Presente e futuro della Cybersecurity industriale: la nuova frontiera della resilienza
Tre domande a Nicola Mugnato di Gyala

In vista di mcT Cybersecurity - Mostra Convegno dedicata alla Cybersecurity e alla Sicurezza Industriale in programma il 14 aprile alla Fiera di Bergamo, abbiamo fatto una chiacchierata con Nicola Mugnato, CTO & Co-founder di Gyala.



Fondata nel 2016 con il supporto del Piano Nazionale di Ricerca Militare, Gyala è cresciuta rapidamente trasformando la propria esperienza ventennale in ambito militare in soluzioni di cybersecurity avanzate per il mercato civile.
Dal 2021, Gyala collabora con aziende leader nei settori sanitario, industriale, navale ed energetico, offrendo una risposta concreta alle sfide di sicurezza più complesse e garantendo continuità operativa in contesti critici.
Oggi con la piattaforma all-in-one di cybersecurity Agger protegge infrastrutture IT/OT/IoT da minacce sempre più sofisticate, garantendo una difesa proattiva, personalizzabile e conforme alle normative europee.

Qual è il punto di vista di Gyala e quali sono le principali vulnerabilità negli impianti industriali e nelle infrastrutture critiche?

La cybersecurity industriale oggi non è più un tema esclusivamente IT. La convergenza tra IT, OT e IoT ha ampliato in modo esponenziale la superficie d'attacco delle aziende manifatturiere, delle utility e delle infrastrutture critiche. Il punto di vista di Gyala è chiaro: **non si può proteggere un impianto industriale con gli stessi paradigmi pensati per l'IT tradizionale.**
Le principali vulnerabilità che riscontriamo negli impianti industriali riguardano:
- Sistemi OT legacy con cicli di vita superiori ai 10–15 anni, spesso non aggiornabili e privi di patch di sicurezza.
- Accessi remoti dei fornitori non adeguatamente monitorati o segmentati.
- Mancanza di visibilità unificata IT/OT, che crea silos e ritarda la risposta agli incidenti.
- Assenza di reazioni automatiche, con tempi di contenimento incompatibili con la velocità degli attacchi moderni.
- Reti flat o scarsamente segmentate, che favoriscono movimenti laterali.

In ambito OT, inoltre, la compromissione non comporta solo perdita di dati, ma può generare fermo impianto, danni fisici e rischi per la sicurezza delle persone.

Gyala affronta queste criticità con un **approccio orientato alla Cyber Resilience IT/OT/IoT**: **non solo detection, ma reaction automatica a livello di singolo endpoint e dispositivo OT,** anche in reti segregate o ambienti air-gapped.
La nostra **piattaforma AGGER, nata in contesto militare e oggi adottata anche in ambito civile, integra XDR, Network Detection, OT Defence e Risk Management in un'unica architettura all-in-one**. **L'obiettivo è ridurre il tempo medio di reazione a zero secondi**, automatizzando le azioni di contenimento secondo regole personalizzabili e coerenti con il contesto operativo industriale. Inoltre supporta anche sistemi legacy.
Per noi, la **cybersecurity industriale non è solo protezione: è resilienza.**

Quali soluzioni presenterete ai professioni del settore alla giornata mcT?

A mcT Cybersecurity presenteremo AGGER, la nostra piattaforma 100% italiana di Cyber Automated Resilience IT/OT/IoT progettata per garantire resilienza operativa in ambienti industriali e infrastrutture critiche.
AGGER è una soluzione all-in-one composta da cinque moduli integrati:
- Extended Detection & Response (XDR)
- Network Security Appliance con analisi fino al Layer 7
- OT Defence (monitoraggio attivo e passivo di PLC e dispositivi industriali)
- Correlation & Incident Management
- Risk Management Tool

Ciò che differenzia AGGER sul mercato è **la possibilità di customizzare le regole di Detection e Reaction direttamente all'interno degli agent.** Questo significa che ogni endpoint o apparato OT può reagire autonomamente, e la reazione può essere calibrata sulle specificità dell'endpoint che deve proteggere, anche in assenza di connettività verso un SOC centrale.
Durante l'evento spiegheremo:
1) la nostra unicità ovvero la **possibilità di creare regole di detection e reaction personalizzate e personalizzabili per ogni singolo appaltato OT**
2) il nostro **sistema di tagging avanzato per classificazione asset IT, OT e IoT**
3) il **monitoraggio agentless** di PLC e dispositivi industriali
4) le **potenzialità della Dashboard unificata per la gestione completa di incidenti IT e OT**

La piattaforma è progettata per ambienti industriali complessi, supporta sistemi legacy (Windows XP, Linux, Unix, embedded) ed è installabile on-premise, in cloud o su reti completamente isolate.
Anche alla luce delle più recenti normative (NIS2, IEC 62443, e/DORA, Regolamento Macchine), Agger consente di coniugare protezioni tecniche e compliance, riducendo tempi, costi e complessità di integrazione.
A mcT porteremo una visione concreta: passare dalla difesa manuale alla resilienza autonoma.

Quali sono i progetti che Gyala sta sviluppando per il futuro?

Il futuro della cybersecurity industriale sarà caratterizzato da tre elementi chiave: autonomia, intelligenza distribuita e compliance by design.
Gyala sta investendo nello sviluppo di **un'architettura sempre più orientata alla Autonomous Cyber Resilience**, in cui **potenziare le capacità di detection e reaction** già presenti e ad ampliare la copertura dei sistemi OT.

Le principali direttrici di sviluppo riguardano:
- **Evoluzione dei modelli di AI comportamentale** per ambienti OT e IoT
- **Rafforzamento della protezione agentless** su PLC, RTU e SCADA
- **Integrazione avanzata con framework di compliance**

L'esperienza maturata in ambito Difesa – dove la soluzione Agger è stata testata in contesti ad alta criticità – rappresenta un vantaggio competitivo che oggi trasferiamo al mondo industriale e civile.

Il nostro obiettivo non è semplicemente rilevare un attacco, ma continuare a garantire che l'infrastruttura continui a operare anche sotto attacco.

Per maggiori informazioni:
gyala.com

GYALA
Cyber security