NIER

Safeguard-PLC: Cybersecurity in Automazione Industriale (SCAI)

SCAI (Safeguard-PLC: Cybersecurity in Automazione Industriale) è un sistema di diagnostica avanzato con lo scopo di proteggere le reti di PLC da attacchi informatici.
Esso permette di:
• Rilevare in modo accurato e tempestivo eventi critici riconducibili ad un'intrusione attraverso le funzioni di Monitoraggio e Registrazione del traffico di rete;
• Generare ALERT e ALLARMI (parametrizzabili e configurabili) sulla base degli eventi rilevati;
• Monitorare KPI ed Asset aziendali attraverso una dashboard di monitoraggio (MOD – MOnitoring Dashboard) semplice e intuitiva, garantendo la compliance alle normative NIS 2 (Direttiva UE 2022/2555) e Cyber Resilience Act (CRA – Direttiva UE 2024/2847).
In particolare, è sviluppato in moduli indipendenti, ciascuno dei quali assolve ad una funzione specifica, ma che al tempo stesso possono interagire tra di loro. Questo consente:
• una maggiore manutenibilità del software
• di integrare nuove funzionalità sulla base delle specifiche esigenze aziendali

Laboratorio	NIERING
Area di specializzazione	Digitale
Referenti	silvia prodi
Keyword	Cybersecurity, OT, PLC, Compliance NIS2, IEC 62443 e CRA

"SCAI: lo scudo digitale per i sistemi OT"



Fig. 1: Logo SCAI

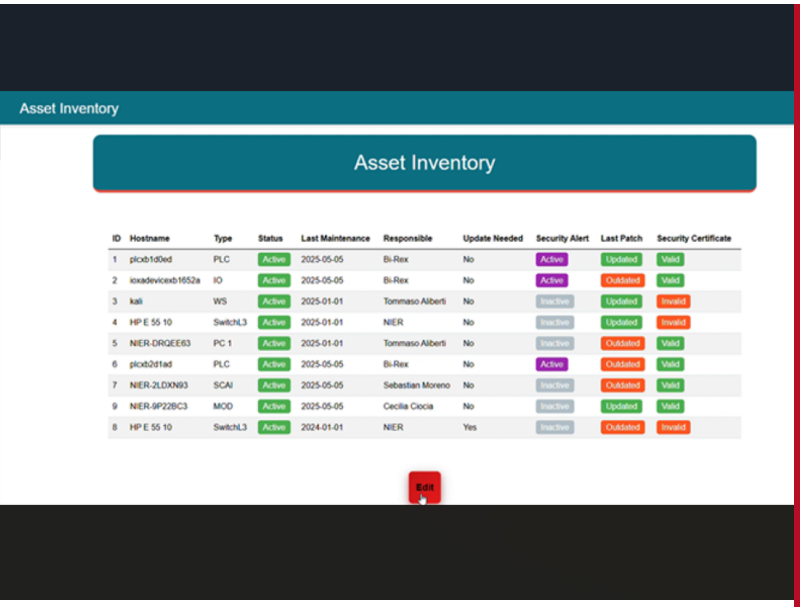


Fig. 2: SCAI – Sezione "Asset Inventory" della dashboard MOD

Descrizione

SCAI è una soluzione software che si rivolge a tutte le realtà industriali che intendono proteggere i loro sistemi OT da minacce informatiche e rispettare le normative NIS 2 e CRA.
È pensato per essere un gateway tra la rete INTERNA, cioè la rete OT (dove ci sono i PLC e i moduli I/O), e la rete ESTERNA, che per semplicità può essere definita come tutto ciò che non è OT: stando "nel mezzo", SCAI può controllare in real-time il traffico tra le due reti in modo da rilevare anomalie. Gli elementi principali sono:

• Back-end, che consente di:

1. Registrare i dati, sia quelli nella rete esterna, sia quelli nella rete interna
2. Salvare i dati in un database dedicato
3. Generare log di sistema, alert e allarmi

• Front-end (MOD), che fornisce una user-experience semplice ed intuitiva, consentendo l'accesso alle diverse sezioni dell'applicazione web in pochi click. In particolare, attraverso MOD, un operatore OT può:

1. Gestire gli allarmi generati dal back-end mediante le operazioni di lettura, presa in carico e risoluzione del problema sollevato dall'allarme stesso
2. Monitorare i KPI aziendali, sia in condizioni nominali della linea industriale sia in condizioni critiche (attacco in corso)
3. Monitorare gli Asset della linea produttiva attraverso la funzionalità "Asset Inventory": tale funzionalità permette di individuare gli asset critici di tutta la linea produttiva grazie alla gestione automatica degli aggiornamenti di sicurezza

Aspetti innovativi

Conformità normativa
SCAI integra nativamente i requisiti NIS 2, IEC 62443 e il Cyber Resilience Act nel modello di gestione del rischio, offrendo mappature automatiche tra eventi, asset e controlli richiesti. Così si ottiene visibilità completa e misurabile sui dispositivi industriali e si può dimostrare la conformità in modo trasparente.

Detection realmente proattiva
SCAI sfrutta un motore progettato per i protocolli industriali, capace di intercettare indicatori di compromissione OT che strumenti IT o ibridi non vedono. Questo permette di anticipare guasti, attacchi e comportamenti anomali a livello di PLC, I/O e comunicazioni. Il risultato è la riduzione dei tempi di inattività e una maggior capacità di risposta.

Modularità per l'integrazione OT
SCAI ha un'architettura basata su moduli indipendenti che consente un'integrazione a basso impatto anche in impianti critici o legacy. Inoltre, ogni componente comunica tramite API standardizzate, facilitando connessioni dirette e senza frizioni con SIEM, XDR e sistemi di monitoraggio avanzati. Questo permette di estendere la cybersecurity OT nel perimetro IT esistente senza sostituire strumenti già presenti.

Applicazioni

SCAI è una soluzione software modulare e scalabile per la protezione delle linee di produzione industriale contro le minacce informatiche. È compatibile con qualsiasi architettura OT e può essere implementata come gateway di sicurezza tra domini di rete diversi, ad esempio tra IT e DMZ, abilitando un modello di difesa multilivello. Inoltre, SCAI supporta le organizzazioni nel percorso di conformità alla Direttiva NIS2, IEC 62443 e al Cyber Resilience Act, fornendo funzionalità di monitoraggio, controllo e governance che semplificano l'adozione di misure di cybersecurity adeguate e dimostrabili.

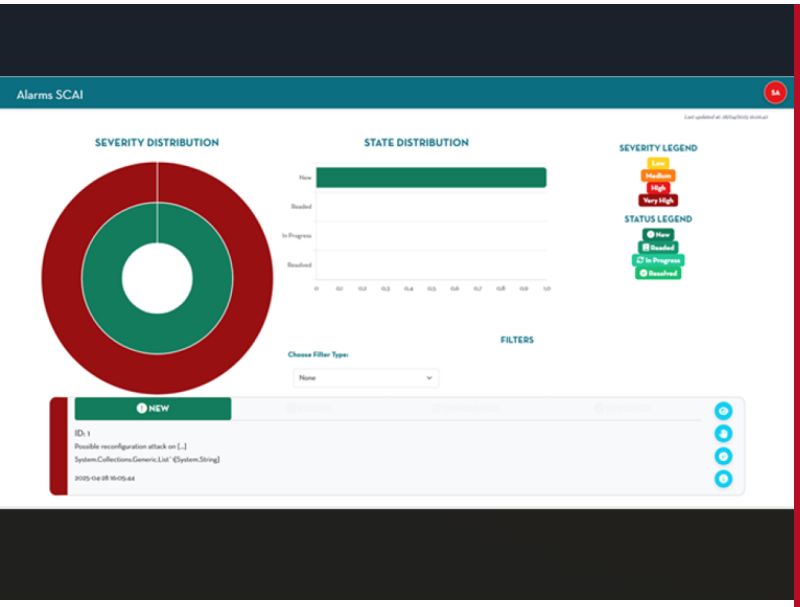


Fig. 3: SCAI – Detection attacco di "Reconfiguration": allarme visibile sulla dashboard MOD

Partner coinvolti	Bi-Rex (Big Data Innovation & Research Excellence)
Tempi di realizzazione	1 mese/uomo
Livello di maturità tecnologica	TRL 6 - tecnologia dimostrata in ambiente rilevante
Valorizzazione applicazione	È in corso una ricerca di partner aziendali per ulteriori applicazioni.

Esempio di applicazione

Simulazione e detection di cyber-attacchi in una rete OT semplice mediante SCAI.

In una rete OT semplice, costituita da un solo PLC ed un unico Modulo I/O, sono stati simulati tre attacchi cyber:

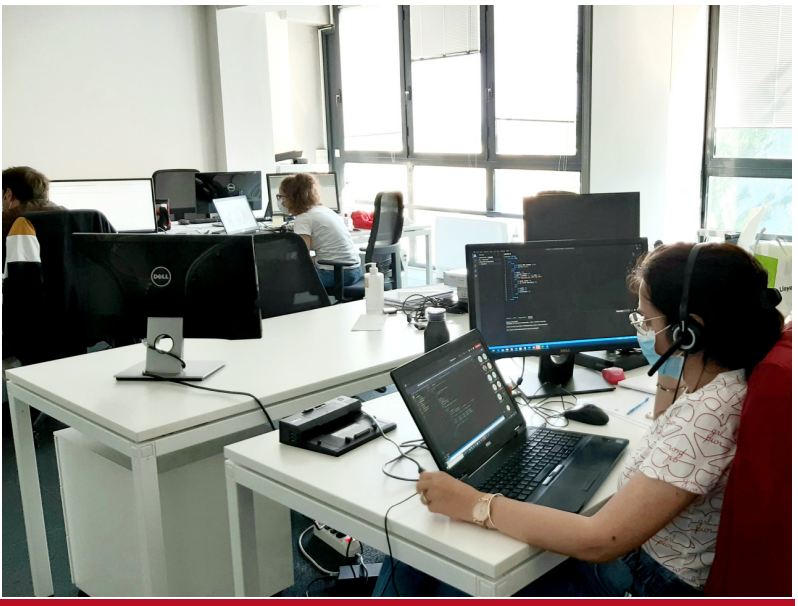
- **Flood di rete**: bombardamento della rete tramite l'iniezione di un volume elevato di pacchetti, tipicamente generato da una botnet (esempio: malware BlackEnergy)
- **Reconfiguation attack**: modifica non autorizzata delle configurazioni dei PLC per causare malfunzionamenti o disservizi (esempio: malware Stuxnet)
- **Disconnessione fisica**: interruzione volontaria o accidentale dei cavi del PLC e/o del Modulo I/O (azione umana volontaria o involontaria)

Tali attacchi hanno tutti lo stesso fine, ovvero interrompere la comunicazione PLC-Modulo I/O, e la loro scelta è dovuta al fatto che sono pericoli reali ed attuali per le linee di produzione industriale.
Gli attacchi sono stati correttamente diagnosticati da SCAI e gli operatori sono stati tempestivamente avvisati tramite gli **Alert** e gli **Alarm** visibili su MOD, riducendo drasticamente i tempi di inattività della linea. Inoltre, il monitoraggio dei **Key Performance Indicator** della linea produttiva si è dimostrato uno strumento efficace di **Incident Analysis**, consentendo di valutare il comportamento della rete interna nella finestra temporale in cui l'attacco è stato eseguito.

NIER

NIERING

NIER Ingegneria Spa



NIER, laboratorio della Rete Alta Tecnologia, è una società di consulenza di servizi tecnico scientifici con competenze specifiche in: analisi di affidabilità e sicurezza, in particolare nei contesti che richiedono elevati standard e sono soggetti a normative e procedure specifiche.
Con circa 180 collaboratori (di cui oltre il 15% con un dottorato di ricerca), ha sede principale a Bologna e coinvolge principalmente laureati in ingegneria. Gli ambiti in cui NIER opera con queste metodologie sono primariamente l'ambito trasporti e biomedico.
Le competenze di NIER sono interdisciplinari e coinvolgono ingegneri e ricercatori elettronici, meccanici, energetici ed informatici.
Il contesto particolarmente mutevole, la crescente complessità dei sistemi e la presenza imponente di tecnologie e software, specialmente in contesti safety- critical, fanno di questa disciplina una materia in evoluzione che richiede in modo importante attività di ricerca e innovazione.
NIER è particolarmente attiva su temi quali la sostenibilità ambientale, la salute e sicurezza sul lavoro, l'analisi di rischio e la modellazione multi-fisica di sistemi complessi. Recentemente, anche per far fronte al crescente contesto data-driven, NIER Ingegneria ha iniziato un progetto interno di sviluppo di soluzioni basate su tecniche di machine learning e data analysis.

Sito web http://www.niering.it

Data pubblicazione 14/01/2026