



Security Summit OT

Milano 24 settembre 2026



Dalla visibilità alla resilienza: il percorso di Edison Next per la sicurezza OT

Vito Calzo, Forescout | Systems Engineer
Gaspere Ceselli, Edison | Cyber Security Architect

SECURITY SUMMIT CLUSIT — MILANO, 24 SETTEMBRE

Dalla visibilità alla resilienza

Il percorso di Edison Next per la sicurezza OT

Sfide reali in ambiente OT e risposte concrete con Forescout

Conoscere • Rilevare • Prioritizzare • Reagire.

Relatori:

*Edison - **Gaspare Ceselli** – Cyber Security Architect*

*Forescout - **Vito Calzo** – Systems Engineer*

Un ambiente che non può fermarsi

<2

finestre di change
programmate all'anno

35+

di sonde Forescout OT
sugli impianti

24/7

monitoraggio affidato
al CERT (servizio gestito)

1/mese

SAL di revisione
con la sicurezza Edison
Next

- Centrali termiche ex Fenice a servizio di grandi stabilimenti industriali (es. Mirafiori, Cassina).
- Continuità di esercizio prioritaria: fuori dalle finestre di manutenzione non si interviene, salvo incidenti.
- Fornitura e implementazione tramite partner di progetto; gestione operativa quotidiana in capo al CERT.

Non si protegge ciò che non si conosce

LA SFIDA

- Inventario degli asset OT parziale e raccolto manualmente sugli impianti.
- Ruolo dei dispositivi nel processo e flussi di comunicazione poco tracciati.
- Interventi invasivi non praticabili su sistemi in esercizio continuo.

LA RISPOSTA CON FORESCOUT

- Sonde in ascolto passivo su SPAN port: nessun impatto sul processo produttivo.
- Inventario continuo con identificazione di dispositivo, ruolo e comunicazioni.
- Console condivisa tra Edison Next e il team CERT come base comune di lavoro.

Esito: una fotografia veritiera e aggiornata dell'ambiente OT, senza toccare gli impianti.

Reagire senza introdurre rischio operativo

LA SFIDA

- Fuori dalle due finestre annuali di change ogni intervento va valutato sull'impatto d'impianto.
- Rilevare tardi un'anomalia significa spostarla alla finestra successiva.
- Necessità di distinguere subito cosa è realmente un incidente.

LA RISPOSTA CON FORESCOUT

- Rilevazione continua delle anomalie e notifica al CERT, che apre e gestisce i ticket.
- Contesto sull'asset coinvolto per valutare l'impatto prima di qualsiasi azione.
- Soluzione complementare all'endpoint protection già presente sugli impianti.

Esito: riconoscere prima e meglio, decidendo l'intervento con cognizione dell'impatto operativo.

In OT non tutte le vulnerabilità pesano uguale

LA SFIDA

- Criticità operativa dell'asset determina la reale priorità dell'intervento.
- Evidenze a supporto per NIS 2 raccolte a mano, impianto per impianto.
- Piano di remediation da negoziare con i fornitori OT dei singoli sistemi.

LA RISPOSTA CON FORESCOUT

- Risk scoring basato sulla criticità del dispositivo e sul suo contesto di rete.
- Dati estratti dalla console e riutilizzati come evidenze per NIS 2.
- SAL mensile: dai rilevamenti al piano di aggiornamento con i fornitori.

Esito: priorità guidate dalla criticità operativa ed evidenze di compliance sempre disponibili.

Prima e dopo: dove va l'effort

PRIMA

3 FTE

consulenti in campo per raccogliere le informazioni sugli impianti

OGGI

1 FTE

team di servizio che opera quotidianamente sulla console Forescout

- La raccolta annuale delle evidenze richiedeva circa tre mesi di lavoro: oggi il dato è già nella console.
- Il valore non è solo tecnologico: nasce da un team che usa la soluzione ogni giorno e la mantiene viva.
- Piani di sviluppo (integrazioni via API, CMDB, flussi verso il team GRC)