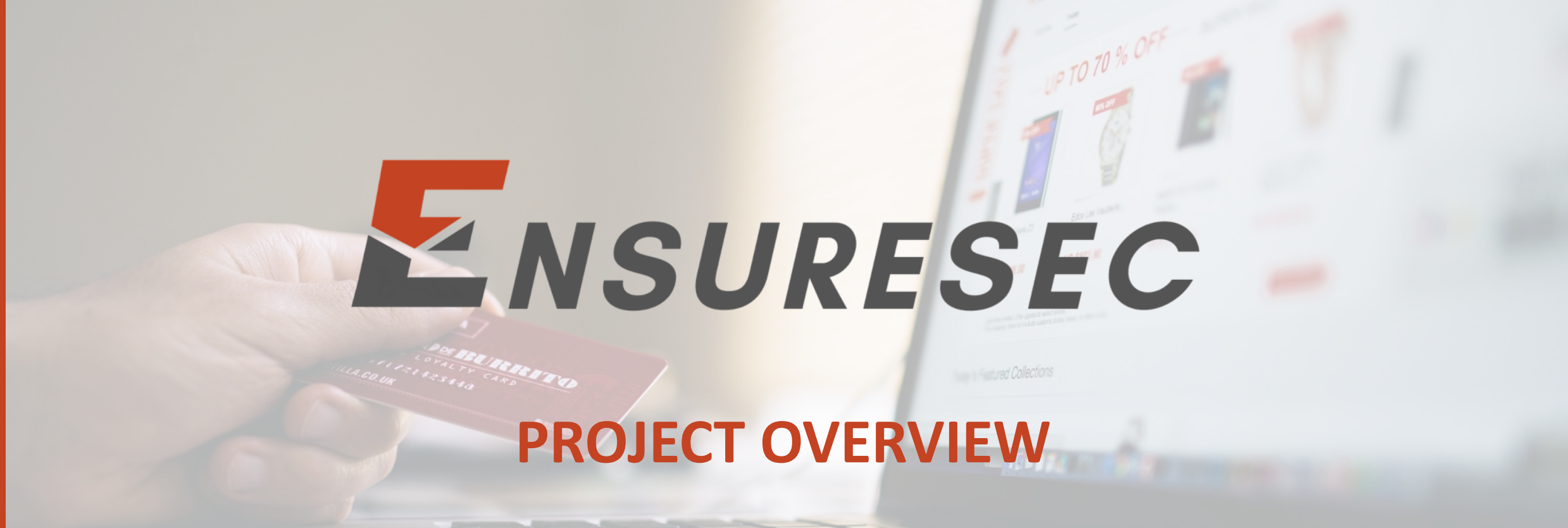


ENSURESEC

PROJECT OVERVIEW

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

Emiliano Anzellotti

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

Project Overview – Il Consorzio 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 – La missione

- **Il commercio elettronico** è un pilastro principale del mercato unico digitale dell'UE e come tale è fondamentale per il futuro e l'autonomia dell'UE**.**
- Al fine di fornire un migliore accesso ai beni e servizi digitali, è necessario **creare fiducia e sicurezza tra gli attori del commercio elettronico**. Ciò è particolarmente impegnativo negli ecosistemi di e-commerce a causa dell'ampia superficie di attacco che deve essere affrontata e della visibilità limitata delle varie entità coinvolte nella catena del valore.

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

Project Overview – Principali obiettivi

- ENSURESEC mira a sviluppare una soluzione per fornire alle infrastrutture e agli ecosistemi di e-commerce una **protezione permanente contro le minacce informatiche, cyber-fisiche e fisiche, compresi gli effetti a cascata**.
- L'obiettivo è sviluppare un toolkit di sicurezza che affronti l'intero arco dell'ecosistema dell'e-commerce, con le sue varie forme di pagamento e consegna (virtuali, online e fisiche) attraverso l'implementazione di diversi moduli che assicurano che le operazioni siano protette dalla progettazione, oltre a fornire misure di monitoraggio, risposta, ripristino e mitigazione continue in fase di esecuzione.

- Il progetto creerà inoltre consapevolezza riguardo la sicurezza tra le PMI e i loro clienti, promuovendo al contempo la fiducia nell'ecosistema dell'e-commerce, attraverso la creazione di contenuti dedicati e l'implementazione di strumenti per la formazione e l'educazione degli stakeholder dell'e-commerce sulla sicurezza informatica e migliorerà la resilienza di l'ecosistema.
- Infine, la soluzione sarà dimostrata e convalidata in un ambiente pertinente entro la fine del progetto, applicando i concetti ENSUESEC in tre diversi casi d'uso.

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

ENSURESEC

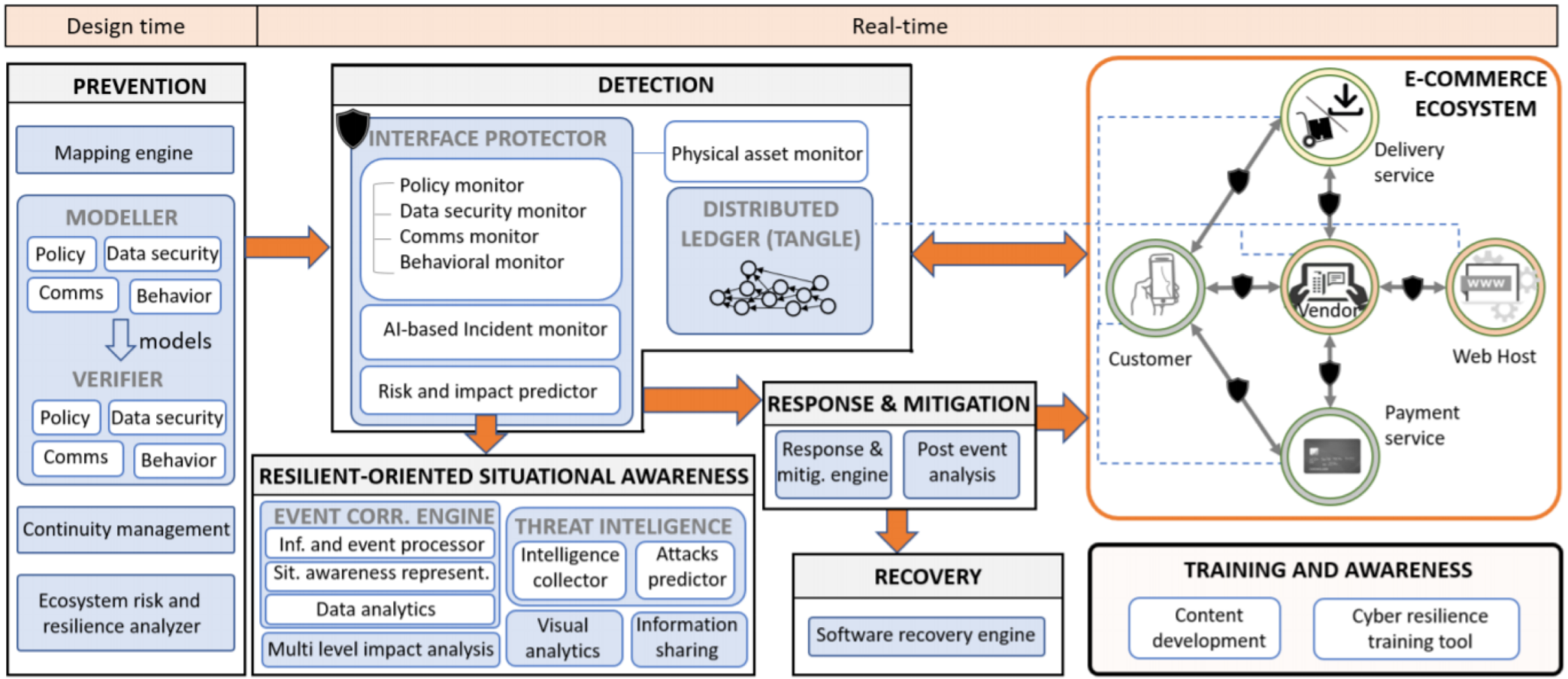
La soluzione Socio-Tecnologica

Principali linee guida

- Il concetto ENSURESEC si basa su un toolkit di sicurezza open source distribuito per proteggere le interfacce dell'ecosistema e-commerce, attraverso l'integrazione di sei moduli principali:
  - **Prevenzione (by design)** – Valuta e certifica che il design delle interfacce di sistema sia sicuro contro determinate classi di attacchi critici e vulnerabilità;
  - **Detection** – monitora le operazioni dell'interfaccia di runtime a livello di applicazione e di rete per verificarne la resilienza contro le minacce note e sconosciute;
  - **Response and mitigation** – Comunica una risposta adeguata agli utenti e ai partner interessati e tenta di mitigare l'impatto;
  - **Recovery** – Recupera lo stato del sistema identificando il problema sulla base di una diagnosi basata sulla principio «causa- effetto»;
  - **Continuous situational awareness** – Impiega tecniche avanzate per rilevare continuamente qualsiasi incidente e visualizzarne l'impatto e le interdipendenze;
  - **Training and awareness** – Strumenti basati su giochi e creazione di contenuti dedicati per sensibilizzare i cittadini clienti delle PMI dell'e-commerce sulle potenziali minacce alla sicurezza e formarsi su come evitarle.

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

L’Architettura della soluzione tecnologica di ENSURESEC



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

L’interfaccia operativa

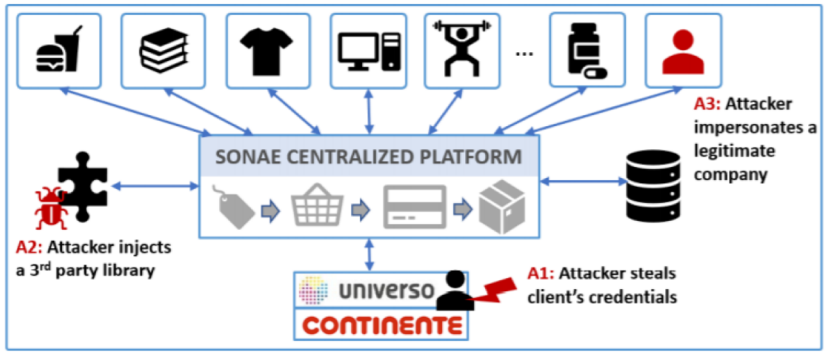
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883242.

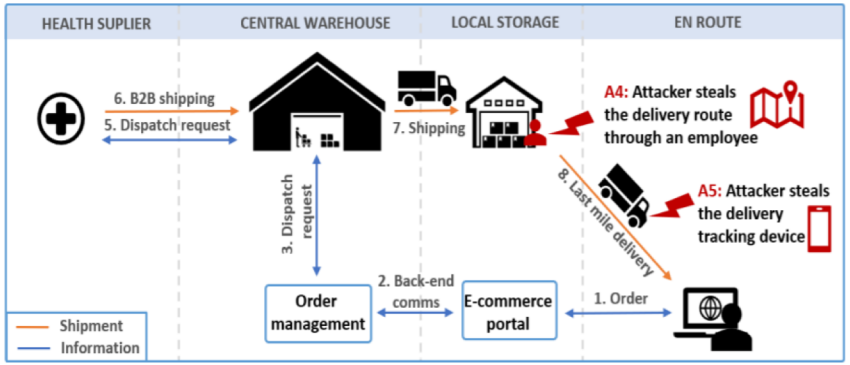
Use Cases e Scenari

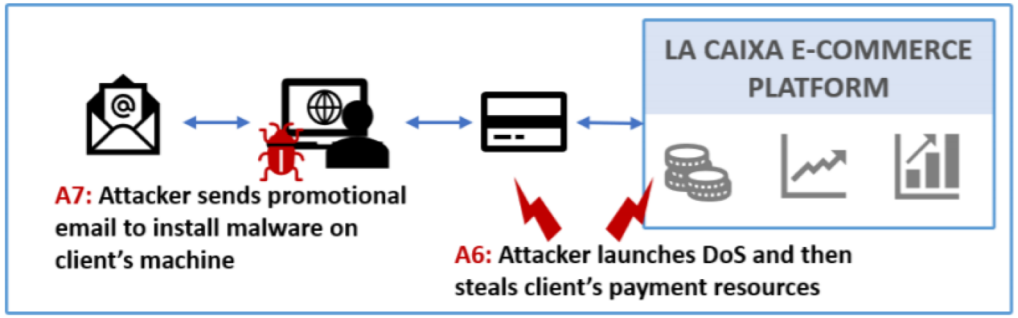
- **Pilot Use Case 1: Cyber-attack a piattaforme e-commerce**
  - Principali utilizzatori– Grande multinazionale del commercio al dettaglio
  - Principali obiettivi – Protezione dati dei clienti

- **Pilot Use Case 2: Physical attack a operatori dell'e-commerce**
  - Principali utilizzatori– Farmacia online, società di logistica, società di trasporto sicuro
  - Principali obiettivi – Protezione della catena di approvvigionamento da attacchi fisici e mitigazione degli effetti a cascata

- **Pilot Use Case 3: Cyber-physical attack a una Banca/PSP per servizi di pagamento online**
  - Principali utilizzatori– Istituzione finanziaria che fornisce servizi di pagamento online all'e-commerce
  - Principali obiettivi– Protezione delle operazioni di pagamento online e mitigazione delle frodi relative ai pagamenti



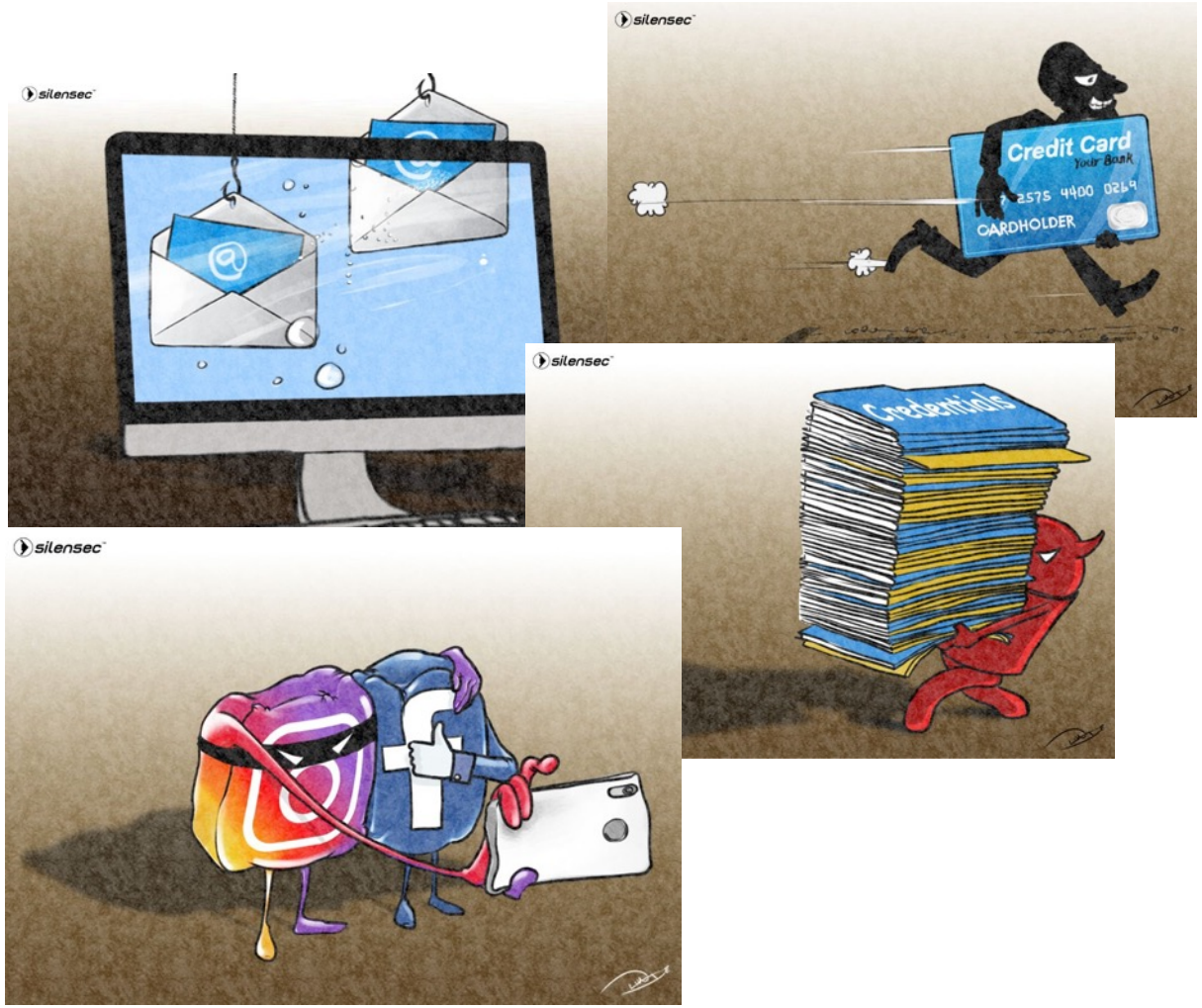




This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883242.

Training e Awareness

- Sviluppo di contenuti e strumenti di formazione e sensibilizzazione alla cybersecurity ad hoc per l'e-commerce
- Sviluppo di oltre 100 illustrazioni per sensibilizzazione alla sicurezza
  - parte della campagna di comunicazione
  - su misura per diversi target di pubblico
- Modelli per simulazioni di attacco
  - Malicious Landing Pages and Websites
  - Sample T&C
  - Social Media Campaigns
  - Sample phishing emails
- Traduzione in 6 lingue europee (English, Greek, Italian, Spanish, Romanian, German)
- 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.

ENSURESEC

Impatto atteso

Impatti attesi di progetto

Breve termine

- State of the art analysis – Identificazione degli **asset più critici** nell'e-commerce, vulnerabilità fisiche e informatiche, scenari di rischio e tecnologie di rilevamento
- User validation – **dimostrazione** delle tecnologie sviluppate e valutazione da parte degli utenti finali e delle parti interessate in merito alla loro accettazione, usabilità, utilità e fiducia

Medio Termine

- Strumenti, concetti e tecnologie innovativi per la protezione dell'e-commerce – Soluzioni innovative per prevenire, rilevare, rispondere e mitigare le minacce fisiche e informatiche, nonché per monitorare l'ambiente e per proteggere e formare gli utenti
- Metodologia di gestione del rischio basata su standard: metodologia per valutare, valutare, prevedere e gestire i rischi combinati per la sicurezza informatica e fisica
- Dissemination – Ampia diffusione dei risultati tra i pertinenti gruppi di utenti e una varietà di parti interessate

Lungo Termine

- Standardisation
  - Promuovere la convergenza degli standard di sicurezza e protezione e favorire la distribuzione dei risultati del progetto tra gli organismi di normalizzazione
  - Contributi a iniziative normative direttamente o indirettamente legate al commercio elettronico

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

Impatti attesi sul mercato

- Ridurre le perdite finanziarie e di posti di lavoro nelle PMI dell'e-commerce:
  - ENSURESEC contribuisce alla crescita del mercato unico digitale proteggendo le aziende di e-commerce (soprattutto le PMI) dai danni economici e dalla perdita di posti di lavoro causati da violazioni della sicurezza, nonché formando i cittadini a essere resilienti e sicuri di se stessi contro tali minacce.
- Promuovere la trasparenza delle operazioni di e-commerce:
  - ENSURESEC promuove la responsabilità sociale attraverso una trasparenza senza precedenti tra le aziende e gli utenti cittadini, fornendo una traccia di controllo completa degli incidenti di sicurezza informatica e fisica.
- Ridurre la paura, lo stress e l'ansia dei cittadini nei confronti delle minacce alla sicurezza dell'e-commerce:
  - ENSURESEC previene l'impatto psicologico e la paura causati dalla percezione di un aumento del rischio per la sicurezza nell'e-commerce. Raggiunge questo obiettivo riducendo il numero di incidenti che si verificano e aumentando la comprensione da parte degli utenti cittadini del rischio preciso e di come proteggersi da esso.
- Promuovere l'uguaglianza nell'uso dell'e-commerce, indipendentemente dal background e dal contesto:
  - ENSURESEC contribuisce all'equità e all'uguaglianza nell'uso dell'e-commerce, dal punto di vista sia dell'azienda che fornisce l'e-commerce che del cittadino che lo utilizza. Raggiunge questo obiettivo adattando la formazione alle esigenze di utenti con background ed esperienza tecnologica diversi e rendendo la sua offerta tecnologica open source e disponibile per le organizzazioni indipendentemente dalle loro capacità finanziarie.

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.