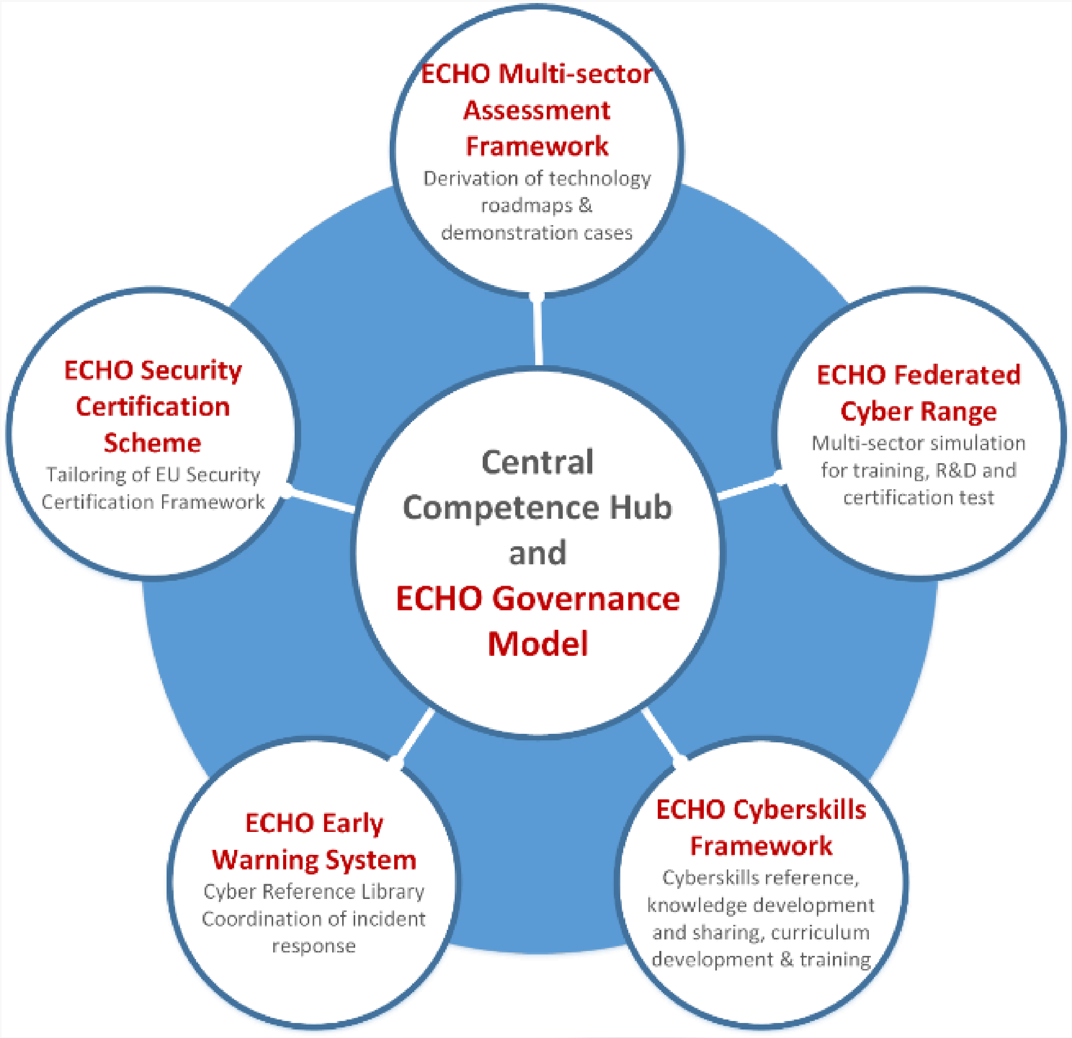
These challenges **can be particularly relevant for EU SMEs**

Project main objectives

- Network of cyber research and competence centres, with a central competence hub
  - Demonstrate a network of cyber research and competence centres, with a central competence hub, having a mandate for increasing participation through a new partner engagements model, including collaboration with other networks funded under the same call
  - Address all the aforementioned weaknesses, developing an adaptive model for information sharing and collaboration among the network of cybersecurity centres, supported by an early warning system and a framework for improved cyberskills development and technology roadmap delivery, in a multiple-sector context

Innovations and Impact

- Main Innovations
  - **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 from ENISA
  - **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


ECHO Multi-sector Assessment Framework
Derivation of technology roadmaps & demonstration cases
ECHO Security Certification Scheme
Tailoring of EU Security Certification Framework
Central Competence Hub and ECHO Governance Model
ECHO Federated Cyber Range
Multi-sector simulation for training, R&D and certification test
ECHO Early Warning System
Cyber Reference Library Coordination of incident response
ECHO Cyberskills Framework
Cyberskills reference, knowledge development and sharing, curriculum development & training

Innovations and Impact

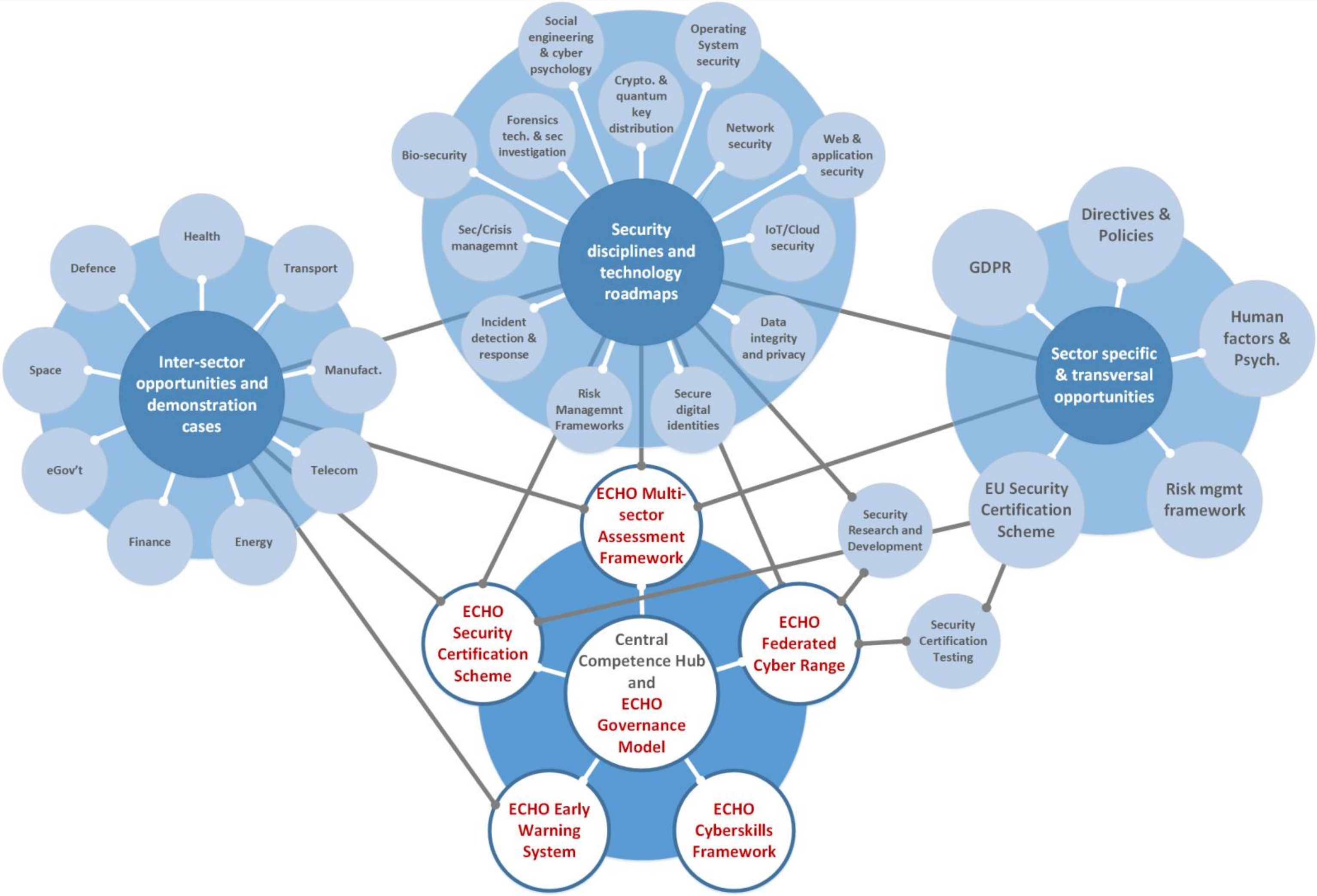
- ECHO Governance model
  - Manages **ongoing and new partner** engagements
  - 30 existing partners
  - 6 Academic/Institutional, 7 Industrial cyber centres connected from the start
  - 5 SMEs
- Engagements with new partners (including SMEs)
  - **Minimum 15 new engagements**
  - **Access to** ECHO Early Warning System
  - **Access to** ECHO Federation of Cyber Ranges
  - **Access to** Cyberskills framework and trainings
  - **Participation in** Technology Roadmaps (R&D)
- **Sustainable model** for long term operations

Key summary:

- **30 existing partners**
- **15 new partner engagements**
- **13 Existing centres**
- **16 nations**
- **9 industrial sectors**
- **13 security disciplines**
- **5 demonstration cases**
- **6 technology roadmaps**
- **3 multi-sector scenarios**

Innovations and Impact

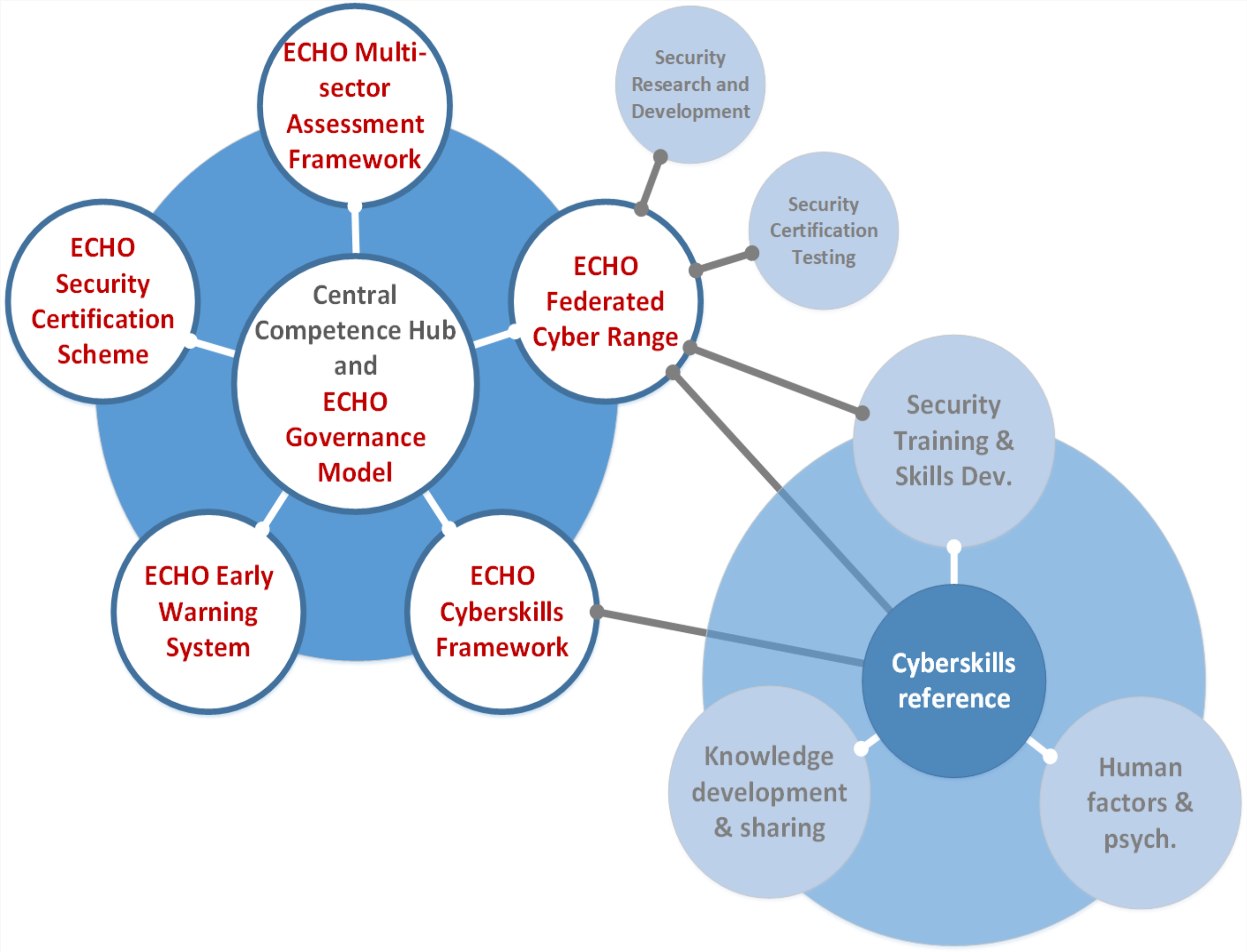
- ECHO Multi-sector assessment framework
  - Mechanism to define and refine **technology roadmaps** and **demonstration cases**
- Risk based method to analyse multi-sector security needs including
  - **Inter-sector opportunities** (potential solutions) to security challenges further analysed as **demonstration cases**
  - **Comprehensive analysis** of potential contributions to **technology roadmaps** across **security disciplines** as means to improve security posture
  - Analysis of **sector specific needs** and **transversal opportunities** to identify potential for improvement



Social engineering & cyber psychology
Operating System security
Crypto. & quantum key distribution
Forensics tech. & sec investigation
Network security
Bio-security
Web & application security
Sec/Crisis managemnt
Security disciplines and technology roadmaps
IoT/Cloud security
Incident detection & response
Data integrity and privacy
Risk Managemnt Frameworks
Secure digital identities
Health
Defence
Transport
Space
Inter-sector opportunities and demonstration cases
Manufact.
eGov't
Telecom
Finance
Energy
Directives & Policies
GDPR
Human factors & Psych.
Sector specific & transversal opportunities
EU Security Certification Scheme
Risk mgmt framework
Security Research and Development
ECHO Multi-sector Assessment Framework
ECHO Security Certification Scheme
Central Competence Hub and ECHO Governance Model
ECHO Federated Cyber Range
Security Certification Testing
ECHO Early Warning System
ECHO Cyberskills Framework

Innovations and Impact

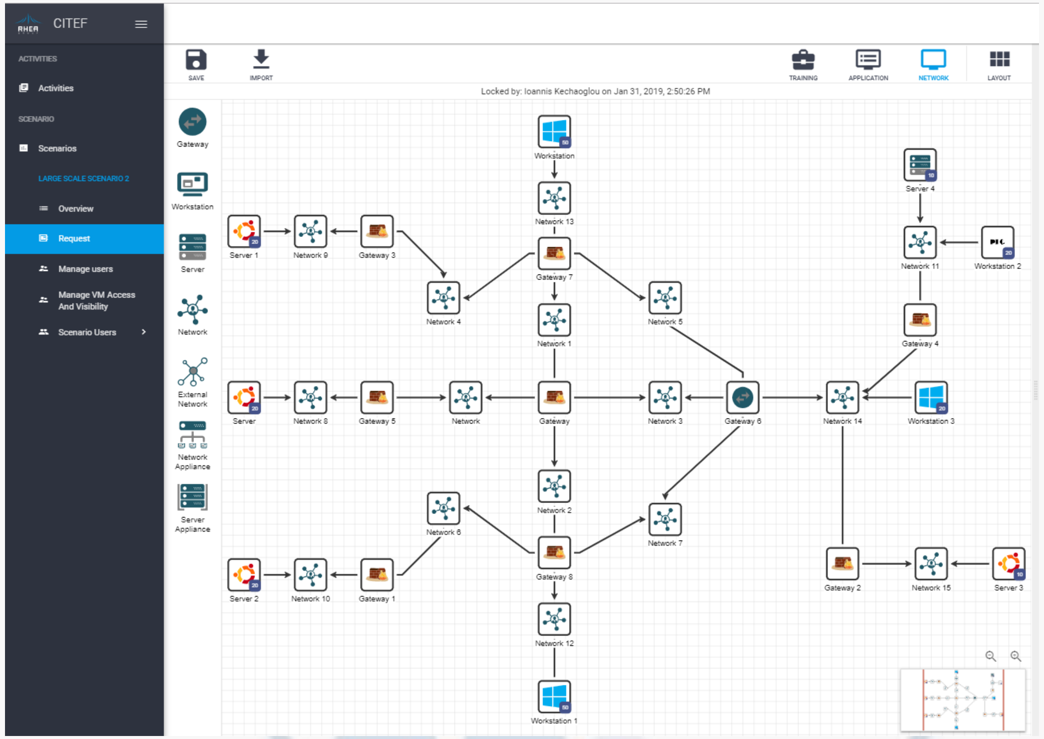
- ECHO Cyberskills framework
  - Mechanism to improve the **human capacity** of cybersecurity across Europe
- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome 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
Security Research and Development
ECHO Security Certification Scheme
Central Competence Hub and ECHO Governance Model
ECHO Federated Cyber Range
Security Certification Testing
Security Training & Skills Dev.
ECHO Early Warning System
ECHO Cyberskills Framework
Cyberskills reference
Knowledge development & sharing
Human factors & psych.

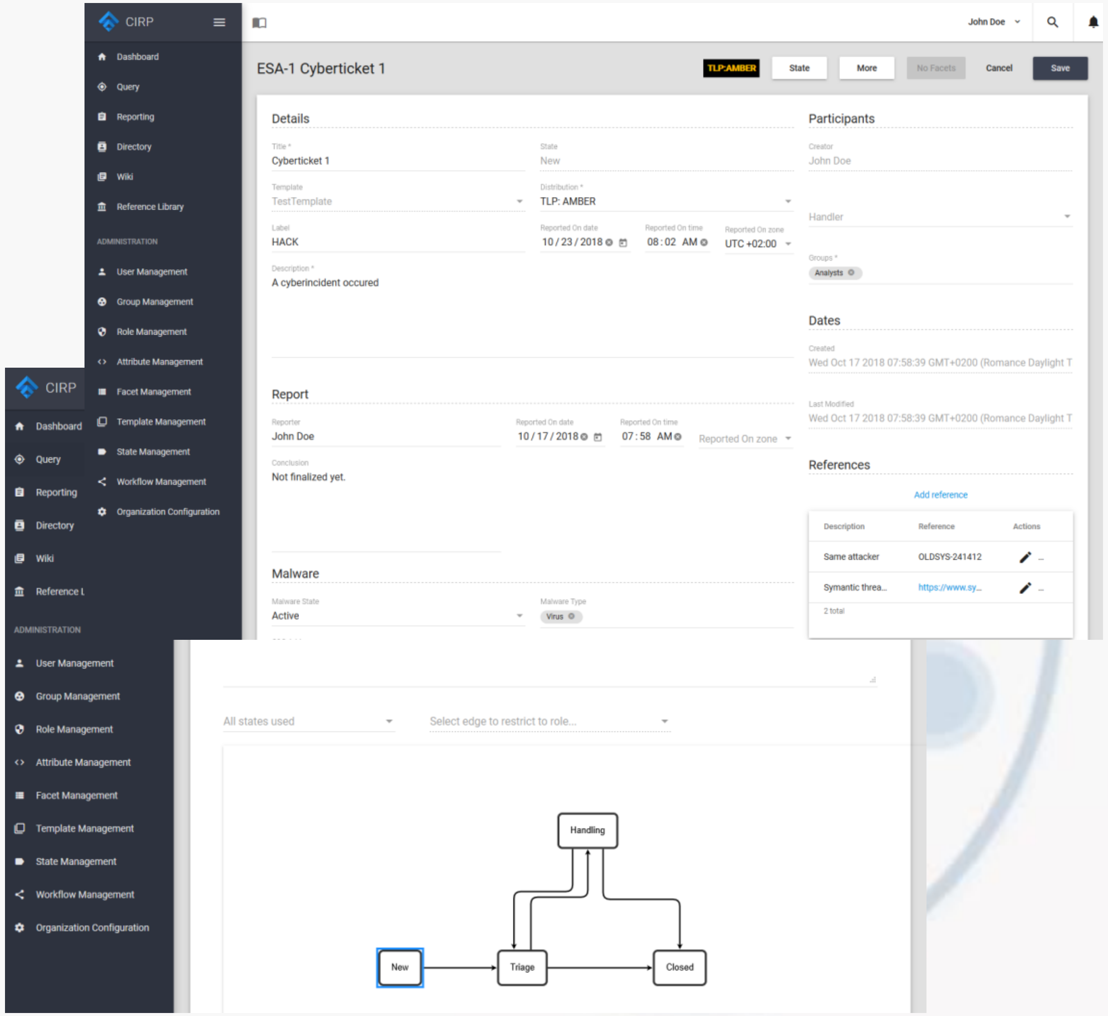
Innovations and Impact

- ECHO Federated Cyber Range
  - Interconnect existing (X 7) and new cyber range capabilities through a portal
  - Portal operates as a **broker** among cyber ranges
  - Enables access to emulations of **sector specific and unique technologies**
- 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 Kechagoglou on Jan 31, 2019, 2:50:26 PM

Innovations and Impact

- 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



ESA-1 Cyberticket 1

Details

Title *
Cyberticket 1

State
New

Template
TestTemplate

Distribution *
TLP: AMBER

Label
HACK

Reported On date
10 / 23 / 2018

Reported On time
08 : 02 AM

Reported On zone
UTC +02:00

Description *
A cyberincident occured

Report

Reporter
John Doe

Reported On date
10 / 17 / 2018

Reported On time
07 : 58 AM

Reported On zone

Conclusion
Not finalized yet.

Malware

Malware State
Active

Malware Type
Virus

Participants

Creator
John Doe

Handler

Groups *
Analysts

Dates

Created
Wed Oct 17 2018 07:58:39 GMT+0200 (Romance Daylight T

Last Modified
Wed Oct 17 2018 07:58:39 GMT+0200 (Romance Daylight T

References

Add reference

Description	Reference	Actions
Same attacker	OLDSYS-241412	...
Symantic threa...	https://www.sy...	...

2 total

Innovations and Impact

- ECHO Cybersecurity Certification Scheme
  - Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
  - Provides **sector oriented** cybersecurity certification schemes
    - Support sector specific and inter-sector security requirements
  - Supports **delivery and acceptance of technologies** resulting from technology roadmaps
    - **Improved security assurance** through use of **certified products**
  - Supports development of **Digital Single Market**
    - Limits duplication and fragmentation of the cybersecurity market
    - **Common** cybersecurity **evaluation methods, acceptance** throughout Europe
    - Applicability across **Information Technologies** (IT/ICT) and **Operations Technologies** (OT/SCADA)

Demonstration cases for validation

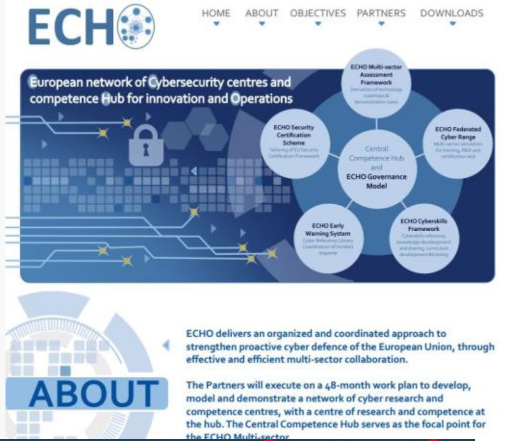
- Sector scenarios
  - Scenarios are subject to the results of the sector and inter-sector analysis to be conducted using the E-MSAF
  - Focus on inter-sector dependencies and sector-specific requirements
  - Actually identified
    - Health
    - Marine
    - Energy
- Technology demonstration cases
- Demonstration cases will be applied to the inter-sector scenarios
  - Overall, ECHO will deliver at least five (5) Demonstration Cases including
    - E-EWS reference library exchange
    - E-EWS cyber incident coordination and response
    - E-FCR use for training and exercise delivery
    - E-FCR use for technology experimentation, research and development
    - E-FCR use for cybersecurity certification testing
  - ECHO will look for “sponsors” for every demonstration case from user community and industry

Benefits for Industry/SMEs

- 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
  - Combined use of E-FCR and 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..)
  - Promotion of improved cyberskills through leveraging diverse education and training options made available by the E-CSF, particularly as it relates to security-by-design best practices

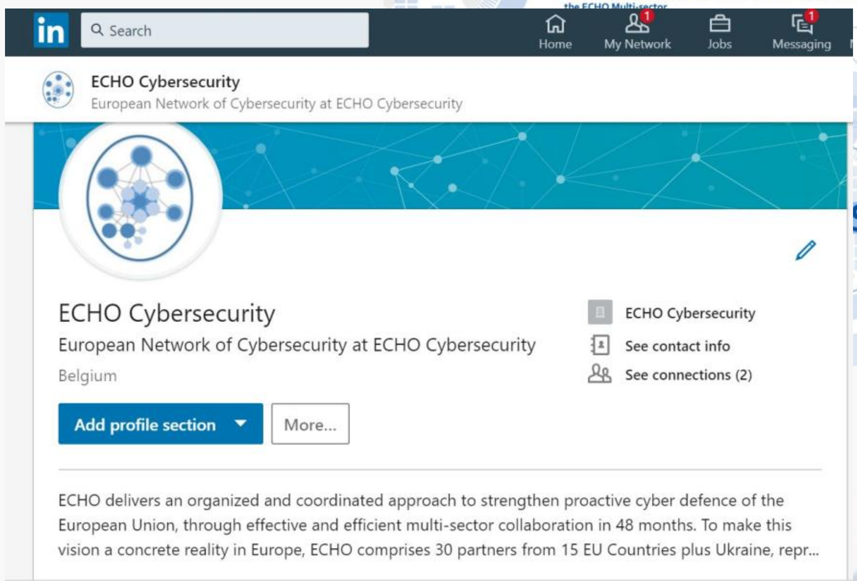
Social Media

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


ECHO
HOME
ABOUT
OBJECTIVES
PARTNERS
DOWNLOADS
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 Federated Cyber Range
ECHO Early Warning System
ECHO Cyberskills Framework
ABOUT

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



ECHO Cybersecurity
European Network of Cybersecurity at ECHO Cybersecurity

ECHO Cybersecurity
European Network of Cybersecurity at ECHO Cybersecurity
Belgium

ECHO Cybersecurity
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 in 48 months. To make this vision a concrete reality in Europe, ECHO comprises 30 partners from 15 EU Countries plus Ukraine, repr...

Thank you!

New partners participation

- Key message about new engagement opportunities:
  - ECHO Targets **minimum 15 new partner engagements** in the life of the project
  - Managed by the **ECHO Multi-sector Innovation and Exploitation Coordinator** (Douglas Wiemer)
  - Managed through the **ECHO Multi-sector Innovation and Exploitation Committee**
- Participation encouraged via:
  - **Project Advisory Committee** (PAC), targets participation by 15 thought leaders
  - **Technology roadmaps** participation and contribution
  - **Multi-sector scenario demonstration cases** participation
  - **ECHO Early Warning System** network participation

Key summary:

- **30 existing partners**
- **15 new partner engagements**
- **13 Existing centres**
- **16 nations**
- **9 industrial sectors**
- **13 security disciplines**
- **5 demonstration cases**
- **6 technology roadmaps**
- **3 multi-sector scenarios**