



## Validazioni in simulazione

Le validazioni in ambiente di simulazione di SATIE si sono svolte tra venerdì 23 aprile e mercoledì 28 aprile 2021 in un evento da remoto. Scopo dell'evento era validare e verificare il Toolkit SATIE sulla piattaforma di simulazione, utilizzando cinque scenari di minaccia ibrida cyber-fisica. Questi scenari di minaccia sono stati messi a punto per essere al tempo stesso fattibili ma realistici e complessi quanto basta per includere le minacce, sia di natura fisica che informatica, che possono impattare le infrastrutture critiche, in particolar modo gli aeroporti. Simili attacchi possono essere eseguiti da un aggressore per causare gravi danni sia alle operazioni aeroportuali che alla vita umana. Negli scenari di validazione i complessi attacchi sviluppati hanno lo scopo di essere eseguibili sulla base dei sistemi aeroportuali coinvolti e di eventuali vincoli tecnici ed operativi legati agli ambienti di produzione. Pertanto, la configurazione degli attacchi è stata analizzata ed aggiornata durante tutto il progetto prima che potesse aver luogo la validazione. Infine, gli scenari di minaccia cyber-fisica sono stati personalizzati per simulare tali attacchi negli aeroporti mentre gli operatori aeroportuali hanno utilizzato il Toolkit SATIE per verificare quanto sia in grado di rispondere alle proprie esigenze e aspettative di sicurezza.

All'evento hanno partecipato 15 professionisti aeroportuali – con comprovata esperienza nel Security Operation Center (SOC), Airport Operation Center (AOC) e come agenti di polizia – provenienti da tre aeroporti europei (Atene, Zagabria e Milano). Nelle simulazioni Human-in-the-Loop (HITL), i partecipanti si sono confrontati con gli scenari di minaccia, durante i quali hanno dovuto utilizzare il Toolkit SATIE per contrastare gli attacchi. Agli operatori è stato chiesto di utilizzare il Toolkit SATIE proprio come un comune sistema di sicurezza aeroportuale per comprendere quali attacchi si stanno verificando, quali risorse sono interessate e per mettere in pratica l'avvio delle necessarie procedure di mitigazione, nonché per informare i primi soccorritori.

Wyświetlanie ekranu urządze...

## Feedback and Impressions

1. What is your general impression of the SATIE solution and the simulation itself?
2. What are your additional remarks not covered by the questionnaires?
3. What are the SATIE Solution benefits compared to your current operations?

28/04/2021 6 SATIE

L'evento è stato preceduto da sessioni di formazione per fornire agli operatori aeroportuali adeguati materiali didattici ed insegnamenti su come utilizzare il Toolkit SATIE. Tutto questo è stato realizzato attraverso corsi di formazione a distanza di un'intera giornata con gli sviluppatori del tool. Nel tempo che ha preceduto la conduzione delle validazioni di simulazione, gli operatori della sicurezza hanno avuto accesso gratuito alla piattaforma di simulazione attraverso un portale web di facile utilizzo. Ciò ha permesso loro di esercitarsi nell'uso del Toolkit SATIE e di acquisire dimestichezza con le sue principali funzionalità prima di procedere alla validazione.

Durante il processo di validazione, il Toolkit SATIE è stato convalidato secondo criteri di accettazione, usabilità, utilità e fiducia per soddisfare le esigenze degli operatori aeroportuali della sicurezza, sia fisica che informatica. L'attività è stata supportata da un esaustivo questionario, cui è seguita un'analisi preliminare del feedback degli esperti in cui si è evidenziata una reazione molto positiva al Toolkit SATIE e ai suoi singoli componenti, tutti classificati come adeguati allo scopo. Il Toolkit SATIE è stato percepito come un miglioramento significativo rispetto ai sistemi attualmente in uso, consentendo un rilevamento ed una risposta più rapidi alle minacce sia fisiche che informatiche. Gli operatori hanno inoltre ritenuto che gli avvisi cyber-fisici generati dal motore di correlazione siano di notevole valore aggiunto e altamente rilevanti per affrontare situazioni di emergenza. Allo stesso tempo, sono state evidenziate aree di miglioramento, ad iniziare da una maggiore integrazione con i sistemi aeroportuali esistenti. Inoltre, ulteriori analisi sui dati delle prestazioni sono in corso di realizzazione per calcolare valori oggettivi per il rilevamento ed i tempi di reazione.

Le validazioni della simulazione di SATIE sono state un passo importante verso le dimostrazioni finali che si svolgeranno negli ambienti aeroportuali. Il feedback raccolto da questi processi di validazione verrà utilizzato per perfezionare ulteriormente il Toolkit SATIE per le prossime dimostrazioni nei tre aeroporti e che verranno svolte in ambienti quasi reali.

*Disclaimer: Questo progetto ha ricevuto finanziamenti dal programma di ricerca e innovazione Horizon 2020 dell'Unione europea ai sensi della convenzione di sovvenzione n. 832969. Questo prodotto riflette il solo punto di vista degli autori e l'Unione europea non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto le informazioni in esso contenute.*

### **Il progetto SATIE**

Il Progetto SATIE H2020 adotta un approccio olistico alla prevenzione, rilevamento, risposta e mitigazione delle minacce negli aeroporti, garantendo al contempo la protezione dei sistemi critici, dei dati sensibili e dei passeggeri. Le infrastrutture critiche, di cui gli aeroporti fanno parte, sono solitamente protette contro singole minacce fisiche o informatiche, ma non contro scenari complessi che combinano entrambe le categorie di minacce. Per gestirle, SATIE sviluppa un toolkit interoperabile che migliora le correlazioni cyber-fisiche, le indagini forensi e la valutazione dell'impatto dinamico negli aeroporti. Avendo una consapevolezza situazionale condivisa, gli esperti della sicurezza e i gestori aeroportuali collaborano in modo più efficiente alla risoluzione delle crisi. Le procedure di emergenza possono essere attivate contemporaneamente attraverso un sistema di allerta al fine di riprogrammare le operazioni airside/landside, informare i primi soccorritori, i team di sicurezza informatica e di manutenzione per un recupero rapido.

Soluzioni innovative sono integrate su una piattaforma di simulazione, che replica parti fondamentali dei sistemi cyber-fisici negli aeroporti al fine di migliorarne l'interoperabilità con il sistema esistente e di convalidarne l'efficienza. Saranno effettuate tre dimostrazioni in diversi aeroporti d'Europa (Zagabria, Milano e Atene) per valutare le soluzioni in condizioni operative. I risultati e le best practice saranno ampiamente divulgate alla comunità scientifica, agli organismi di standardizzazione, agli stakeholder della sicurezza e alla comunità aeronautica. Infine, SATIE apre la strada a una nuova generazione di Security Operation Center (SOC) che saranno inclusi in una policy di sicurezza aeroportuale completa.