Cyber range per industrial security

PROGETTO DI RICERCA

L'obiettivo principale del progetto è la realizzazione di un Cyber Range per reti industriali implementato in ambiente virtuale (cloud), unitamente ad una metodologia ed a tutti i componenti software necessari per dispiegarlo in modo semplice co-localizzato con gli utilizzatori finali.
La creazione del Cyber Range prevede il raggiungimento di una serie di risultati, tra cui:
1. Verifica della postura di sicurezza di impianti e macchinari connessi: le imprese potranno avvalersi del Cyber Range per individuare problemi di sicurezza legati a errori di configurazione e vulnerabilità note, il tutto in un ambiente virtuale per non compromettere le attività di produzione
2. Ambiente avanzato di formazione del personale: la piattaforma fornirà esempi di attacco e strategie di difesa predisposti, da usare sia per formare dipendenti e studenti per diversi gradi di specializzazione, sia per validare le capacità di team già formati, creando quindi le migliori condizioni per colmare il divario attualmente presente fra domanda e offerta di specialisti di sicurezza.
3. Monitoraggio in tempo reale delle prestazioni di un sistema, con la possibilità di effettuare manutenzione preventiva per evitare incident di sicurezza.
4. Riduzione dei costi di produzione e manutenzione di un sistema grazie all'identificazione preventiva di falle di sicurezza in fase di progettazione, evitando costi di riparazione successivi.

PIANO DELLE ATTIVITÀ

I. definire l'architettura generale del Cyber Range, con riferimento ad altre esperienze similari già sviluppate a livello Europeo o nazionale, per scopi di carattere generico e non focalizzati nello specifico sull'applicazione alle reti industriali. Verranno confrontati I metodi di orchestrazione dell'infrastruttura utilizzati e le possibili tecnologie di virtualizzazione (Virtual machine, container, etc.).
II. sviluppare il prototipo di Cyber Range unitamente alle API che verranno messe a disposizione degli utenti finali per la sua implementazione e per la predisposizione dei casi d'uso. Per il dispiegamento del Cyber Range si utilizzeranno metodologie ispirate agli standard dell'NFV-MANO, che permettono, tramite descrittori standardizzati, di descrivere in dettaglio le caratteristiche dell'infrastruttura di rete e dei componenti computazionali coinvolti.
III. simulazione di tipologie di attacco che verranno definite anche in base all'analisi di vulnerabilità effettuata al punto I tramite l'uso di IDS. Si prevede una prima fase di modellazione dei setup per i casi d'uso reali sul prototipo di architettura, in collaborazione con le aziende partner per accertarsi che il Digital Twin possa rappresentare fedelmente i sistemi d'interesse. Si passerà poi a una seconda fase di test basata su quanto definito al punto I