ENSURESEC

PROJECT OVERVIEW

End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem

Luís Júdice Sousa – INOV
Project Coordination
luis.sousa@inov.pt

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

2nd ECSCI Workshop – 27th of April 2022

Agenda

- Project Overview
  - Main information
  - Consortium
  - The challenge
  - Main objectives
- The ENSURESEC Technical Solution
  - Overall concept
  - Architecture
  - Technical results
  - Use Cases and Scenarios
  - The ENSURESEC training and awareness campaign
- Expected Impact

ENSURESEC

Project Overview

Project Overview – Main information

- **Acronym:** ENSURESEC
- **Project Title:** End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem
- **Grant Agreement No.:** 883242
- **Total budget:** 9,305,413.75€
- **Total grant:** 7,701,520.00€
- **Start date:** 1st June 2020
- **End date:** 31st May 2022
- **Website:** www.ensuresec.eu
- **Social Media:**
  - Twitter – ensuresec_eu
  - LinkedIn – ENSURESEC

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

Project Overview – The ENSURESEC Consortium

INOV inesc

SONAE

G4S Telematix

CaixaBank

Atos

ENGINEERING

MILSPED GROUP

To farmakeio mou.gr

relational THE FINANCIAL SOLUTIONS COMPANY

iTTi

silensec

SEARCH-LAB SECURITY EVALUATION ANALYSIS AND RESEARCH LABORATORY

ITML

IOTA FOUNDATION

L3CE Lithuanian Cybercrime Center of Excellence for Training, Research & Education

cea

Fraunhofer IML

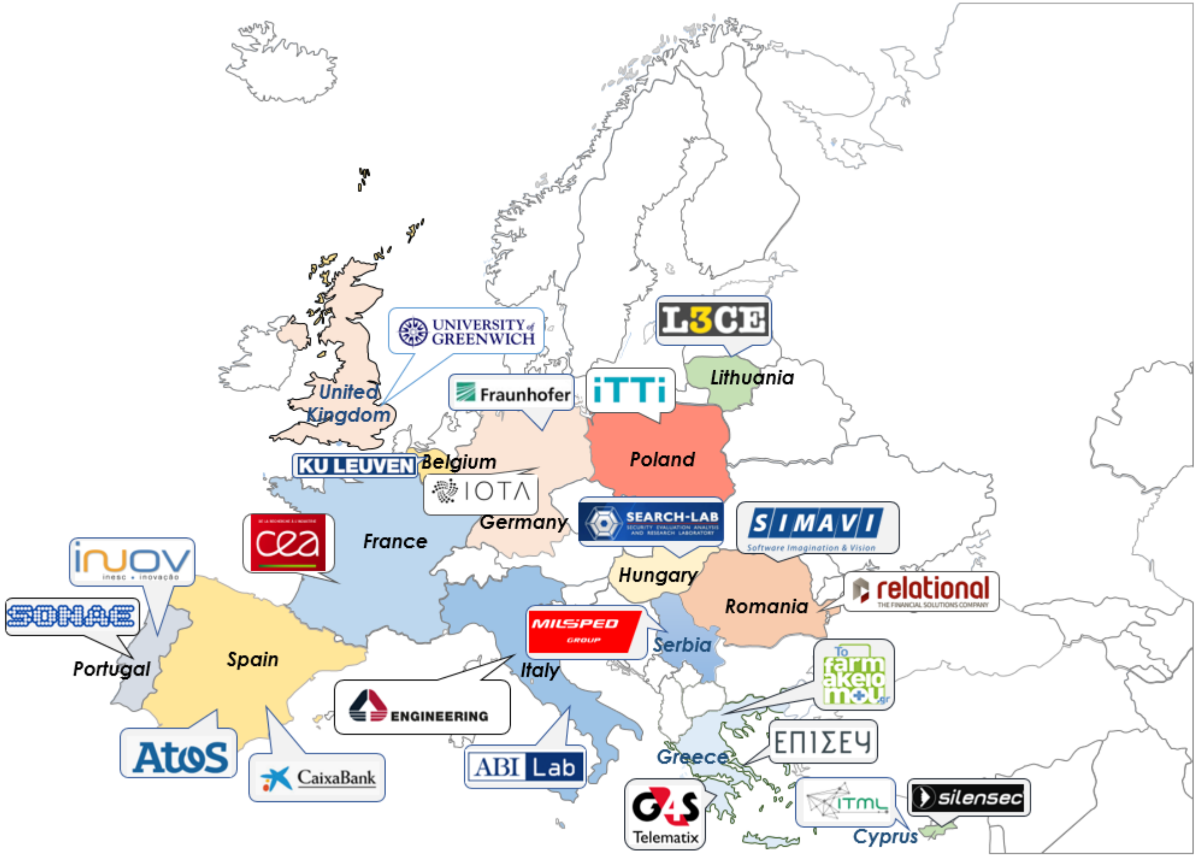
ABI Lab Tecnologia utile

SIMAVI Software Imagination & Vision

ΕΠΙΣΕΥ ICCS

KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

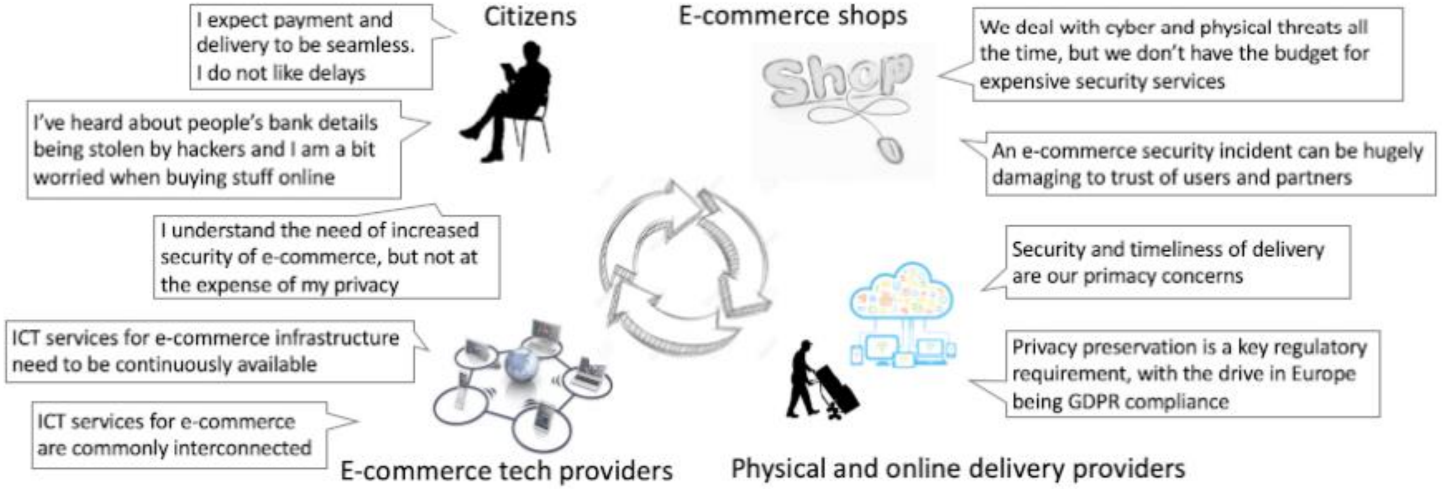
UNIVERSITY of GREENWICH



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

Project Overview – The Challenge

- **E-commerce** is the primary pillar of the **EU Digital Single Market** and as such is **critical for the future and autonomy** of the EU.
- In order to provide **better access to digital goods and services**, there is the need to establish **trust and security** among e-commerce actors. This is particularly **challenging** in e-commerce ecosystems due to the **large attack surface** that needs to be addressed and **the limited visibility of the entities involved in the value chain**.



Citizens
E-commerce shops
Shop
E-commerce tech providers
Physical and online delivery providers

I expect payment and delivery to be seamless. I do not like delays

I've heard about people's bank details being stolen by hackers and I am a bit worried when buying stuff online

I understand the need of increased security of e-commerce, but not at the expense of my privacy

ICT services for e-commerce infrastructure need to be continuously available

ICT services for e-commerce are commonly interconnected

We deal with cyber and physical threats all the time, but we don't have the budget for expensive security services

An e-commerce security incident can be hugely damaging to trust of users and partners

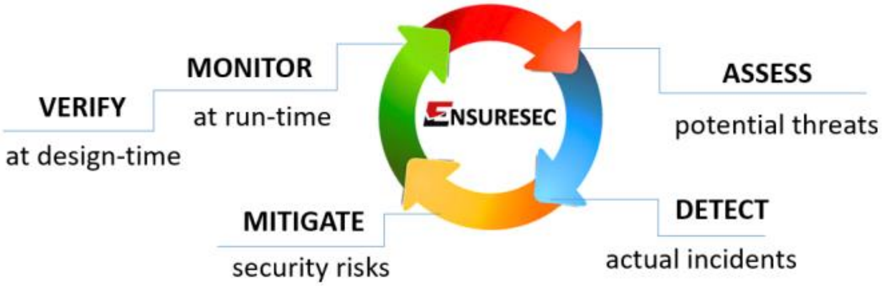
Security and timeliness of delivery are our primacy concerns

Privacy preservation is a key regulatory requirement, with the drive in Europe being GDPR compliance

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

Project Overview – Main Objectives

- ENSURESEC aims at developing a **solution** to provide **e-commerce infrastructures and ecosystems** with through-life **protection** against **cyber, cyber-physical and physical threats**, including **cascading effects**.
- The goal is to develop a **security toolkit** that addresses the **whole span of the e-commerce ecosystem**, with its various forms of payment and delivery (**virtual, online and physical**) through the implementation of **different modules** that ensure that operations are **protected by design**, as well as provide **continuous monitoring, response, recovery and mitigation** measures **at run-time**.



- The project will also create **security awareness** among SMEs and their clients, while **promoting trust in the e-commerce ecosystem**, through the **creation of dedicated content** and the implementation of **tools** for **training and educating** e-commerce stakeholders on cyber security and improve the resilience of the ecosystem.
- Finally, the solution will be **demonstrated and validated in a relevant environment** by the end of the project, by applying the ENSURESEC concepts in **three different use cases**.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.

ENSURESEC

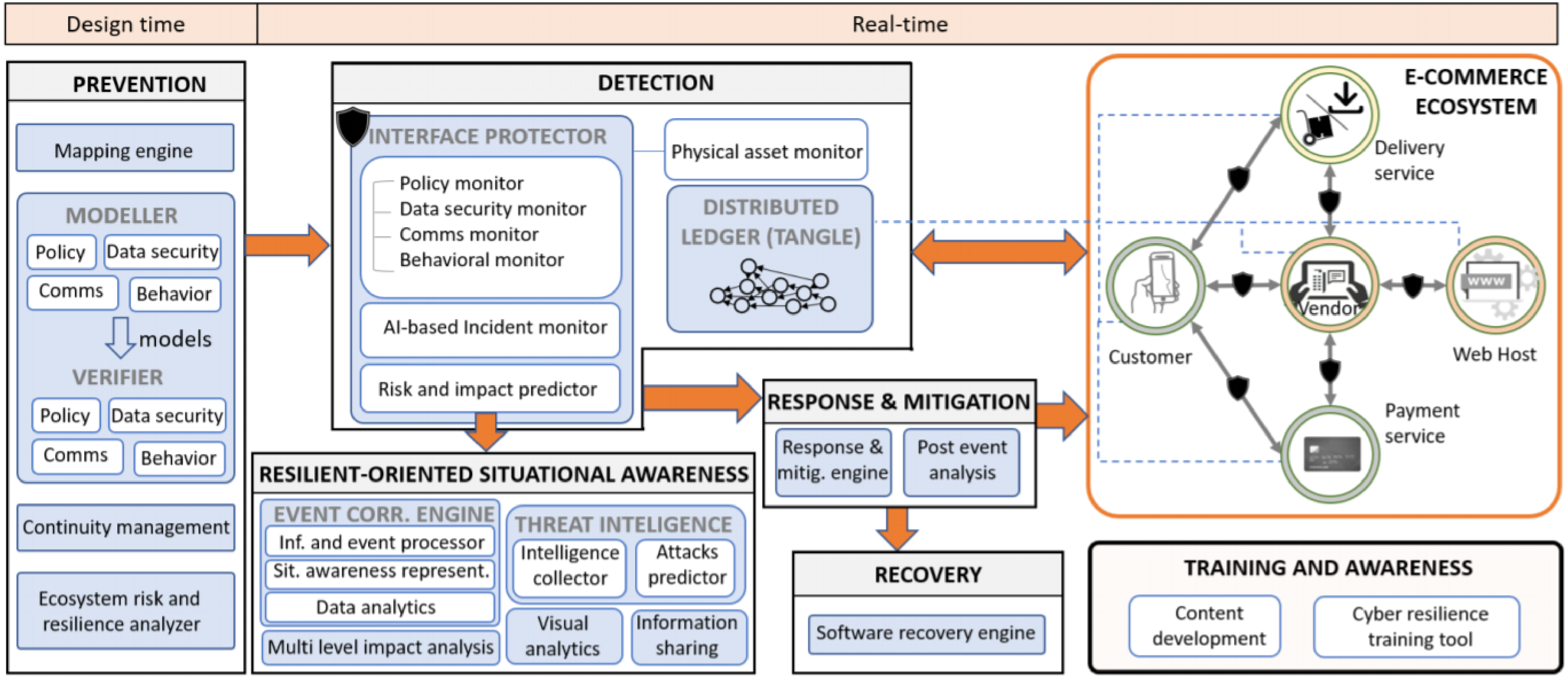
The ENSURESEC Technical Solution

The ENSURESEC Technical Solution – Overall concept

- The ENSURESEC concept is based on an **open source security toolkit** deployed **to protect the interfaces of the e-commerce ecosystem**, through the integration of **six main modules**:
  - **Prevention (by design)** – Assesses and certifies that the design of the system interfaces is secure against certain classes of critical attacks and vulnerabilities;
  - **Detection** – monitors run-time interface operations at the application level and network level for resilience against both known and unknown threats;
  - **Response and mitigation** – Communicates an appropriate response to the affected users and partners and attempts to mitigate the impact;
  - **Recovery** – Recovers the system‘s state by identifying the problem based on a dependency-directed diagnosis;
  - **Continuous situational awareness** – Employs advanced ML techniques to continuously detect any suspicious incident and visualize its impact and interdependencies;
  - **Training and awareness** – Tools based on serious games and creation of dedicated content to make citizen clients of e-commerce SMEs aware of potential security threats and train on how to avoid them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

The ENSURESEC Technical Solution – Architecture



Design time

Real-time

PREVENTION

Mapping engine

MODELLER

Policy

Data security

Comms

Behavior

models

VERIFIER

Policy

Data security

Comms

Behavior

Continuity management

Ecosystem risk and resilience analyzer

DETECTION

INTERFACE PROTECTOR

Policy monitor

Data security monitor

Comms monitor

Behavioral monitor

AI-based Incident monitor

Risk and impact predictor

Physical asset monitor

DISTRIBUTED LEDGER (TANGLE)

RESILIENT-ORIENTED SITUATIONAL AWARENESS

EVENT CORR. ENGINE

Inf. and event processor

Sit. awareness represent.

Data analytics

Multi level impact analysis

THREAT INTELIGENCE

Intelligence collector

Attacks predictor

Visual analytics

Information sharing

RESPONSE & MITIGATION

Response & mitig. engine

Post event analysis

RECOVERY

Software recovery engine

E-COMMERCE ECOSYSTEM

Delivery service

Customer

Vendor

Web Host

Payment service

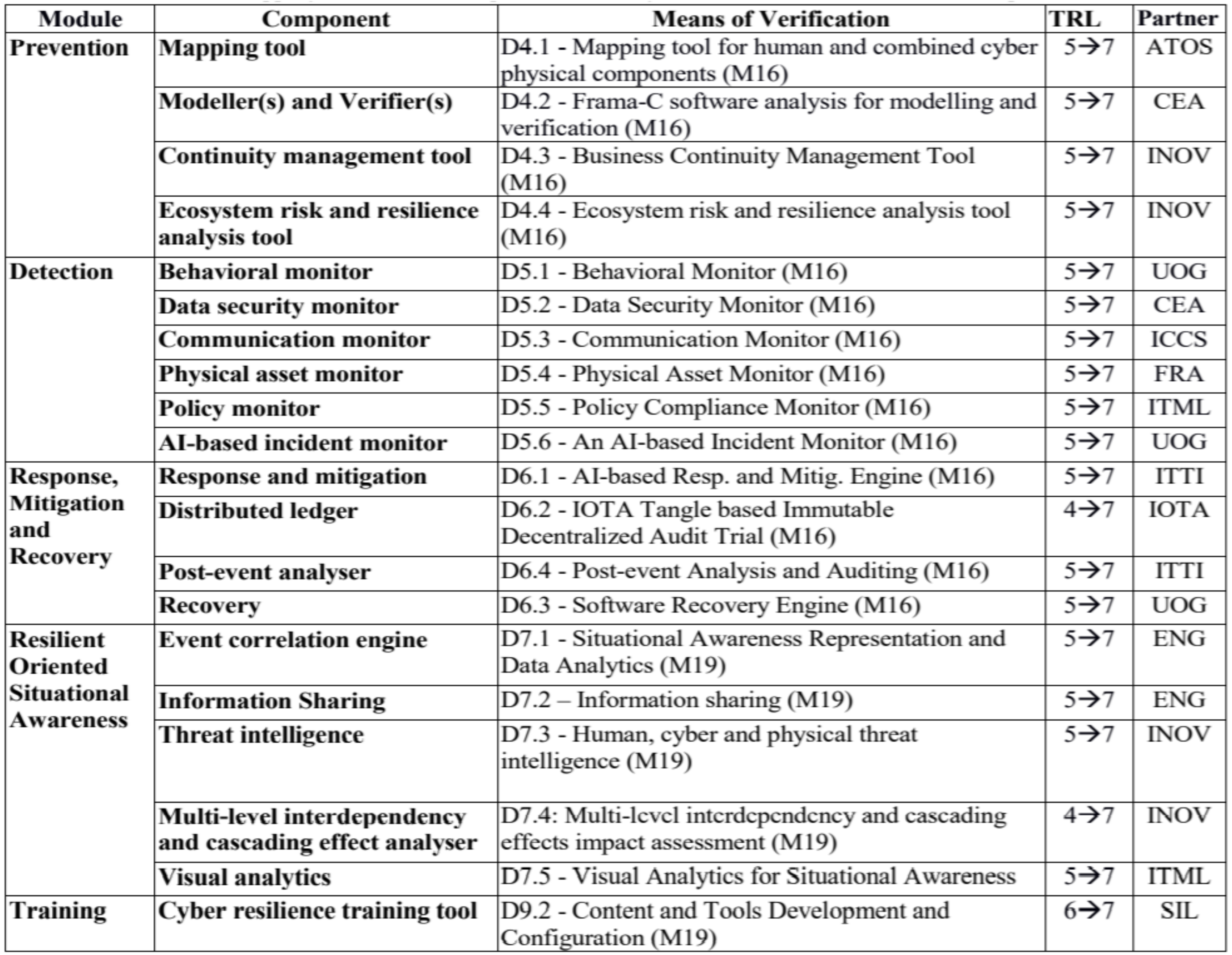
TRAINING AND AWARENESS

Content development

Cyber resilience training tool

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

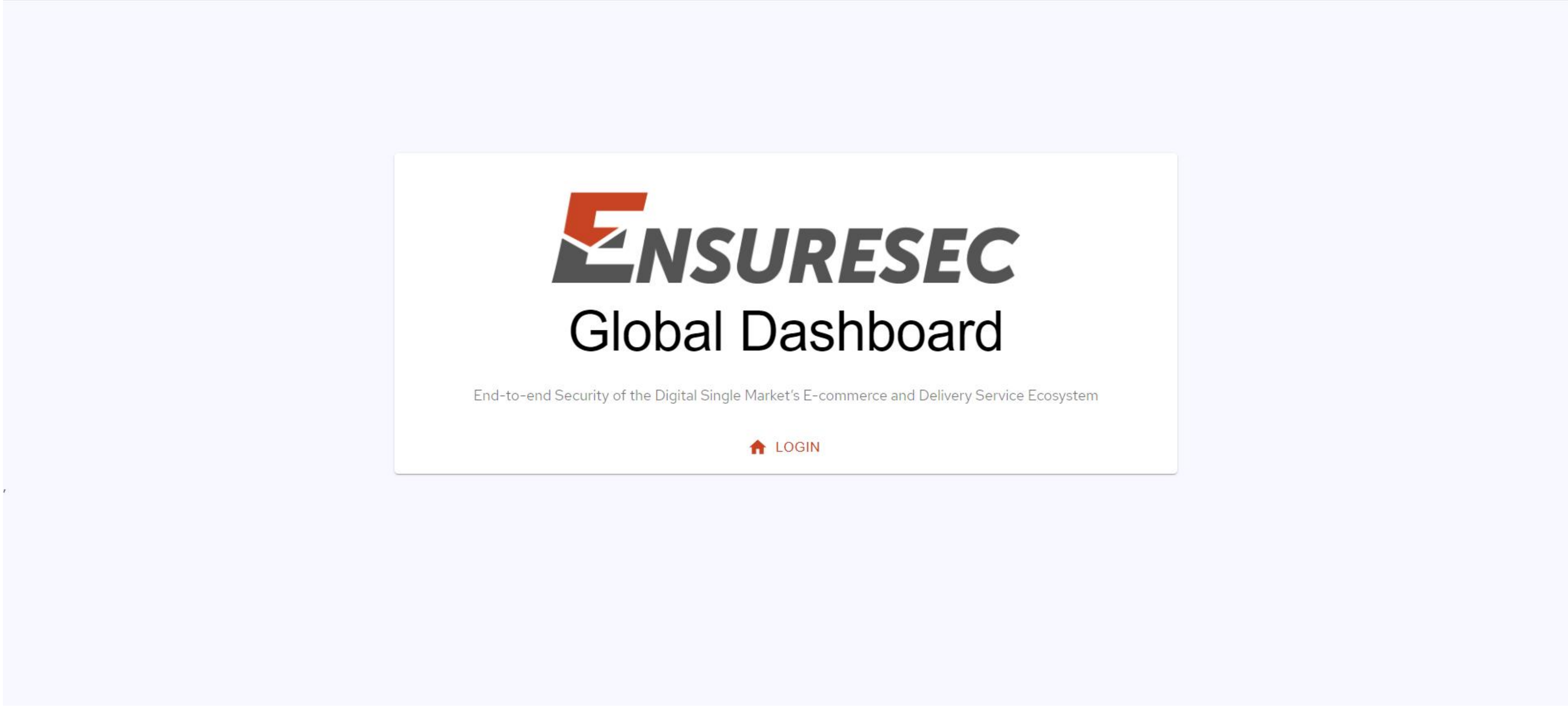
The ENSURESEC Technical Solution – Technical Results



Module	Component	Means of Verification	TRL	Partner
Prevention	**Mapping tool**	D4.1 - Mapping tool for human and combined cyber physical components (M16)	5→7	ATOS
	Modeller(s) and Verifier(s)	D4.2 - Frama-C software analysis for modelling and verification (M16)	5→7	CEA
	Continuity management tool	D4.3 - Business Continuity Management Tool (M16)	5→7	INOV
	Ecosystem risk and resilience analysis tool	D4.4 - Ecosystem risk and resilience analysis tool (M16)	5→7	INOV
Detection	**Behavioral monitor**	D5.1 - Behavioral Monitor (M16)	5→7	UOG
	Data security monitor	D5.2 - Data Security Monitor (M16)	5→7	CEA
	Communication monitor	D5.3 - Communication Monitor (M16)	5→7	ICCS
	Physical asset monitor	D5.4 - Physical Asset Monitor (M16)	5→7	FRA
	Policy monitor	D5.5 - Policy Compliance Monitor (M16)	5→7	ITML
	AI-based incident monitor	D5.6 - An AI-based Incident Monitor (M16)	5→7	UOG
Response, Mitigation and Recovery	**Response and mitigation**	D6.1 - AI-based Resp. and Mitig. Engine (M16)	5→7	ITTI
	Distributed ledger	D6.2 - IOTA Tangle based Immutable Decentralized Audit Trial (M16)	4→7	IOTA
	Post-event analyser	D6.4 - Post-event Analysis and Auditing (M16)	5→7	ITTI
	Recovery	D6.3 - Software Recovery Engine (M16)	5→7	UOG
Resilient Oriented Situational Awareness	**Event correlation engine**	D7.1 - Situational Awareness Representation and Data Analytics (M19)	5→7	ENG
	Information Sharing	D7.2 – Information sharing (M19)	5→7	ENG
	Threat intelligence	D7.3 - Human, cyber and physical threat intelligence (M19)	5→7	INOV
	Multi-level interdependency and cascading effect analyser	D7.4: Multi-lcvcl intcrdcpcndcncy and cascading effects impact assessment (M19)	4→7	INOV
	Visual analytics	D7.5 - Visual Analytics for Situational Awareness	5→7	ITML
Training	**Cyber resilience training tool**	D9.2 - Content and Tools Development and Configuration (M19)	6→7	SIL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

The ENSURESEC Technical Solution – Technical Results



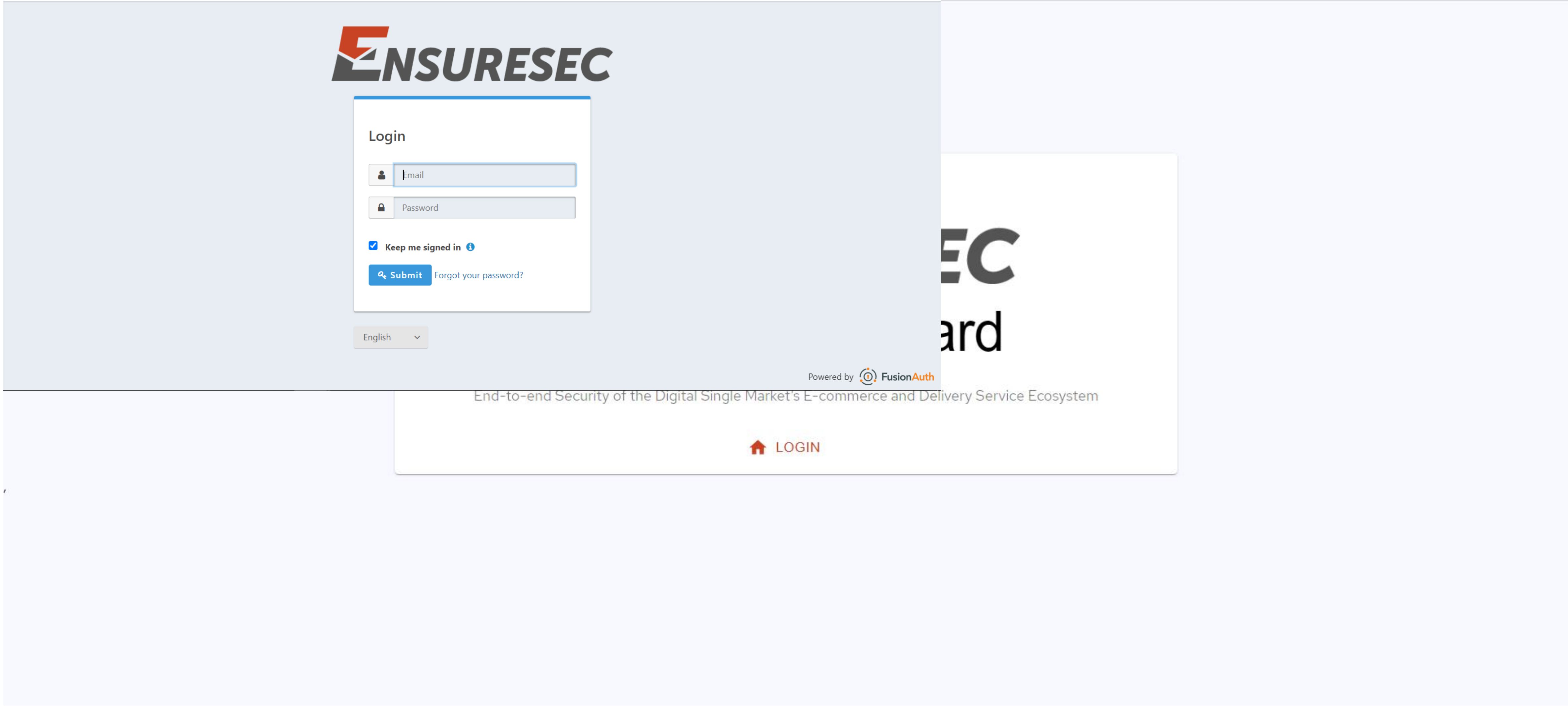
ENSURESEC

Global Dashboard

End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

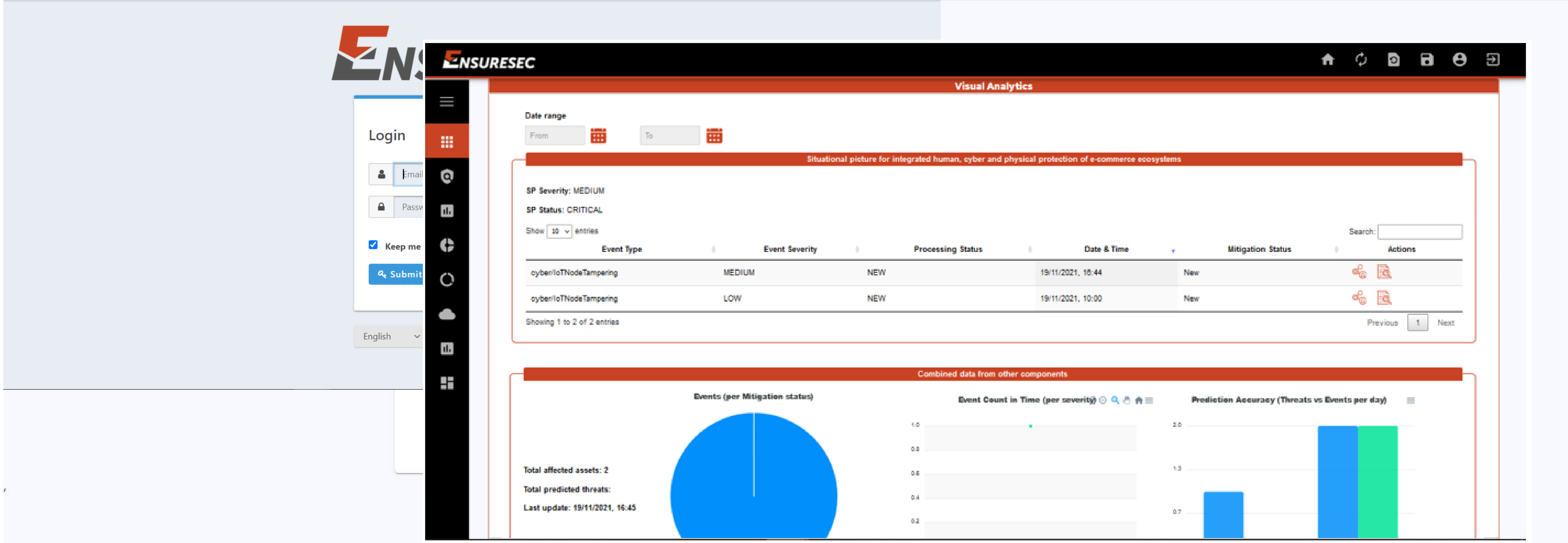
The ENSURESEC Technical Solution – Technical Results



End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

The ENSURESEC Technical Solution – Technical Results



Visual Analytics

Date range

From

To

Situational picture for integrated human, cyber and physical protection of e-commerce ecosystems

SP Severity: MEDIUM

SP Status: CRITICAL

Show 10 entries

Search:

Event Type	Event Severity	Processing Status	Date & Time	Mitigation Status	Actions
cyber/IoTNodeTampering	MEDIUM	NEW	19/11/2021, 16:44	New	
cyber/IoTNodeTampering	LOW	NEW	19/11/2021, 10:00	New	

Showing 1 to 2 of 2 entries

Previous 1 Next

Combined data from other components

Total affected assets: 2

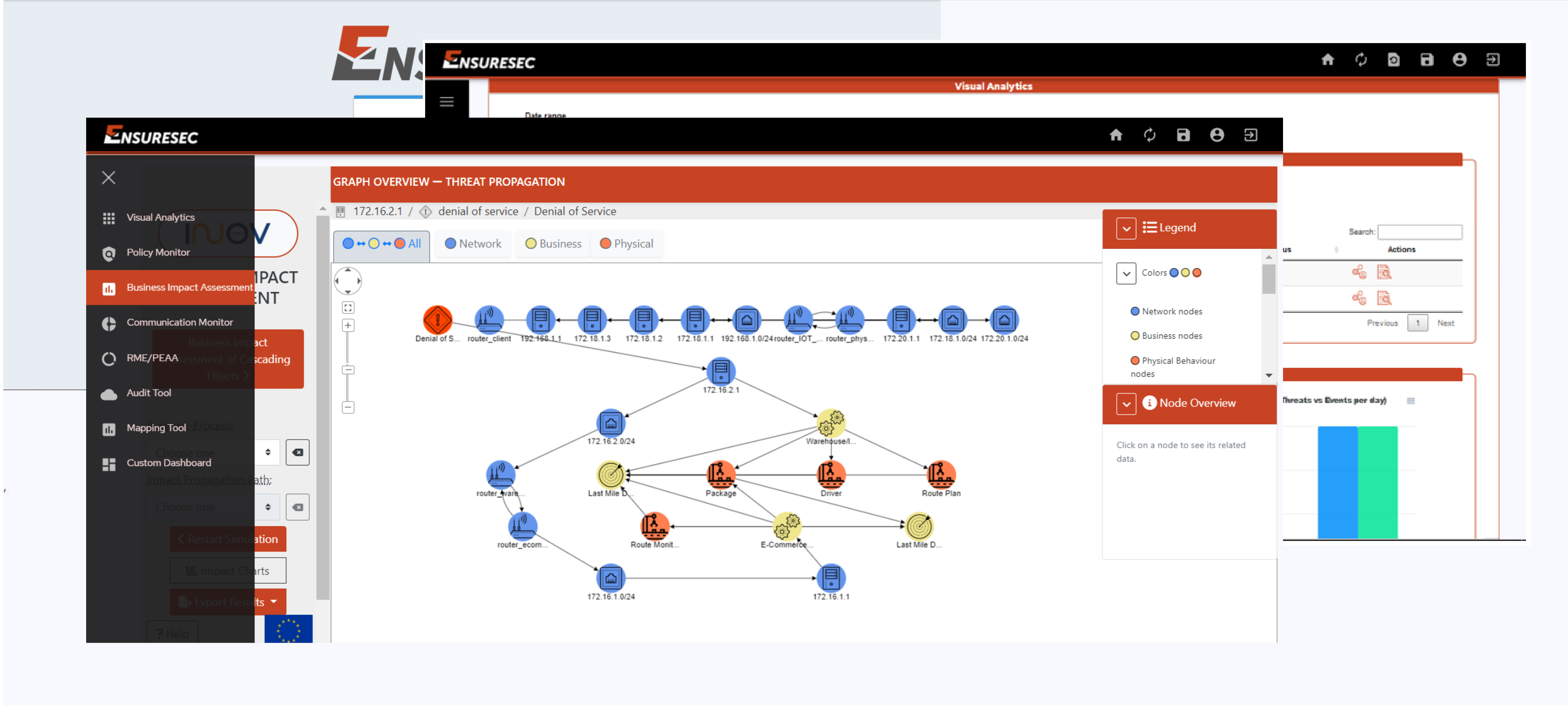
Total predicted threats:

Last update: 19/11/2021, 16:45

Events (per Mitigation status)
Event Count in Time (per severity)
1.0
0.8
0.6
0.4
0.2
Prediction Accuracy (Threats vs Events per day)
2.0
1.3
0.7

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

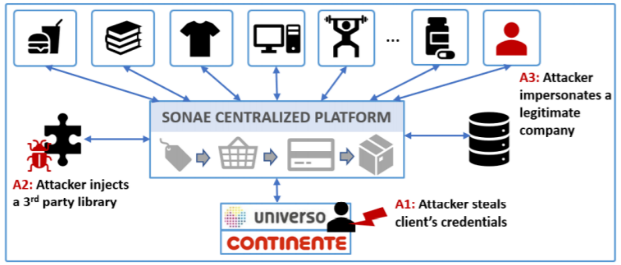
The ENSURESEC Technical Solution – Technical Results



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

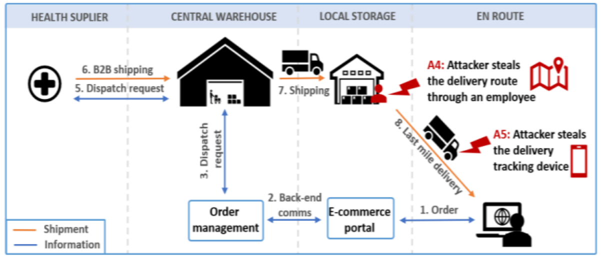
The ENSURESEC Technical Solution – Use Cases & Scenarios

- **Pilot Use Case 1: Cyber-attacks on e-commerce platform**
  - Main end-user – Large multinational retail company
  - Main goal – Protection of customers' data
  - Types of threats considered:
    - Phising campaign
    - Injection attack
    - Third-party attack

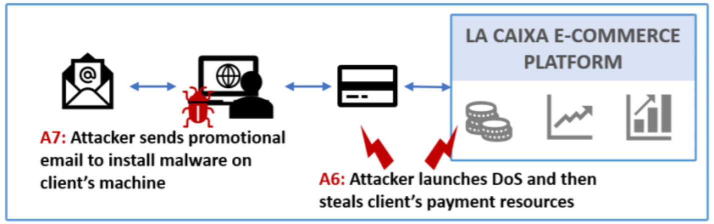


...
A3: Attacker impersonates a legitimate company
SONAE CENTRALIZED PLATFORM
A2: Attacker injects a 3rd party library
universo
CONTINENTE
A1: Attacker steals client's credentials

- **Pilot Use Case 2: Physical attacks on pharmacy e-commerce operator**
  - Main end-users – Online pharmacy, logistics company, secure transportation company
  - Main goal – Protection of the supply chain from physical attacks, and mitigation of cascading effects
  - Types of threats considered:
    - Attacker steals the product delivery route through a corrupted/malicious insider
    - Attacker steals the delivery tracking device through a corrupted/malicious insider



- **Pilot Use Case 3: Cyber-physical attacks on Bank providing online payment services**
  - Main end-users – Financial institution providing online payment services to e-commerce
  - Main goal – Protection of online payment operations and mitigation of payment frauds
  - Types of threats considered:
    - Attacker steals sensitive client's payment resources through ransomware attack
    - Attacker steals client's data through social engineering attack to the client or an employee

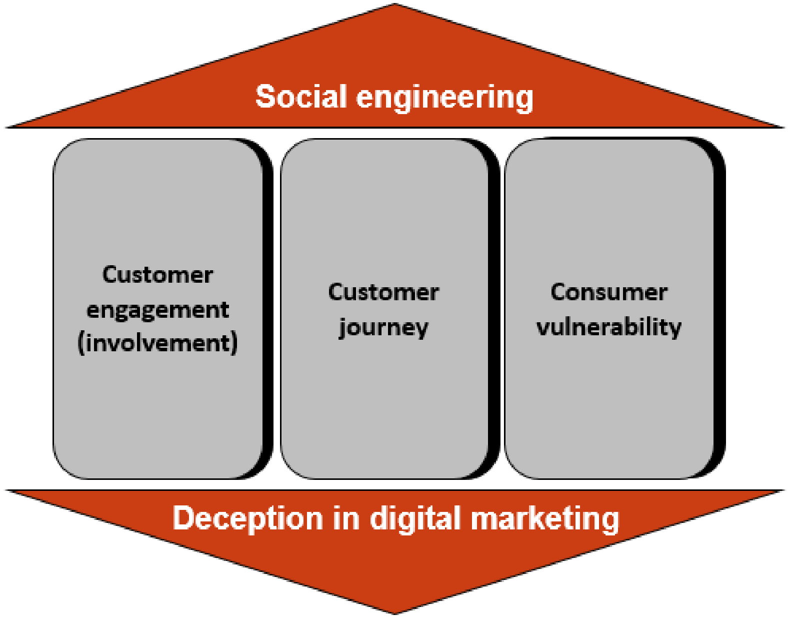


LA CAIXA E-COMMERCE PLATFORM
A7: Attacker sends promotional email to install malware on client's machine
A6: Attacker launches DoS and then steals client's payment resources

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

The ENSURESEC Training and Awareness Campaign

- Investigation of **malicious marketing** through consumer behaviour studies
- Review **tools, techniques and methodologies** used today for both legitimate purposes in digital marketing, and for malicious purposes to commit online frauds and other cybercrimes
- Review **user shopping habits** and common e-commerce and social media human **interaction vulnerabilities** that can be exploited by malicious users



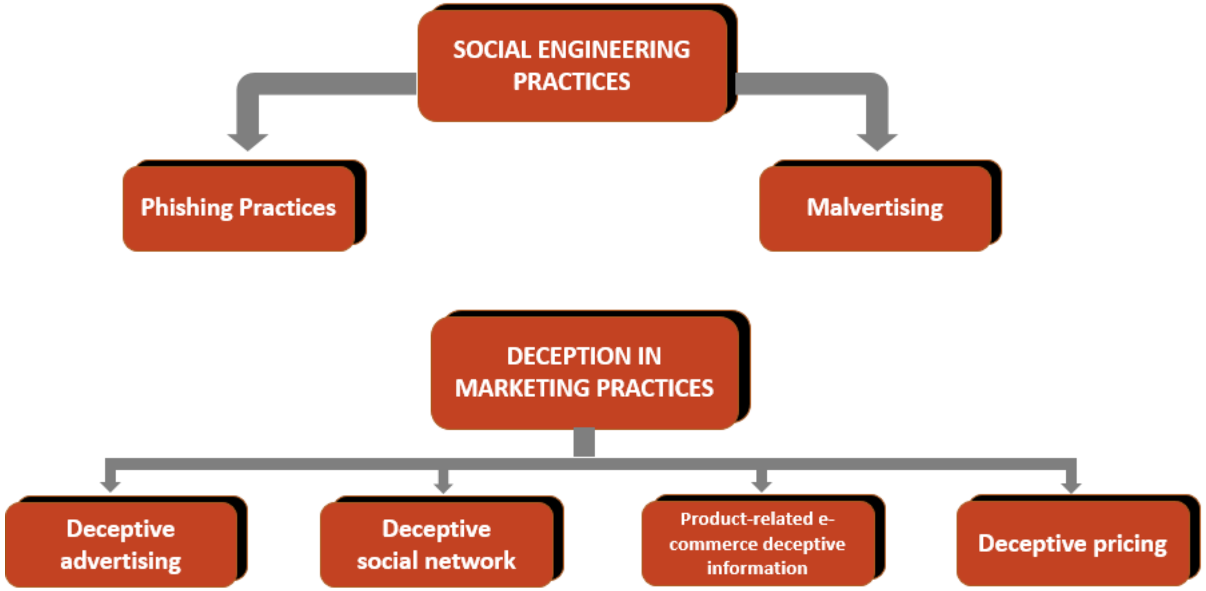
Social engineering

Customer engagement (involvement)

Customer journey

Consumer vulnerability

Deception in digital marketing



SOCIAL ENGINEERING PRACTICES

Phishing Practices

Malvertising

DECEPTION IN MARKETING PRACTICES

Deceptive advertising

Deceptive social network

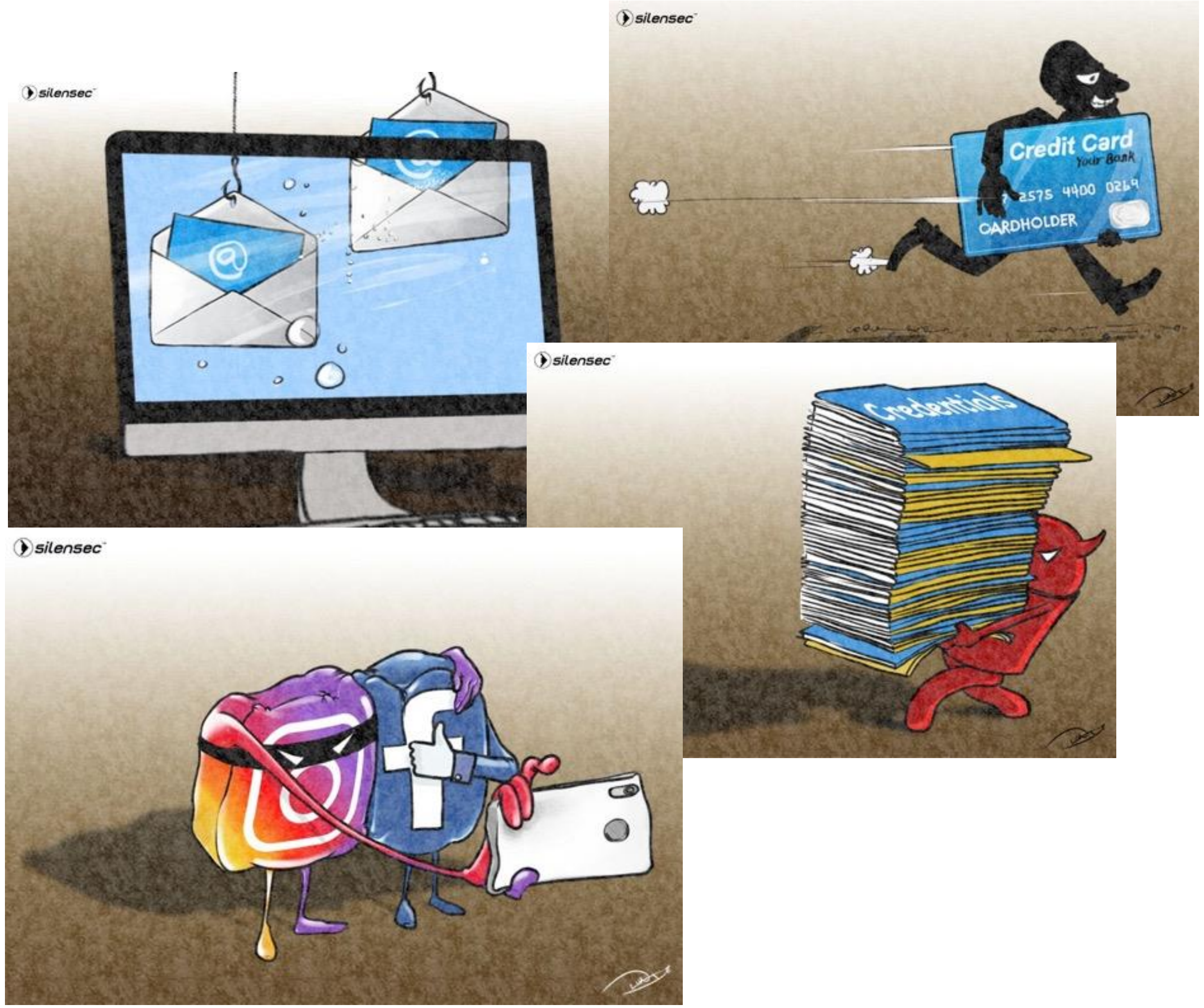
Product-related e-commerce deceptive information

Deceptive pricing

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.

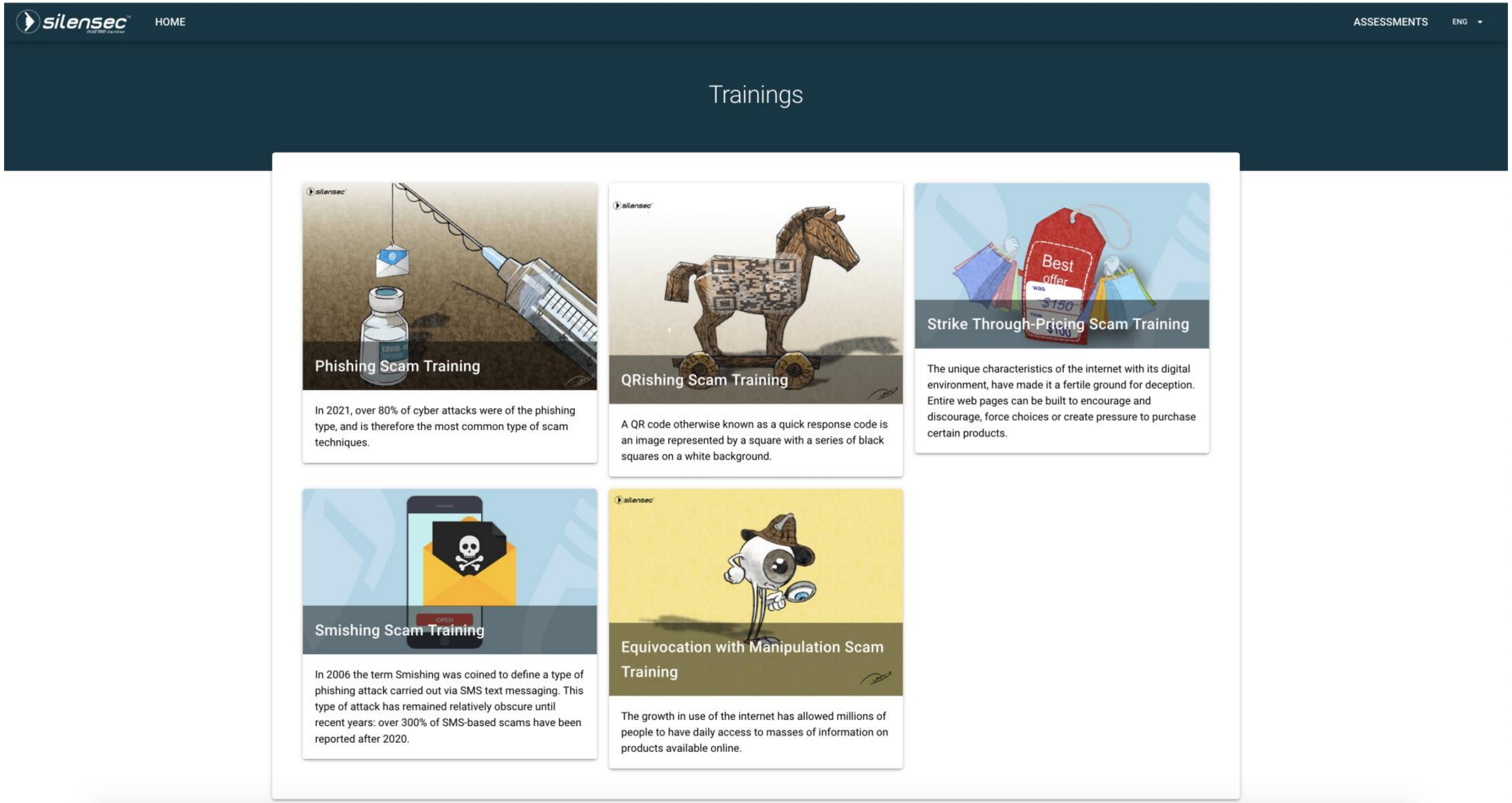
The ENSURESEC Training and Awareness Campaign

- Development of e-commerce tailored cybersecurity training and awareness **contents and tools**
- Development of over 100 illustrations for the **security awareness content**
  - Delivered as part of the campaign
  - Tailored to different target audience
- Templates for **attack simulations**
  - Malicious Landing Pages and Websites
  - Sample T&C
  - Social Media Campaigns
  - Sample phishing emails
- Training and Awareness Content
- Translation to 6 European languages (English, Greek, Italian, Spanish, Romanian, German)
- Campaign: https://becyberaware.eu/



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

BeCyberAware – Training Videos



Trainings

Phishing Scam Training

In 2021, over 80% of cyber attacks were of the phishing type, and is therefore the most common type of scam techniques.

QRishing Scam Training

A QR code otherwise known as a quick response code is an image represented by a square with a series of black squares on a white background.

Strike Through-Pricing Scam Training

The unique characteristics of the internet with its digital environment, have made it a fertile ground for deception. Entire web pages can be built to encourage and discourage, force choices or create pressure to purchase certain products.

Smishing Scam Training

In 2006 the term Smishing was coined to define a type of phishing attack carried out via SMS text messaging. This type of attack has remained relatively obscure until recent years: over 300% of SMS-based scams have been reported after 2020.

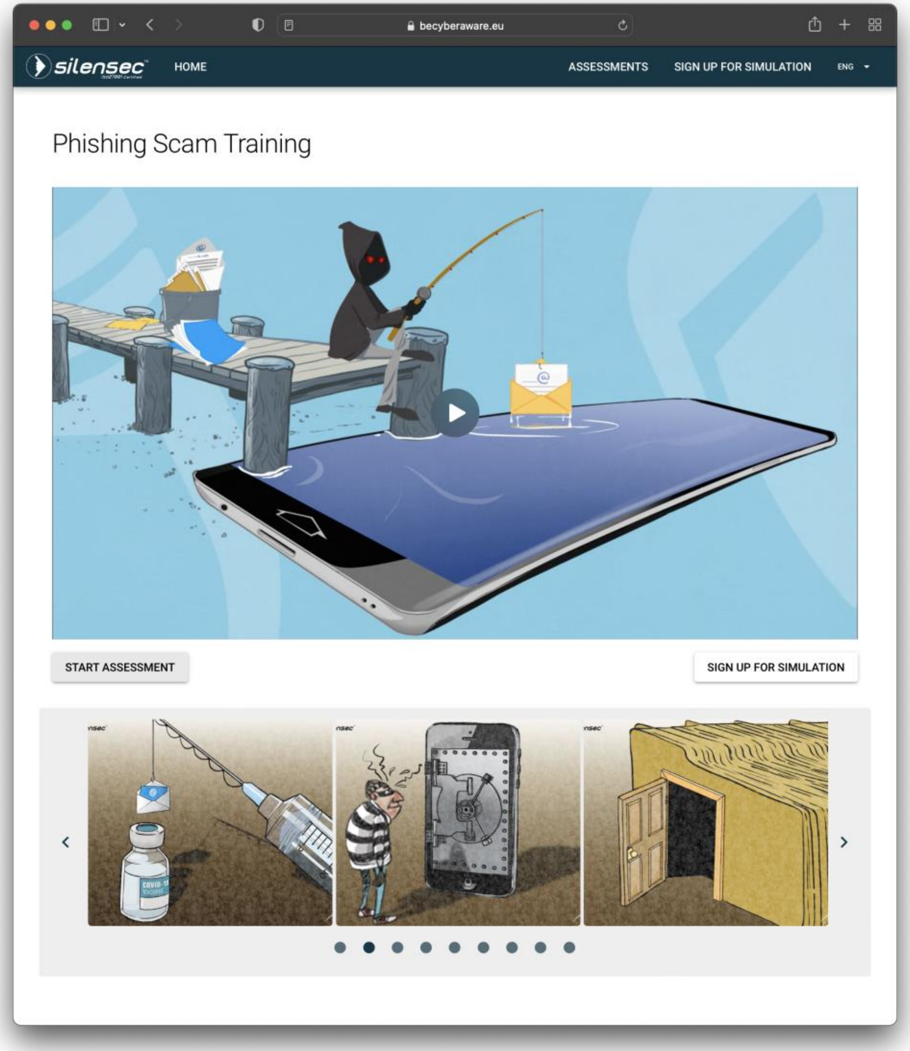
Equivocation with Manipulation Scam Training

The growth in use of the internet has allowed millions of people to have daily access to masses of information on products available online.

https://becyberaware.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

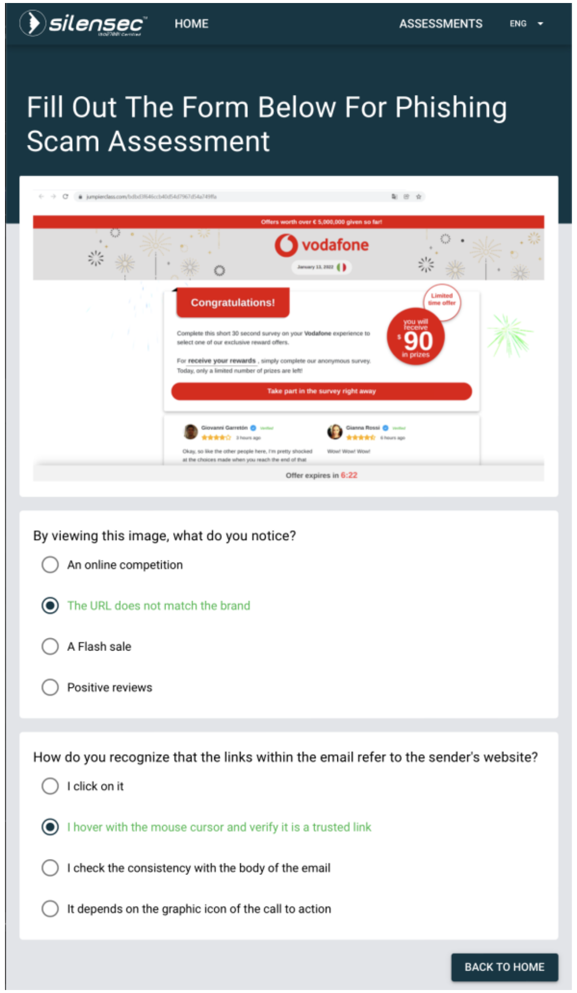
BeCyberAware – Sample Training Videos and Posters



- Video Training
- Poster Illustrations
- Navigation
    - Self assessment
    - Sign up for the simulation

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.

BeCyberAware – Self-Assessment Questions



Fill Out The Form Below For Phishing Scam Assessment

jumpierclass.com/bdbd3f646ccb40d54d7967d54a749ffa

Offers worth over € 5,000,000 given so far!

vodafone

January 13, 2022

Congratulations!

Limited time offer

you will receive $ 90 in prizes

Complete this short 30 second survey on your **Vodafone** experience to select one of our exclusive reward offers.

For **receive your rewards** , simply complete our anonymous survey. Today, only a limited number of prizes are left!

Take part in the survey right away

Giovanni Garretón Verified ★★★★☆ 3 hours ago
Okay, so like the other people here, I'm pretty shocked at the choices made when you reach the end of that

Gianna Rossi Verified ★★★★★ 6 hours ago
Wow! Wow! Wow!

Offer expires in 6:22

By viewing this image, what do you notice?

○ An online competition

● The URL does not match the brand

○ A Flash sale

○ Positive reviews

How do you recognize that the links within the email refer to the sender's website?

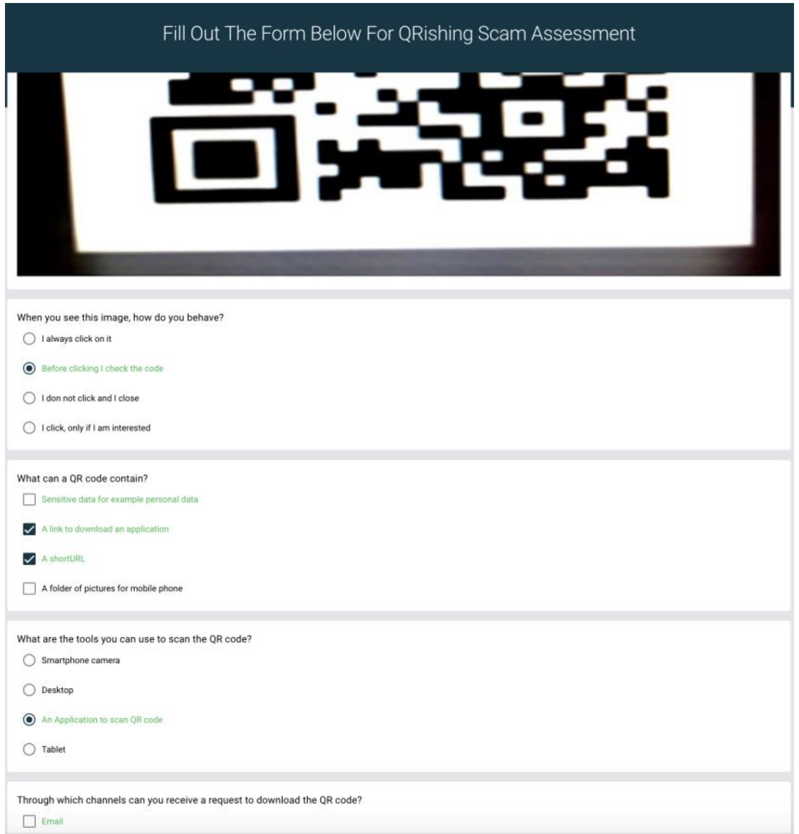
○ I click on it

● I hover with the mouse cursor and verify it is a trusted link

○ I check the consistency with the body of the email

○ It depends on the graphic icon of the call to action

BACK TO HOME



Fill Out The Form Below For QRishing Scam Assessment

When you see this image, how do you behave?

○ I always click on it

● Before clicking I check the code

○ I don not click and I close

○ I click, only if I am interested

What can a QR code contain?

□ Sensitive data for example personal data

☑ A link to download an application

☑ A shortURL

□ A folder of pictures for mobile phone

What are the tools you can use to scan the QR code?

○ Smartphone camera

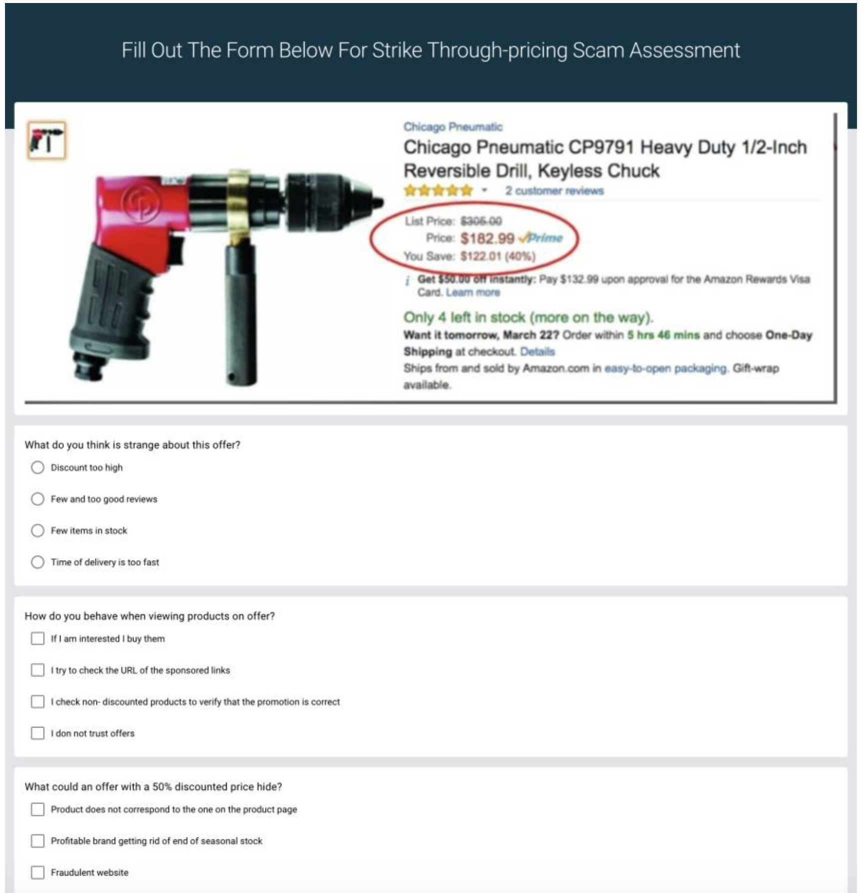
○ Desktop

● An Application to scan QR code

○ Tablet

Through which channels can you receive a request to download the QR code?

□ Email



Fill Out The Form Below For Strike Through-pricing Scam Assessment

Chicago Pneumatic

Chicago Pneumatic CP9791 Heavy Duty 1/2-Inch Reversible Drill, Keyless Chuck

★★★★★ 2 customer reviews

List Price: ~~$306.00~~
Price: $182.99 ✓Prime
You Save: $122.01 (40%)

Get $50.00 off instantly: Pay $132.99 upon approval for the Amazon Rewards Visa Card. Learn more

Only 4 left in stock (more on the way).

Want it tomorrow, March 22? Order within 5 hrs 46 mins and choose **One-Day Shipping** at checkout. Details

Ships from and sold by Amazon.com in easy-to-open packaging. Gift-wrap available.

What do you think is strange about this offer?

○ Discount too high

○ Few and too good reviews

○ Few items in stock

○ Time of delivery is too fast

How do you behave when viewing products on offer?

□ If I am interested I buy them

□ I try to check the URL of the sponsored links

□ I check non- discounted products to verify that the promotion is correct

□ I don not trust offers

What could an offer with a 50% discounted price hide?

□ Product does not correspond to the one on the product page

□ Profitable brand getting rid of end of seasonal stock

□ Fraudulent website

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

ENSURESEC

Expected Impact

ENSURESEC Expected Impact

Short term
Medium term
Long term

Short term

- State of the art analysis – identification of the most **critical assets** in e-commerce, physical and cyber **vulnerabilities**, **risk scenarios**, as well as **detection technologies**
- User validation – **demonstration** of the developed technologies and evaluation by end-users and relevant stakeholders regarding their **acceptance, usability, usefulness and trust**

Medium term

- Innovative tools, concepts and technologies for e-commerce protection – **Innovative solutions** to **prevent, detect, respond and mitigate** physical and cyber **threats**, as well as to **monitor the environment**, and to **protect and train the users**
- Standard-based risk management methodology – **methodology** to **assess, evaluate, predict and manage** combined **cyber and physical security risks**
- Dissemination – **Wide dissemination of results** among relevant user groups and a variety of stakeholders

Long term

- Standardisation
  - Promote the **convergence of safety and security standards** and fostering the **distribution of project‘s outcomes** among standardization bodies
  - Contributions to relevant **sectorial frameworks or regulatory initiatives** directly or indirectly related to e-commerce

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.

ENSURESEC Expected Impact

- Reducing financial and job losses in e-commerce SMEs:
  - ENSURESEC contributes to the **growth of the Digital Single Market** by **protecting** e-commerce companies (especially SMEs) **against economic damage and jobs losses** caused by security breaches, as well as by training citizens to be resilient and confident in themselves against such threats.
- Promoting the transparency of e-commerce operations:
  - ENSURESEC promotes **social accountability through unprecedented transparency** among businesses and citizen users, by providing a complete audit trail of cyber and physical security incidents.
- Reducing citizens' fear, stress and anxiety towards e-commerce security threats:
  - ENSURESEC **prevents the psychological impact and fear** caused by the perception of increased security risk in e-commerce. It achieves this by reducing the number of incidents occurring and by increasing citizen users‘ understanding of the precise risk and how to protect against it.
- Promoting equality in the use of e-commerce, regardless of background and context:
  - ENSURESEC contributes to **fairness and equality in the use of e-commerce**, from the perspective of both the company providing e-commerce and the citizen using it. It achieves this by tailoring training to the needs of users of different backgrounds and technological experience, and by making its technological offering open-source and available to organizations regardless of their financial capacities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

ENSURESEC

Thank you!

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.