ServiTecno

WHITE PAPER

Come migliorare la sicurezza e la continuità operativa:

il caso Fidia Farmaceutici

Abstract

La piattaforma Claroty xDome, distribuita e supportata in Italia da un ecosistema di partner, tra cui ServiTecno, offre una **visibilità completa e un monitoraggio costante degli asset, migliorando la gestione dei rischi e la resilienza dei processi industriali**. L'esperienza di **Fidia Farmaceutici** dimostra l'efficacia di questo approccio, che ha permesso di trasformare la **cybersecurity da voce di costo a fattore strategico** in grado di migliorare l'efficienza e supportare la conformità alle normative. Focus sull'**anomaly detection**, una tecnologia fondamentale per migliorare la sicurezza e la continuità operativa delle imprese, grazie alla sua capacità di identificare comportamenti anomali sfruttando tecnologie avanzate come il machine learning e la deep packet inspection.

Indice

Introduzione

In Italia il Piano Industria 4.0, poi Transizione 4.0, ha dato una forte spinta alla digitalizzazione del settore industriale. Le aziende italiane hanno investito, tra il 2020 e il 2022, quasi **23 miliardi di euro in tecnologie avanzate**, secondo le rilevazioni di Banca d'Italia e del Ministero delle Imprese e del Made in Italy. È la risposta italiana a un trend globale: **produrre in modo più intelligente, interconnesso e sostenibile**.

La rapida transizione al digitale e la richiesta, da parte della normativa, di interconnettere i macchinari per accedere agli incentivi hanno però comportato una **crescente integrazione tra information technology (IT) e operational technology (OT)**. Il "contatto" tra questi due domini, tradizionalmente separati, si è reso necessario per garantire, oltre al rispetto dei requisiti normativi, il flusso di dati necessario a monitorare in tempo reale la "salute" dei macchinari e a implementare approcci orientati alla manutenzione predittiva.

Purtroppo gli investimenti in soluzioni per la cyber-security non sono aumentati di pari passo con l'aumento dell'esposizione degli asset. Questo ha creato una serie di "falle" **ampiamente sfruttate dai cybercriminali**. Lo conferma il rapporto Clusit 2025: i dati raccolti mostrano, infatti, che il **manifatturiero italiano è colpito da attacchi informatici quasi tre volte più della media mondiale**, rappresentando il 16% degli incidenti nazionali.

La digitalizzazione e l'interconnessione dei sistemi manifatturieri hanno **ampliato in modo significativo la potenziale superficie di attacco**, rendendo inefficaci i tradizionali paradigmi che miravano a proteggere il perimetro delle operations.

L'anomaly detection è una tecnologia che permette di fare dei significativi passi avanti sulla sicurezza, offrendo enormi benefici anche in termini di continuità operativa (o resilienza che dir si voglia), **garantendo l'integrità, la disponibilità e la confidenzialità dei dati nei sistemi critici** che governano i processi produttivi.

Tuttavia, come vedremo, oltre a permettere di erigere un'efficace difesa contro i cyberattacchi, l'implementazione di una piattaforma di anomaly detection **abilita anche ulteriori benefici operativi e strategici** che vanno oltre la sola sicurezza informatica.

Capitolo 1

Sicurezza OT, un mercato in grande crescita

Il mercato globale della cybersecurity sta vivendo una fase di espansione accelerata, a riprova della crescente percezione del rischio e della maturità delle minacce. Le proiezioni indicano che il settore è in crescita costante, con una dimensione valutata da Business Research Insights a circa **193,73 miliardi di dollari nel 2024**. Si prevede che il giro d'affari raggiungerà i **643 miliardi di dollari entro il 2033**, con un tasso di crescita media annua **(CAGR) di circa il 14,3%**. Secondo gli Osservatori del Politecnico di Milano, in Italia ha raggiunto 2,48 miliardi di euro nel 2024, segnando una crescita del 15% rispetto all'anno precedente.

All'interno di questo vasto perimetro, il segmento specifico dell'**anomaly detection** mostra dinamiche ancora più impetuose, trainato dalla necessità di soluzioni predittive e dall'aumento esponenziale degli incidenti. **Precedence Research** ha stimato un mercato globale nel **2025** di circa **6,90 miliardi di dollari** e prevede che raggiungerà i **28 miliardi di dollari entro il 2034**, con un CAGR del **16,83%**.

MERCATO CYBERSECURITY

193,73 mld $
nel 2024

(CAGR) 14,3%

643 mld $
nel 2033

ANOMALY DETECTION

6,90 mld $
nel 2025

(CAGR) 16,83%

28 mld $
nel 2034

A originare questa situazione contribuiscono diversi fattori chiave. In primo luogo, la proliferazione delle iniziative di digitalizzazione, l'integrazione di sistemi internet of things (IoT) e industrial IoT (IIoT) e la convergenza IT/OT hanno introdotto **complessità senza precedenti** per numero e tipi di configurazione, rendendo i metodi di sicurezza tradizionali insufficienti. Poi ci sono **diverse normative cogenti**, prima fra tutte la direttiva **NIS 2**, che stanno spingendo le aziende, in particolare quelle operanti come infrastrutture critiche o soggetti essenziali, a elevare drasticamente la propria postura difensiva, rendendo **obbligatoria l'adozione di strumenti di monitoraggio continuo e avanzato**.

Inoltre, come evidenzia Markets & Markets, il frenetico ricorso all'**intelligenza artificiale** (AI) e al **machine learning** (ML) sta trasformando l'efficacia dei tool di AD, offrendo capacità di analisi predittiva e di rilevamento delle minacce molto più sofisticate e veloci.

Per quanto concerne i driver settoriali, gli analisti di **Precedence Research** ci dicono che l'**industria manifatturiera e farmaceutica** sono i settori che offrono le migliori opportunità di ricavi per gli attaccanti.

Capitolo 2

L'esperienza di Fidia Farmaceutici

L'esperienza di **Fidia Farmaceutici**, azienda italiana leader mondiale nella ricerca, sviluppo, produzione e commercializzazione di prodotti innovativi a base di acido ialuronico e suoi derivati in aree strategiche quali joint care, skin care, eye care, specialty care e health&wellness care, è un **esempio significativo di come affrontare le sfide della convergenza IT/OT in un settore altamente regolamentato** (GMP/GxP).

La necessità di un **assessment** sull'automazione è stata accelerata dall'emergenza sanitaria globale del 2020, che ha evidenziato l'urgenza di controllare un'**infrastruttura di rete in continua evoluzione**.

La **principale criticità risiedeva nella gestione di un vasto parco di asset OT**, con centinaia di sistemi di controllo a bordo macchina, caratterizzati da forte eterogeneità, applicazioni sviluppate in epoche diverse, tecnologie legacy (alcune con trent'anni di anzianità) e driver obsoleti.

Questi apparati industriali, a differenza degli asset IT, hanno un ciclo di vita molto più lungo, estendendosi fino a 20-25 anni.

Di fronte a tale **eterogeneità e obsolescenza**, l'opzione convenzionale del revamping totale dei sistemi di controllo è stata scartata. Una scelta – spiega **Gilberto Rossi, Corporate OT & Industrial Process Automation Manager di Fidia Farmaceutici** – dovuta a diversi fattori: "In primo luogo gli elevati rischi operativi, dovuti alle potenziali criticità delle attività di revamping, ma anche l'impatto dei fermi macchina, non sempre controllabile in temini di tempistiche, e per finire l'impatto delle verifiche e della riconvalida richiesti dalle normative di settore"; tutti questi fattori ostacolavano la gestione di un progetto efficace a breve termine.

Per superare questa impasse, Fidia, attraverso il team gestito da Gilberto Rossi e Marco Casarin, Plant Automation Manager, con il supporto dei consulenti di ServiTecno, ha adottato un "approccio non convenzionale, privilegiando una **strategia top-down** di messa in sicurezza dell'infrastruttura a livello di rete, anziché intervenire sull'asset singolo", sottolinea Rossi.

Questa strategia, sviluppata in collaborazione con ServiTecno, è partita dalla **segregazione tra la rete IT e la rete OT** e dall'introduzione di meccanismi di monitoraggio attraverso la **piattaforma specializzata Claroty xDome**.

Il ruolo di **Claroty** è stato quello di fornire una governance dell'infrastruttura in fase di progettazione e un security framework per incapsulare i macchinari vulnerabili.

Parte della soluzione è il sistema di **anomaly detection**, di cui parleremo dopo in maniera più estesa e che si è rivelato particolarmente efficace in ambito industriale (OT) poiché il comportamento dei dispositivi è largamente deterministico.

In ambito OT le macchine eseguono quasi sempre le stesse operazioni, rispettando gli stessi tempi e utilizzando canali di comunicazione rigidi.

Pertanto qualsiasi anomalia – un cambio nel funzionamento tradizionale, nello scambio di dati o un'inaspettata comunicazione – viene percepita e notificata immediatamente.

L'anomaly detection supporta l'azienda nell'individuazione di attacchi cyber e anche di anomalie dovute a configurazioni errate o all'introduzione di malware tramite dispositivi deboli, come le chiavette USB, un canale di vulnerabilità comune su apparati OT non protetti da antivirus.

I **vantaggi ottenuti** sono stati immediati. "Tra i benefici tangibili che abbiamo ottenuto – sottolinea Rossi –, abbiamo riscontrato un **netto aumento del controllo e una diminuzione delle risorse dedicate al monitoraggio**. La piattaforma ha consentito l'aggiornamento continuo e automatico del system inventory e della risk analysis, attraverso il costante upgrade dell'indice di vulnerabilità, per tutti i dispositivi di campo, fornendo una **reportistica aggiornata** in tempo reale sugli asset e sulla gestione delle modifiche introdotte".

Questo ha permesso a Fidia di **tracciare i flussi** che precedono l'attuazione di modifiche e azioni correttive, "migliorando la gestione del change management e la prontezza di risposta agli incidenti".

Fidia inoltre ha progettato e qualificato l'infrastruttura e la sua Gestione Operativa, utilizzando come riferimento le linee guida di settore, in particolare la **GAMP 5 Second Edition**, che suggerisce l'impiego dei tools (come Claroty) per la gestione in compliance della rete, per garantire la conformità dei processi e ridurre la necessità di controlli manuali.

Tale **attenzione alla sicurezza e alla business continuity ha permesso di anticipare** una parte delle azioni correttive in risposta ai requisiti della **direttiva NIS 2**, che introduce diversi livelli di responsabilità per le funzioni aziendali, e impone attività di prevenzione e obbligo di notifica degli incidenti, secondo i principi della Business Continuity, che fanno parte della regolamentazione.

L'obiettivo ultimo dell'azienda è di estendere i tool di controllo centralizzati agli altri stabilimenti e di realizzare il concetto di "ready for audit".

Questo significa dimostrare in ogni momento la **robustezza della security posture industriale** e la conformità alle normative, classificando e prevenendo rapidamente le anomalie basate sullo storico operativo.

> *L'implementazione di Claroty xDome* – conclude Rossi – *ha trasformato una potenziale fonte di rischio e business continuity in un elemento di spinta all'**eccellenza operativa e supporto alla gestione della governance in ottica di conformità normativa**.*

L'esperienza di Fidia è una dimostrazione pratica che, in un contesto in cui l'aggiornamento completo dei sistemi è sostanzialmente improponibile, **la soluzione risiede nel rafforzamento del contesto operativo**, utilizzando l'anomaly detection per sfruttare la prevedibilità dei sistemi OT come scudo di sicurezza e strumento di governance.

Capitolo 3

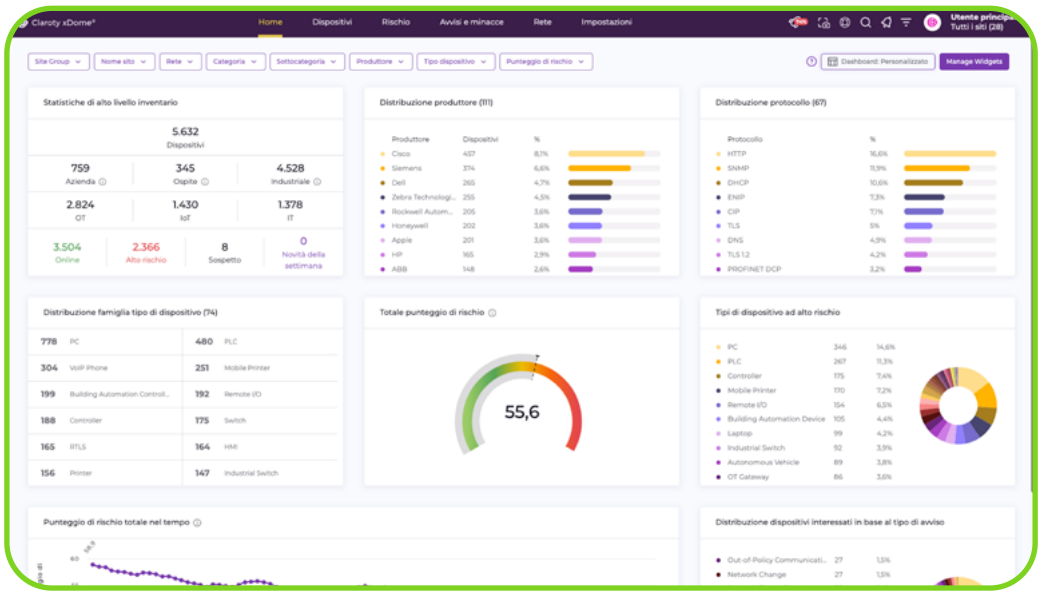
Claroty xDome, una soluzione efficace per la sicurezza OT

Tra le soluzioni più complete e avanzate per la sicurezza industriale c'è **Claroty xDome**, una piattaforma completa, che non si limita alla sola anomaly detection, ma che la utilizza come pilastro fondamentale.

Il valore aggiunto della soluzione risiede nella sua profonda **specializzazione per il dominio OT**. La Knowledge base di Claroty xDome è stata infatti **sviluppata anche grazie al contributo di importanti vendor industriali** (come Siemens e Rockwell Automation), che hanno supportato l'arricchimento della base di Know How relativamente a device e protocolli di comunicazione utilizzati in campo. Questa expertise tecnica si traduce nella capacità di supportare l'**analisi di oltre 500 protocolli proprietari e legacy**, una competenza essenziale sia per l'efficacia della deep packet inspection e sia per l'identificazione precisa dei dispositivi SCADA, PLC e IIoT.

Claroty xDome combina in modo sinergico l'approccio basato sul machine learning per l'identificazione di pattern anomali con la precisione della DPI, garantendo un'**elevata affidabilità nella rilevazione delle minacce** e nella riduzione dei falsi positivi. Si tratta di una piattaforma unificata e modulare, basata su cloud, che offre la semplicità e la scalabilità di una soluzione SaaS senza compromettere l'ampiezza e l'accuratezza dei controlli di visibilità, protezione e monitoraggio. xDome fornisce un inventario completo delle risorse, supporto nella gestione delle vulnerabilità e del rischio, controlli di segmentazione di rete e funzionalità avanzate di rilevamento e risposta alle minacce.

Rappresenta, quindi, una soluzione importante per la gestione della **cybersecurity industriale**, progettata per offrire **visibilità, protezione** e threat detection, in ottica **Monitoring & Governance**, in combinazione con l'eventuale *enforcement* (blocchi, isolamento, micro-segmentazione), realizzato tramite l'integrazione con firewall, switch, NAC o altri sistemi terzi, in una logica di **sicurezza orchestrata**.



Questo modello di combinazione di soluzioni in logica di sicurezza orchestrata, **in ambito** OT, IoMT e IoT (XIoT), supporta le aziende nella gestione dei rischi e nella protezione di equipment e devices vulnerabili.

La piattaforma Claroty xDome, **abilita inoltre l'inventario e la classificazione automatica degli asset in tempo reale**, mappando l'intera infrastruttura e aggiornando continuamente l'indice di vulnerabilità, fornendo una visione olistica e dinamica.

La gestione degli accessi è, infine, affidata a **Claroty xDome Secure Access**, una soluzione di accesso remoto creata specificamente per gli ambienti cyber-fisici, che garantisce il giusto equilibrio tra accesso senza restrizioni e controllo sicuro delle interazioni di terze parti con i CPS, migliorando così la produttività, riducendo le complessità e i rischi.

L'adozione dei principi **Zero Trust** realizzata tramite **Secure Access**, pur non sostituendo le funzionalità **PAM** (Priviledge Access Management) e **IGA Enteprise** (Identity Governance Administration), offre un livello di controllo, audit e tracciabilità perfettamente adeguato ai requisiti operativi degli impianti industriali e delle terze parti di manutenzione.

L'adozione di Claroty xDome, dunque, non si limita all'aspetto del rilevamento degli attacchi cibernetici, ma si estende al **monitoraggio del processo produttivo**, potendo segnalare deviazioni funzionali che, pur non essendo necessariamente attacchi, indicano un malfunzionamento del device o una drift funzionale del sistema. Questo approccio integrato è fondamentale per le aziende che necessitano di un **controllo centralizzato, reattività e gestione efficace del change management**, specialmente in contesti regolamentati.

Il valore di tali controlli aumenta ulteriormente grazie a un ampio ecosistema di integrazioni, alla solida API e alle opzioni flessibili di implementazione adatte a tutti i tipi di infrastrutture, architetture e ambienti.

Per cogliere al meglio le opportunità offerte da una soluzione per l'anomaly detection come Claroty xDome è però fondamentale adottare un approccio in grado di **coniugare una nuova strategia con le necessità e gli asset produttivi** delle aziende. È questa la via che segue ServiTecno, azienda che distribuisce e supporta la piattaforma Claroty xDome, forte di oltre 40 anni di esperienza nell'automazione industriale e nella cybersecurity OT. Attraverso la realizzazione di soluzioni ad hoc **ServiTecno** è in grado di soddisfare necessità specifiche in modo da **raggiungere gli obiettivi di sicurezza richiesti per assicurare la business continuity**.

Capitolo 4

Che cos'è e come funziona l'anomaly detection

Storicamente protetti dal concetto di **air gap** (isolamento fisico dalla rete), apparati OT come **PLC** (programmable logic controller), **HMI** (human-machine interface) o **SCADA** (supervisory control and data acquisition) visti spesso come sistemi di controllo isolati, sono ora interconnessi e ad altri sistemi attraverso l'intera infrastruttura aziendale a seguito delle spinte evolutive dell'Industria 4.0. Ne consegue che asset che non erano concepiti per essere esposti ai pericoli della rete siano oggi oggetto di un **ampio spettro di minacce** che sfruttano **protocolli e sistemi operativi legacy o proprietari**, intrinsecamente vulnerabili e per i quali solitamente non è facile trovare patch aggiornate.

L'anomaly detection funge da **cassetta degli attrezzi** che permette di gestire al meglio il nuovo perimetro ibrido, offrendo alle imprese la visibilità necessaria a **monitorare il comportamento** deterministico tipico di questi apparati e a **intercettare qualsiasi variazione** dal loro regime operativo standard in termini di flussi di comunicazione, scambio di dati, protocolli utilizzati o localizzazione fisica, **segnalando tempestivamente** anomalie che potrebbero essere il campanello di allarme di un'intrusione o di un vero e proprio attacco.
L'essenza dell'anomaly detection risiede nella capacità di **identificare deviazioni da un comportamento ritenuto standard o baseline** all'interno di un sistema, un processo o una rete. A differenza dei sistemi di sicurezza convenzionali, che si basano sulla conoscenza di firme di attacco predefinite (come gli intrusion detection system che sfruttano le signature), l'anomaly detection adotta **un approccio proattivo e adattivo**, che consente il rilevamento di minacce zero-day o di attacchi interni anche non fraudolenti, ma capaci di degenerare in incidenti gravi.

L'importanza di questa metodologia diventa ancor più strategica nel **contesto OT**, dove l'interruzione dei processi può comportare **ingenti perdite economiche e la compromissione della business continuity**, ma anche **mettere a repentaglio la sicurezza fisica degli operatori** o la salute umana (si pensi al settore farmaceutico o alle infrastrutture essenziali come acqua, gas ed elettricità).

Capitolo 5

Tecnologie e metodologie utilizzate nell'anomaly detection

L'identificazione delle anomalie nei contesti di rete e di processo si fonda su un **set eterogeneo di metodologie**, ognuna mirata a stabilire un profilo comportamentale baseline da cui è possibile misurare le deviazioni.

La tecnica predominante nell'ambito dell'anomaly detection per l'OT è il **monitoraggio passivo del traffico di rete**, spesso implementato attraverso l'uso di sonde posizionate strategicamente sui punti chiave di aggregazione del traffico industriale. Questi dispositivi operano senza interagire attivamente con gli asset di campo, **garantendo l'assenza di rischi per l'operatività** del sistema e la sua stabilità.

L'analisi passiva è coadiuvata dalla **deep packet inspection** (DPI), una tecnologia che estende la tradizionale ispezione degli header di pacchetto per analizzare il contenuto a livello di payload. Nel contesto OT, la DPI è **indispensabile per decodificare e comprendere gli oltre 500 protocolli industriali** proprietari e legacy (come Modbus, EtherNet/IP, Profinet, ecc.), determinando con granularità assoluta quali dati e flussi sono consentiti e in quale sequenza. Bisogna tenere conto che, a differenza di quello che accade nel mondo IT, nel mondo OT le comunicazioni sono codificate e relativamente stabili e la deviazione rispetto alla "norma" è quasi sempre indice di un malfunzionamento o, peggio, di un'intrusione.

L'altra componente tecnologica essenziale è il **machine learning**, che utilizza algoritmi per **elaborare grandi volumi di dati storici in tempo reale** al fine di apprendere i pattern comportamentali specifici di ciascuna tipologia di dispositivo (per esempio un particolare modello di PLC o SCADA). Il machine learning opera con la logica della **modellazione statistica**: analizza parametri quali il volume del traffico, la frequenza di comunicazione, gli host di destinazione e la sequenza delle istruzioni, costruendo un modello neurale statico che riproduce il regime operativo standard.

Quando il traffico di rete in entrata o in uscita devia in modo significativo dal modello appreso, il sistema **genera un allarme di anomalia**. Tale deviazione può manifestarsi, per esempio, in un PLC che tenta una connessione inattesa verso un host esterno o che evidenzia un cambio improvviso nella configurazione del suo firmware.

Per mitigare il **fenomeno dei falsi positivi**, tipico dei sistemi puramente basati su ML, le piattaforme più avanzate integrano il monitoraggio passivo iniziale con query attive e integrazioni con human-machine interface o system inventory esterni. L'obiettivo è arricchire il dataset e convalidare la reale criticità dell'anomalia rilevata.

Capitolo 6

Non solo cybersecurity: i vantaggi dell'anomaly detection

L'implementazione di una piattaforma di anomaly detection specifica per l'ambiente OT offre una serie di **benefici operativi e strategici** che trascendono la mera funzione di sicurezza informatica.

Il vantaggio primario è l'ottenimento di una **visibilità completa e in tempo reale sugli asset industriali, inclusi dispositivi legacy e ausiliari** (come, per esempio, telecamere e sistemi antincendio), che altrimenti rimarrebbero non censiti o documentati in modo inaffidabile o quanto meno non aggiornato. L'AD esegue automaticamente un'attività di discovery e di classificazione degli apparati, un prerequisito fondamentale per qualsiasi strategia di cyber risk management e per la conformità normativa. Un effetto "collaterale" è anche l'**aumento significativo del livello di consapevolezza** sugli eventi che si manifestano nell'ambiente operativo.

Grazie alla natura intrinsecamente deterministica degli asset OT, che eseguono cicli e funzioni con tempistiche costanti, le anomalie comportamentali, come un processo inconsueto di comunicazione o un volume di traffico atipico, sono intercettate con un'elevata attendibilità, **riducendo drasticamente il tempo di rilevamento** di una potenziale compromissione (mean time to detect - MTTD).

L'anomaly detection è efficace sia nel **rilevare gli attacchi cibernetici mirati** (minacce intenzionali esterne), sia nel **segnalare incidenti non intenzionali** (errore umano o malfunzionamento del device). Nel contesto industriale il rilevamento di un pivot point (movimento laterale) da un asset meno critico (come una telecamera) verso un PLC critico è un processo che l'anomaly detection identifica rapidamente.

Questa **capacità di early warning** è vitale, poiché i tempi di reazione a disposizione dei decisori, nel caso dei processi industriali, sono minimi: un ritardo nella risposta può tradursi nell'arresto di una linea di produzione o, in contesti critici, può compromettere la qualità del prodotto finale (per esempio, la sicurezza GMP nel farmaceutico).

Infine, l'**anomaly detection supporta l'aggiornamento continuo** dell'indice di vulnerabilità di tutti i dispositivi di campo, fornendo dati per la risk analysis e consentendo alle aziende di **concentrare le limitate risorse di remediation sulle vulnerabilità più critiche** e attivamente sfruttabili.

Capitolo 7

Il ruolo dell'AI nell'anomaly detection

L'intelligenza artificiale e, soprattutto, il machine learning rivestono un ruolo di primaria importanza nell'architettura dei sistemi moderni di anomaly detection, agendo come il **motore analitico che conferisce scalabilità e precisione** al rilevamento.

Il machine learning è essenziale per la creazione della baseline comportamentale, un processo che prevede l'**addestramento di modelli** (spesso reti neurali) su ampi dataset di traffico di rete legittimo e di dati operativi. Questa fase di addestramento consente all'algoritmo di apprendere i pattern ripetitivi e rigidi che caratterizzano gli asset operativi.

Nel contesto OT, il machine learning si specializza nel **riconoscimento di stati macchina e di logiche di controllo specifiche** per dispositivi come PLC e SCADA, superando la complessità derivante dalla loro eterogeneità e dalla presenza di firmware e sistemi operativi proprietari.
Ma c'è anche un rovescio della medaglia e l'uso esclusivo del machine learning può presentare delle criticità. Il lavoro statistico potrebbe **generare falsi positivi**, che possono allarmare il personale di sicurezza con alert non pertinenti. Per mitigare questo rischio e aumentare l'affidabilità, i sistemi di anomaly detection avanzati integrano il machine learning con la precisione forense della deep packet inspection basata sulla **conoscenza ingegneristica dei protocolli**, un'expertise sviluppata dai vendor operando in collaborazione con i produttori di asset industriali.

Si tratta quindi di un approccio ibrido, in cui il ML identifica i pattern statistici anomali e la DPI agisce come strumento di convalida, **stabilendo in modo deterministico e preciso**, a livello di byte del pacchetto, se il flusso di dati rispetta le specifiche operative concesse per quel determinato asset e protocollo.
L'AI quindi potenzia la capacità del sistema di evolvere e **riconoscere nuove minacce che non possiedono una firma nota**, ma la sua efficacia è ottimale solo quando è affiancata da un'intelligenza basata sulla conoscenza approfondita dei protocolli di campo, garantendo un'analisi profonda e contestualizzata degli eventi.

Capitolo 8

Sfide e criticità: quali sono e come superarle

Nonostante i benefici, l'adozione di soluzioni di anomaly detection nel settore dell'operational technology deve affrontare sfide tecniche e operative dovute alla natura dell'ambiente industriale.

Una delle principali criticità è la **gestione dei sistemi legacy e dell'eterogeneità dei device**. L'ambiente OT è popolato da asset con un **ciclo di vita che può estendersi fino a 20-25 anni** (rispetto ai 5 anni tipici del mondo IT), che impiegano **sistemi operativi proprietari** o non più supportati, per cui spesso non si realizzano più patch di sicurezza. E anche nel caso dovessero esistere, la loro applicazione potrebbe seriamente compromettere l'operatività degli equipment a causa di potenziali incompatibilità tra sistemi operativi, driver e software di controllo o hardware non adeguato. In questi casi, **la remediation di una vulnerabilità può comportare un costoso (e rischioso) revamping** elettro-strumentale dell'intera automazione.

Un'altra sfida è rappresentata dalla **limitata visibilità sull'infrastruttura di rete**, che in molti contesti è scarsamente documentata e gestita, rendendo complessa l'attività di discovery iniziale. Per superare questa lacuna, l'anomaly detection si basa sul monitoraggio passivo e sulla DPI, che agiscono come fonti primarie di documentazione e inventario in tempo reale.

Tra gli aspetti significativi di rischio vanno ricordati anche il **fattore umano** e la **gestione degli endpoint vulnerabili**, in particolare tramite l'interfaccia USB, e l'**accesso remoto non governato** da parte del personale di manutenzione e dei provider esterni. Tali vettori sono spesso la via più agevole per l'introduzione di malware o virus in device intrinsecamente vulnerabili. L'anomaly detection affronta questa criticità **monitorando il comportamento del device in relazione a ogni interazione di campo**, segnalando immediatamente l'anomalia comportamentale post-intervento o post-connessione USB.

Da ultimo bisogna porre la massima attenzione alla **collocazione delle sonde**: il sistema di anomaly detection è efficace solo se questi dispositivi intercettano un flusso di informazioni affidabile e completo.

La soluzione a queste sfide non risiede in un singolo strumento, ma in un **framework di sicurezza integrato** che, partendo da un approccio top-down basato sulla rete, utilizzi l'anomaly detection come strumento primario per l'identificazione e la mitigazione dei rischi operativi, isolando o virtualmente applicando le specifiche patch ai dispositivi vulnerabili.

ServiTecno

Se vuoi saperne di più

Contattaci

Via Francesco Koristka, 10 - Milano

info@servitecno.it

+39 02 486141