# ITALIAN PROJECT AWARDS
# City-level Cyber-Secure Multimodal Transport Ecosystem (CitySCAPE)

## Esigenza dell'azienda cliente

Il cliente - l'Agenzia Esecutiva Europea per la Ricerca (REA), organismo di finanziamento per la ricerca e l'innovazione che gestisce le sovvenzioni dell'Unione Europea per la ricerca, ha specificato all'interno del bando Digital Security (H2020-SU-DS-2018-2019-2020) del programma Horizon 2020 l'esigenza di affrontare le cyber-minacce interconnesse propagate per garantire e proteggere le aziende di trasporto pubblico locale. L'obiettivo è quindi quello di fornire soluzioni per proteggere le vulnerabilità che potrebbero avere un impatto grave e effetti di propagazione catastrofici sulle operazioni di trasporto multimodale, ovvero che necessitano di più modalità di trasporto combinate tra loro (ad esempio, treno e bus).

CitySCAPE, un progetto cofinanziato dalla Commissione Europea, coordinato dall'Istituto di Comunicazioni e Sistemi Informatici di Atene (ICCS), che vede coinvolto un consorzio di 15 partner, tra cui l'Azienda Mobilità e Trasporti di Genova (AMT) e il Consiglio dei Trasporti della Città di Tallinn, ha indirizzato questa esigenza con l'ambizione di esplorare le diverse dimensioni della sicurezza informatica nel trasporto multimodale, introducendo tecniche innovative di analisi del rischio e orchestrando una serie di soluzioni software da integrare con i sistemi di gestione del trasporto esistenti, quali:

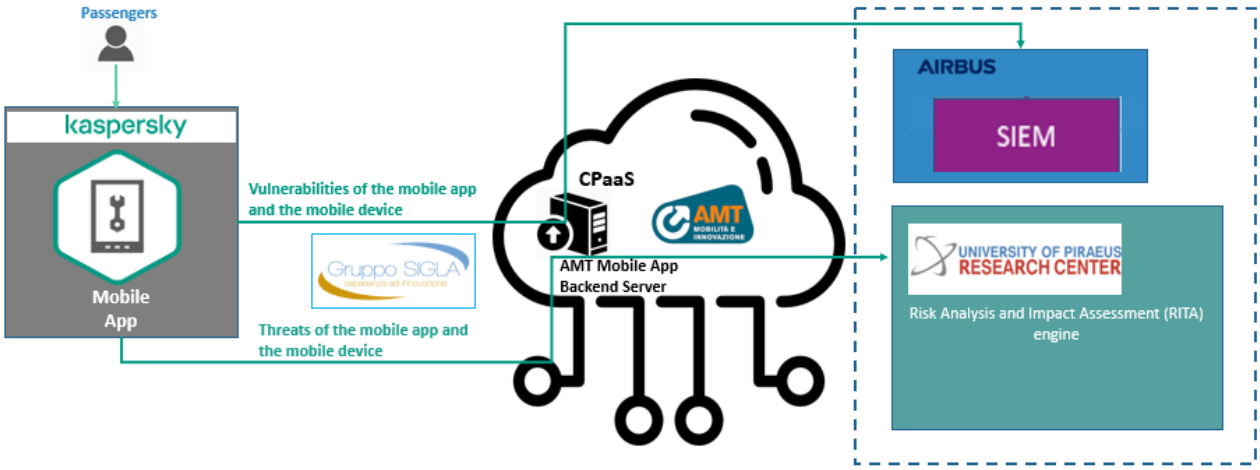
- tecnologie di intelligence sulle minacce per informare costantemente i team incaricati di garantire la sicurezza delle informazioni in una azienda di trasporto sulle minacce in corso e identificare i rischi il prima possibile, con il supporto del Direttorato Nazionale di Cyber Security della Romania (DNSC);
- prodotti di sicurezza per proteggere i dispositivi e la rete dell'Azienda di Trasporto Pubblico e rilevare immediatamente gli attacchi;
- processi per rispondere efficacemente in caso di attacco, comunicando informazioni rilevanti sull'attacco a tutte le parti interessate;
- procedure per ripristinare rapidamente il corretto funzionamento dei sistemi e delle reti dopo un attacco.

## Fasi di sviluppo e realizzazione

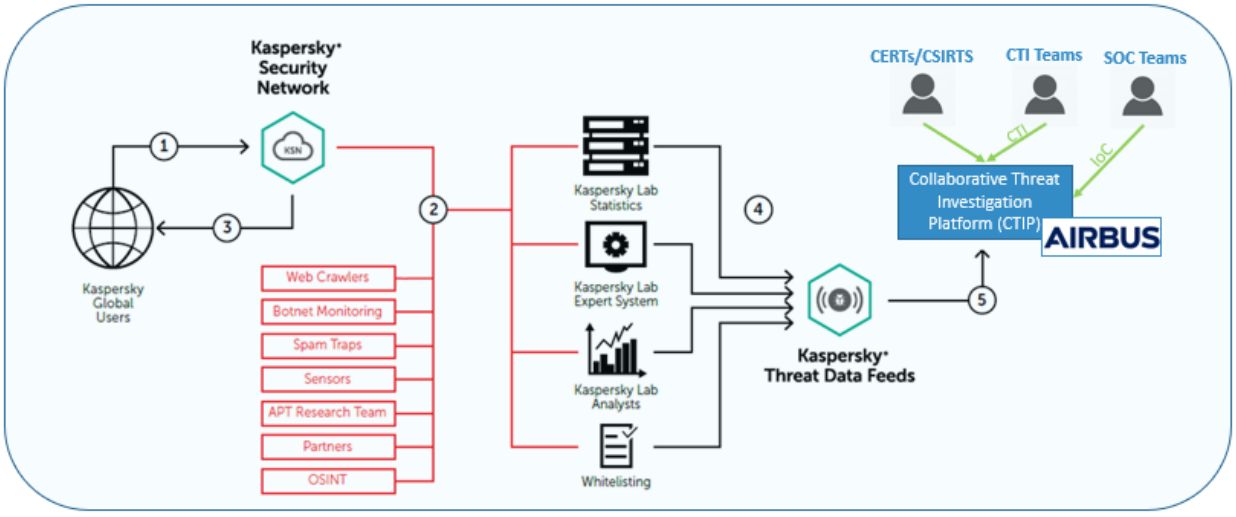
A Genova il progetto si è focalizzato principalmente sulla sicurezza digitale di due scenari relativi ai servizi elettronici forniti agli utenti del trasporto pubblico, quali il sito Web o l'applicazione mobile. Il primo riguarda l'info-mobilità, con l'obiettivo di proteggere e garantire la continuità dei servizi digitali che forniscono informazioni preziose per i passeggeri del trasporto pubblico, quali i tempi di attesa alla fermata del bus o della metro, il programma del servizio di trasporto, le notifiche ai passeggeri sull'aggiornamento del servizio di trasporto. Il secondo scenario è incentrato sulla biglietteria, per difendere da eventuali attacchi a funzionalità critiche quali l'acquisto del biglietto o dell'abbonamento City-Pass dall'app mobile, la convalida di un biglietto elettronico o dell'abbonamento City-Pass, l'uso dello stesso ticket elettronico su un percorso che interessa più mezzi di trasporto (es. sia il bus che il treno urbano).

Le applicazioni mobili utilizzate da passeggeri e controllori, quella ufficiale di AMT e SIGLAMoving, implementata ex-novo per CitySCAPE e che può essere integrata tra le soluzioni di ogni azienda di trasporto, sono state progettate da Gruppo SIGLA seguendo il paradigma 'security-by-design', con l'integrazione del Kaspersky Mobile Security - Software Development Kit (KMS-SDK). La sicurezza è garantita in due modalità:

la prima, orientata alla prevenzione, prevede una valutazione delle vulnerabilità esistenti sui dispositivi mobili dei passeggeri e dei controllori (ad esempio se il dispositivo consente a un utente malintenzionato di assegnare privilegi di amministratore o se il dispositivo è protetto da password); informazioni di dettaglio sulle vulnerabilità individuate sono trasmesse in forma anonima al sistema Security Information and Event Management gestito da AIRBUS, attraverso il quale i responsabili della sicurezza di AMT possono essere informati sulle criticità e possono essere avviate campagne di sensibilizzazione mirate. La seconda modalità, orientata alla rilevazione, consente di individuare minacce sul dispositivo mobile del passeggero, come ad esempio uno spyware che tenta di fiutare dati sensibili dell'utente, quali dati personali o di pagamento o malware in grado di manipolare dati relativi ad orari, percorsi e tempi di attesa; queste informazioni saranno inviate al sistema di analisi del rischio e di valutazione dell'impatto, realizzato dal Centro di Ricerca dell'Università del Pireo, per consentire alle aziende di trasporto pubblico di valutare gli investimenti in cybersecurity a cui dare priorità per complicare la vita ai criminali e fare in modo che il costo di un attacco informatico superi il vantaggio che un utente malintenzionato può trarne.




Un ulteriore aspetto tecnico importante è legato alla Threat Intelligence: CitySCAPE incapsula i Kaspersky Threat Data Feeds all'interno della Piattaforma di Threat Intelligence impostata sulla Collaborazione (CTIP), gestita da AIRBUS, per garantire che i responsabili della sicurezza IT delle aziende di trasporto pubblico siano continuamente aggiornati con informazioni di alta qualità, da utilizzare anche per le attività di monitoraggio quotidiane e per la gestione della fase di risposta agli incidenti.



CitySCAPE tiene in gran considerazione l'importanza del fattore umano. Una minaccia al sistema informatico di un'azienda di trasporto pubblico può essere innescata dall'errore di una persona, tramite l'installazione di un'applicazione dannosa, un clic su un collegamento di phishing o una password troppo debole. Sono fondamentali dunque gli strumenti formativi realizzati per coinvolgere quante più persone possibili tra gli utenti che interagiscono con i servizi digitali di un'azienda di trasporto pubblico, per aumentare il loro livello di competenza in materia di sicurezza dei dati e privacy. Kaspersky fornisce contenuti educativi innovativi basati sul gioco a tutti gli utenti del trasporto pubblico che hanno competenze di sicurezza informatica scarse o assenti, compresi i passeggeri. Attraverso il gioco, ad esempio, stiamo insegnando l'importanza di impostare una password sufficientemente complessa e da non condividere con nessuno, come riconoscere minacce molto comuni come Ransomware e Phishing e come minimizzare i rischi generati, sia per i dispositivi degli utenti che per i sistemi dell'azienda di trasporto pubblico, individuare le minacce nascoste dietro l'uso dei dispositivi mobili e dei social network, senza mai trascurare l'importanza della privacy: stiamo aiutando gli utenti finali a capire quali tra i loro dati hanno valore e sono di interesse per i criminali informatici, mostrando loro come gestire le informazioni riservate e quali sono i diritti e doveri derivanti dal GDPR.


## Risultati e qualche numero

Durante la fase pilota di Genova le nuove versioni sicure delle app mobile di AMT sono state testate da controllori e passeggeri, sotto la supervisione degli esperti di sicurezza di AMT. Gli strumenti di analisi del rischio e di threat intelligence sono stati installati all'interno del CED di AMT e utilizzati dai dipendenti del team di sicurezza.

A settembre 2022, due trainer del Gruppo Sigla certificati da Kaspersky hanno condotto 14 sessioni educative basate sul gioco per 214 dipendenti AMT non esperti in tecnologia e sicurezza digitale, che si sono dimostrati entusiasti e interessati durante la formazione, che hanno trovato utile ed efficace. Negli ultimi mesi dell'anno il focus si è spostato sui passeggeri, per i quali sono in corso a Genova campagne di sensibilizzazione su temi come malware, phishing, GDPR e gestione dei dati personali, sfruttando le potenzialità di una nuova versione del Kaspersky Gamified Assessment Tool (GAT) accessibile da dispositivo mobile, che consente ai passeggeri di misurare le proprie competenze su queste tematiche durante tempi di attesa in stazione o durante gli spostamenti casa-lavoro. Il gioco è stato testato dagli studenti delle scuole superiori, quali l'istituto Italo Calvino di Genova, che a bordo dei mezzi AMT hanno scoperto quali attacchi informatici potrebbero verificarsi in determinate situazioni e come dovrebbero comportarsi di fronte a possibili rischi.