

SUCCESS STORY

Quando la scrittura sul PLC arriva senza change request

OT Threat Score e ripristino guidato: processo e security correlati in un perimetro NIS2.



Settore:
Manifattura in perimetro NIS2



Perimetro:
PLC, SCADA e sensori di linea + firewall, endpoint, accessi remoti



Soluzione:
OT Resilience
OT Threat Score
Runbook di ripristino



01

CONTESTO

**Il SOC vede i log, la fabbrica vede le derive.
Nessuno vede l'insieme**

Manifattura dentro il perimetro NIS2: obblighi di gestione degli incidenti, di risposta e di evidenza documentale, non solo di rilevazione. La superficie d'attacco cresce con la convergenza IT/OT, ma i due mondi restano organizzativamente separati.

Il SOC vede firewall, endpoint, CVE. La fabbrica vede drift di setpoint, tempi ciclo che oscillano, scritture sui PLC. Senza correlazione, gli alert si moltiplicano, i falsi positivi saturano il team e il legame tra evento cyber e impatto su qualità, energia e OEE resta opaco: il SOC non sa quale allarme ferma la produzione.

02

SFIDE DA RISOLVERE

**NIS2 chiede risposta e ripristino,
non un altro rilevatore**



Ogni alert è uguale a tutti gli altri

Senza contesto di processo, un tentativo di accesso e una scrittura anomala su un PLC di linea critica hanno lo stesso peso in coda al SOC. La priorità la decide l'ordine di arrivo, non l'impatto.



I falsi positivi consumano il team

Gli strumenti di detection puri generano volume. Ogni segnalazione da verificare a mano contro lo stato reale dell'impianto costa ore, e insegna al team a ignorare le campane.



La detection senza ripristino lascia a metà

Trovare l'anomalia non rimette in produzione la linea. Serve la sequenza dopo: isolare, verificare la logica contro una baseline affidabile, tornare ai parametri buoni con tracciamento. NIS2 chiede esattamente questo ciclo.



L'audit vuole numeri, non assicurazioni

Tempi di rilevazione e ripristino, copertura degli asset, gestione degli incidenti: la conformità si dimostra con KPI misurati e report periodici, non con l'elenco delle tecnologie installate.

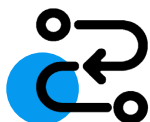
03

SOLUZIONE

Un gemello informativo, uno score, un runbook

Integrato al data lake aziendale, il modulo trasforma i dati di consumo sul campo in emissioni Scope 1 e Scope 2 (Location e Market-Based) tramite fattori ufficiali aggiornati.

Garantisce massima auditabilità distinguendo le stime ML dai dati reali, produce report nativamente conformi ai principali standard (GHG Protocol, ISO 14064, GRI, ESRS E1) e integra un motore what-if per simulare impatto e ritorno degli interventi di decarbonizzazione futuri.



1 · Processo e security nello stesso data model

Parametri macchina e PLC (setpoint, trend, drift) ed eventi di sicurezza (rete, endpoint, accessi remoti) confluiscono nello stesso schema Asset-Event-Metric, dall'Edge Gateway al Data Lake.

La correlazione smette di essere un lavoro manuale tra due console.



2 · OT Threat Score 0-100

Sei fattori pesati: criticità dell'asset, novità e confidenza dell'anomalia, evidenze dai sistemi di sicurezza, exploitability (CVE, esposizione di rete), impatto operativo misurato (scarti, kWh per pezzo, OEE), persistenza del fenomeno.

Soglie operative: 0-39 Info, 40-59 Warning, 60-79 High, 80-100 Critical.

L'alert arriva al SOC con l'impatto operativo stimato, non solo con il log.



3 · Runbook Purdue-compliant fino al rollback

Dall'isolamento della minaccia al ripristino controllato dei parametri sulla baseline golden, con evidence bundle (log, timeline, grafici, contesto operativo) inviato a SIEM e SOAR e tracciamento completo delle azioni.



4 · Dal risk assessment al pilota in settimane

OT Assessment in quattro passi (analisi di rischio di alto livello, vulnerabilità di dettaglio, raccolta dati sul traffico OT, report con quick win a 90 e 180 giorni), poi pilota su un plant da 30-50 asset in 6-10 settimane.

A regime: report mensili con MTDD, MTTA, MTTR, tasso di falsi positivi, copertura asset e percentuale di incidenti correlati processo-security, con SLO rivisti mese per mese.

04 RISULTATI

Due scenari, due score,
due risposte guidate

Scenario Critico (score sopra 80): scrittura sul PLC senza change request

La linea oscilla nei tempi ciclo mentre risulta attività remota non prevista su una workstation e un tentativo di scrittura verso il PLC senza change request.

Lo score sale su drift ad alta confidenza, evidenze di programmazione PLC e sessione remota fuori finestra manutentiva, criticità elevata dell'asset.

Risposta guidata: blocco dell'accesso remoto e isolamento della postazione, PLC in RUN senza forzature, diff della logica contro la baseline golden, rollback controllato e prove funzionali.

Ticket con priorità da score, evidenze al SOC per chiudere il ciclo.

Scenario Alto (score 60-79): scarti in salita e un dispositivo non gestito in rete di cella

Aumentano scarti e kWh per pezzo, i motori mostrano drift di velocità.

In parallelo compare in rete di cella un dispositivo non gestito che genera sonde ICS.

Lo score incrocia gli impatti misurati su qualità ed energia con l'anomalia di rete.

Risposta guidata: quarantena della porta e rimozione del dispositivo, micro-segmentazione, verifica delle ricette e controllo dei set point contro baseline, hardening della cella e aggiornamento dell'inventario, con monitoraggio del rientro dei KPI.

Per l'audit NIS2: il ciclo intero, documentato

Rilevazione con priorità motivata, risposta tracciata, ripristino su baseline, report mensili con MTDD, MTTA, MTTR e copertura asset. È la differenza tra dichiarare di avere una difesa OT e poter esibire come funziona, incidente per incidente.

Disclaimer

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

Elipsis S.r.L.

P.IVA: 04150950360

PEC: elipsis@pec.it

SDI: SZLUBAI

Sede Legale: V.le Vittorio Veneto 221, 41058 Vignola (MO)

