ENSURESEC

CPS4CIP 2021 – CYBER-PHYSICAL SECURITY FOR CRITICAL INFRASTRUCTURES PROTECTION

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.

CPS4CIP 2021 Workshop – 8th of October 2021

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

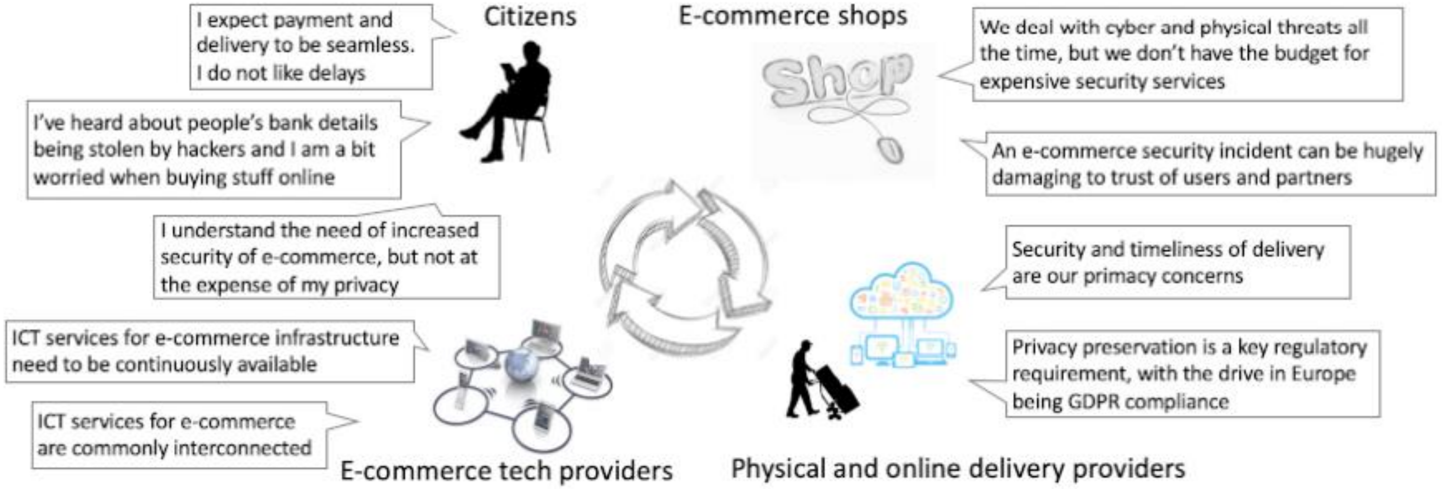
No.	Participant Organisation Name	Acronym	Type	Country
1	INOV INESC Inovação	INOV	RTO	PT
2	Sonae MC Serviços Partilhados	SONAE	LE	PT
3	G4S Telematix	G4S	LE	GR
4	Caixabank S.A.	CXB	LE	ES
5	Atos Spain S.A.	ATOS	LE	ES
6	Engineering	ENG	LE	IT
7	Milsped Group	MSPED	LE	RS
8	Tofarmakeiomou	TOFAR	SME	GR
9	Relational Romania Srl	REL	SME	RO
10	Itti Sp. Z O.O.	ITTI	SME	PO
11	G & N Silensec Ltd	SIL	SME	CY
12	Search-Lab Sec. Eval. Analysis and Research	SLAB	SME	HU
13	Internet of Things Applications and Multi-Layer Development	ITML	SME	CY
14	IOTA Stiftung	IOTA	OTH	DE
15	Lithuanian Cybercrime Center of Excellence	L3CE	NGO	LT
16	Commissariat à L'énergie Atomique et aux Énergies Alternatives	CEA	RTO	FR
17	Fraunhofer - Gesellshaft Zur Forderung der Angewandten Forschung	FRA	RTO	DE
18	Abi Lab Centro Di Ricerca e Innov. per la Banca	ABI	RTO	IT
19	Software Imagination & Vision Srl	SIMAVI	LE	RO
20	Inst. of Communication and Computer Systems	ICCS	RTO	GR
21	Katholieke Universiteit Leuven	KUL	UNIV	BE
22	University of Greenwich	UOG	UNIV	UK

Project Coordinator: INOV; **Technical Manager:** CEA

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

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

E-commerce shops

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

E-commerce tech providers

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

ICT services for e-commerce are commonly interconnected

Physical and online delivery providers

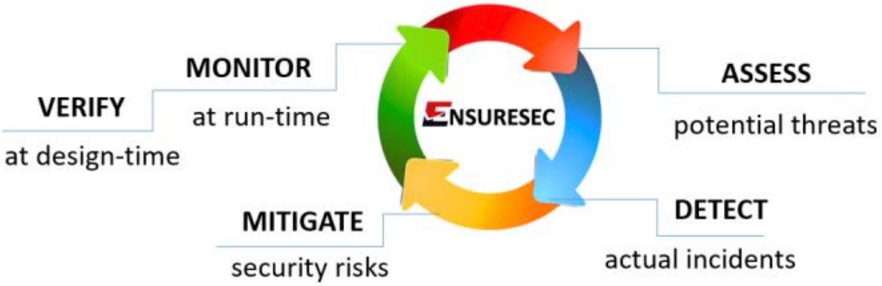
Security and timeliness of delivery are our primacy concerns

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**.

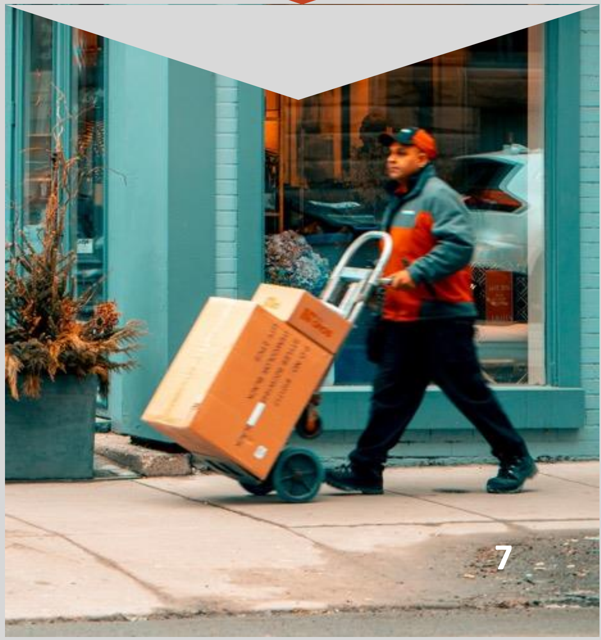


- The project will also create **security awareness** among SMEs and their clients, while **promoting trust in the e-commerce ecosystem**, through the **creation of dedicated content** and the implementation of **tools** for **training and educating** e-commerce stakeholders on cyber security and improve 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

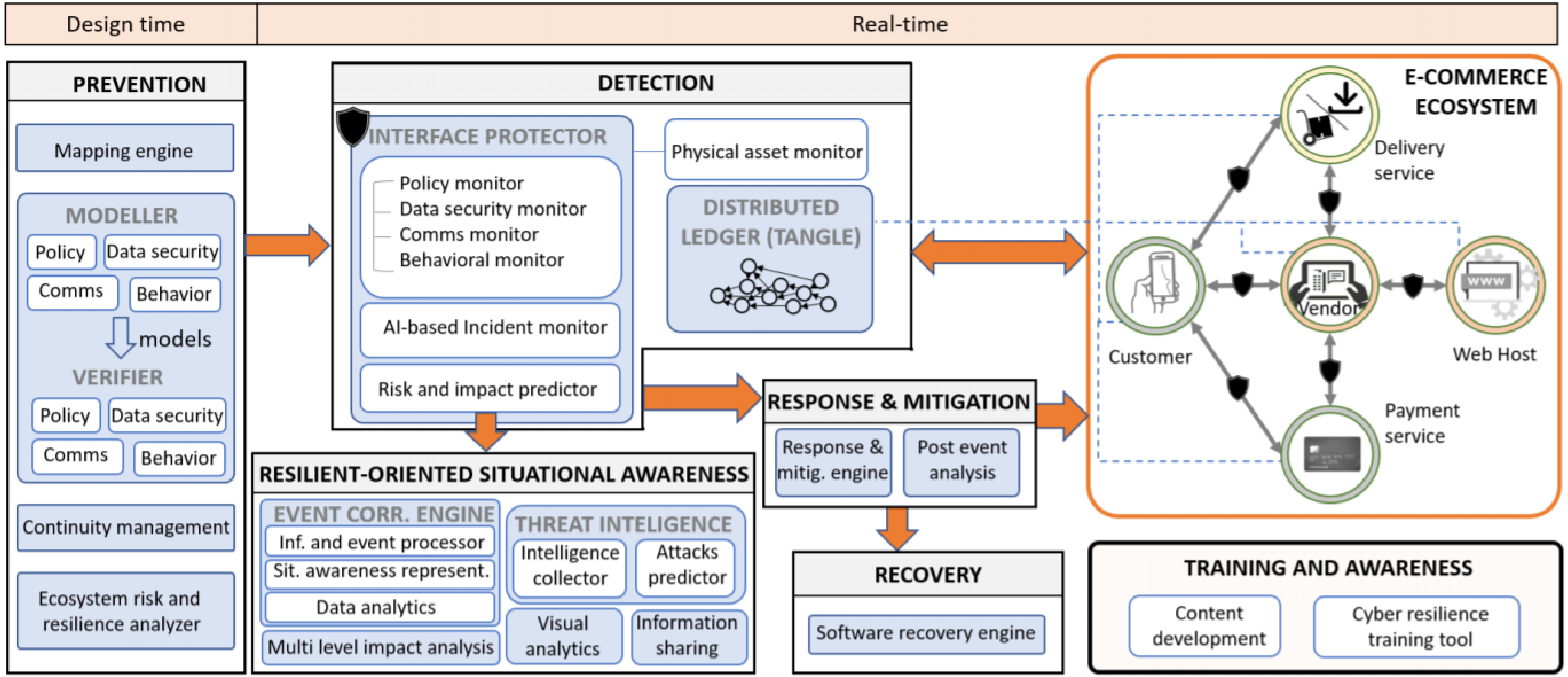


The ENSURESEC Technical Solution – Overall concept

- 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

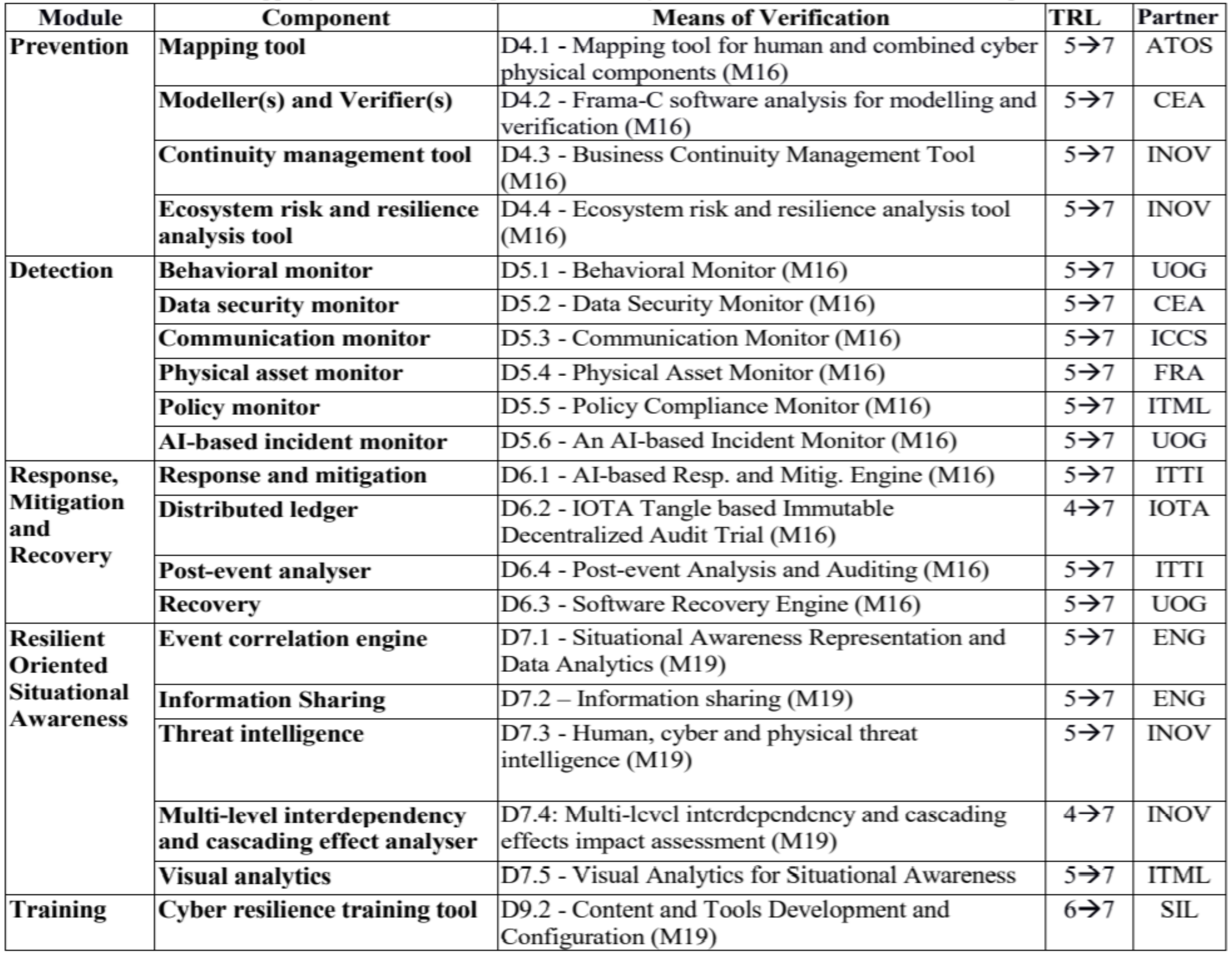
TRAINING AND AWARENESS

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

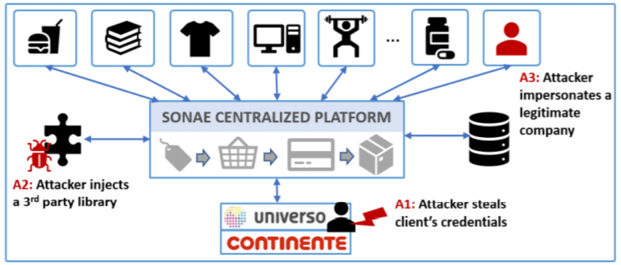


Module	Component	Means of Verification	TRL	Partner
Prevention	**Mapping tool**	D4.1 - Mapping tool for human and combined cyber physical components (M16)	5→7	ATOS
	Modeller(s) and Verifier(s)	D4.2 - Frama-C software analysis for modelling and verification (M16)	5→7	CEA
	Continuity management tool	D4.3 - 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.

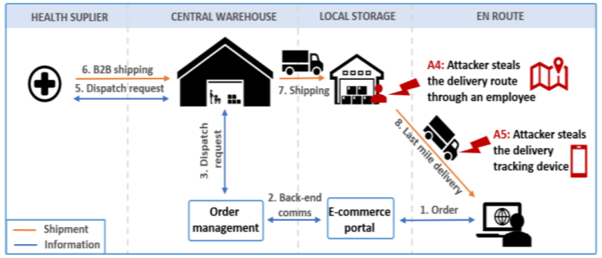
The ENSURESEC Technical Solution – Use Cases & Scenarios

- **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

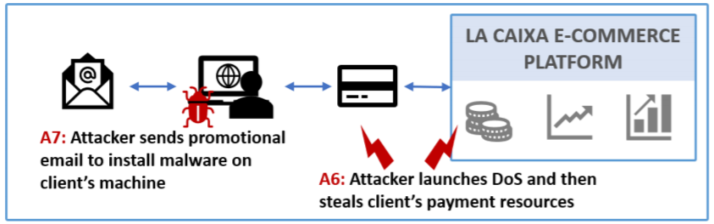


...
A3: Attacker impersonates a legitimate company
SONAE CENTRALIZED PLATFORM
A2: Attacker injects a 3rd party library
universo
CONTINENTE
A1: Attacker steals client’s credentials

- **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

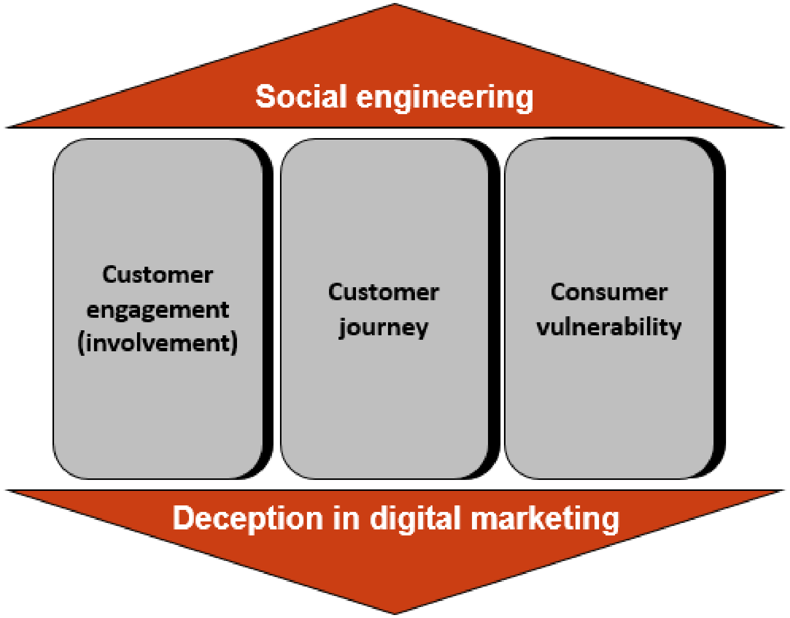


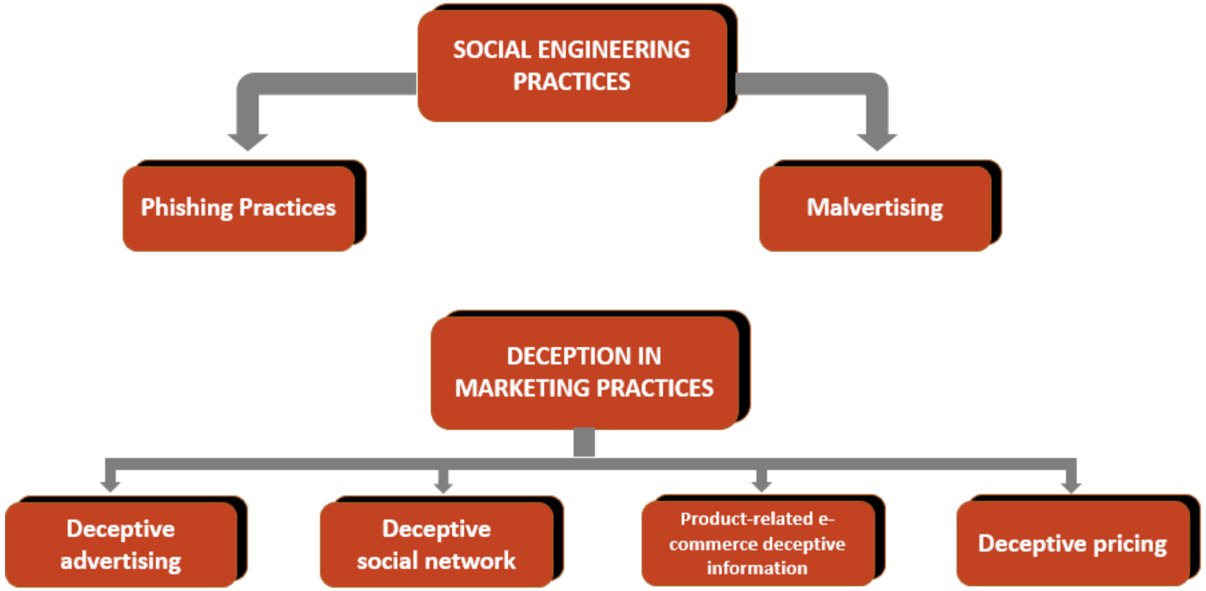
LA CAIXA E-COMMERCE PLATFORM
A7: Attacker sends promotional email to install malware on client’s machine
A6: Attacker launches DoS and then steals client’s payment resources

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

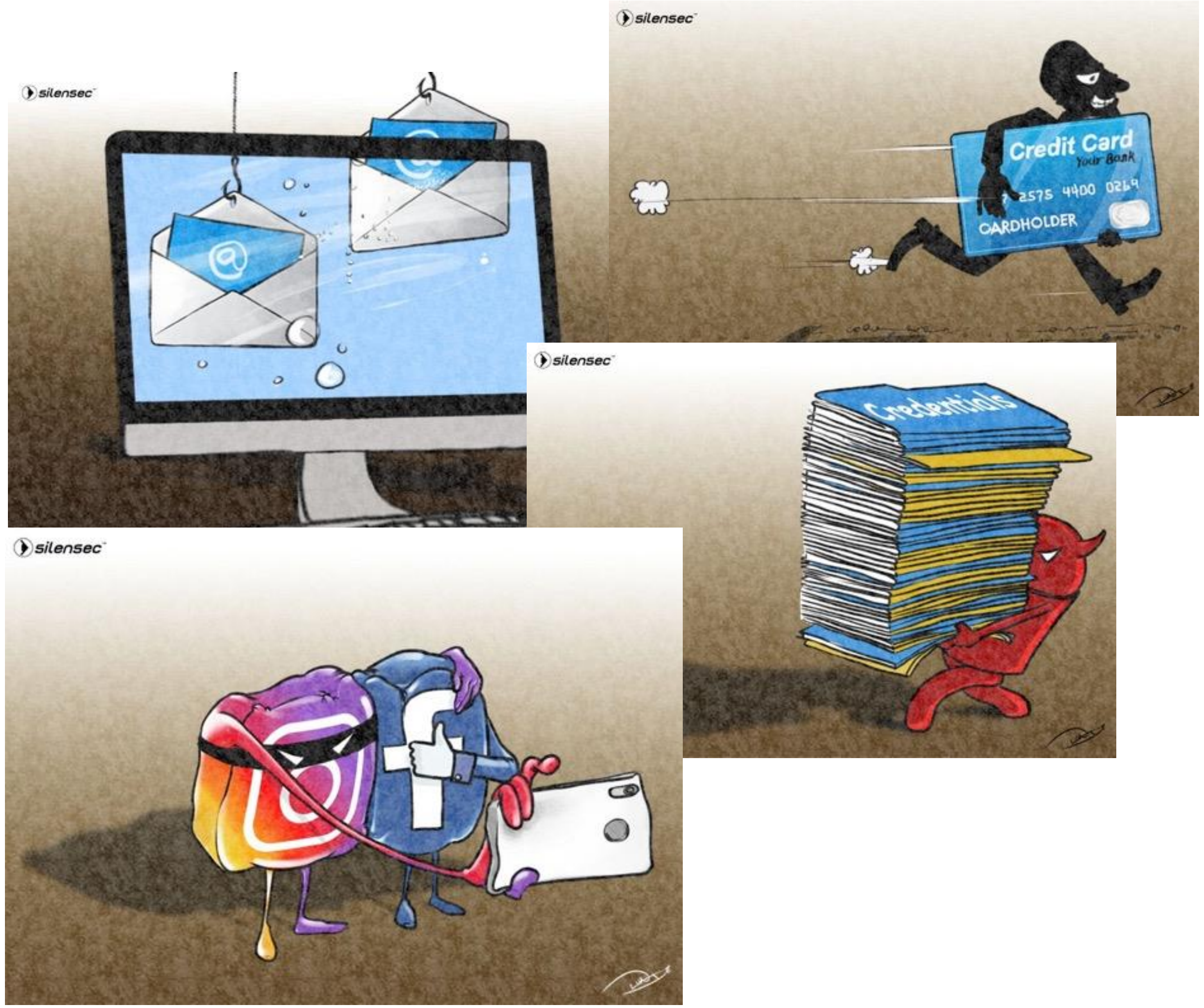

Social engineering
Customer engagement (involvement)
Customer journey
Consumer vulnerability
Deception in digital marketing


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 **contents and tools** needed for the execution of security training and awareness campaign
- 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 at least 5 European languages



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.