AGGER
Powered by Gyala

INDUSTRIAL
CYBER RESILIENCE

Cyber Resilience **IT/OT** per il settore **industriale**

GYALA
Cyber Security

AGGER
Powered by Gyala

INDUSTRIAL CYBER RESILIENCE

5 Moduli

- Endpoint Detection and Response
- Network Security Appliance
- Risk Management Tool
- Correlation Module
- OT Defence

Gyala è l'unico Vendor di Cyber Security ad aver portato l'automazione dei processi di Detection e Reaction anche all'interno dei singoli agent.

Agger è la piattaforma **Made in Italy all-in-one** di Cyber Security che, grazie a sofisticati algoritmi di intelligenza artificiale di derivazione militare, è in grado di prevenire, identificare e gestire automaticamente ogni tipo di minaccia di tipo informatico, massimizzando la IT/OT resilience dell'infrastruttura aziendale.

4 Funzionalità in un'unica piattaforma

Detection

Analizza il traffico di rete e i processi in esecuzione e identifica condizioni anomale utilizzando sia agenti software che sonde di rete con lo scopo di raccogliere e analizzare le comunicazioni di rete **senza interferire con il funzionamento o alterare la compliance di un dispositivo e/o sistema.**

Reaction

La reazione viene eseguita o guidando gli operatori umani attraverso la generazione di procedure dettagliate, o comandando azioni sul sistema IT/OT stesso, o dagli agent pre-istruiti con le azioni di contenimento e reazione che gli esperti di Cyber Security eseguirebbero affrontando i vari tipi di incidente, così da replicarne il comportamento. **Le regole di reaction** (e detection) **sono personalizzabili per singolo agent/endpoint.**

Orchestration

Crea modelli di comportamento dinamico - sulla base dell'analisi - utilizzati poi per identificare eventuali scostamenti.

Investigation

Raccoglie informazioni, eventi e incidenti da condividere poi agli esperti per la post-analysis.

AGGER
Powered by Gyala

INDUSTRIAL CYBER RESILIENCE

REGOLE CUSTOMIZZABILI
ANCHE PER SINGOLO AGENT

PIATTAFORMA ALL-IN-ONE

CLOUD | ON PREMISE | RETI SEGREGATE

SUPPORTA OGNI SISTEMA LEGACY

RESILIENZA IT/OT

DETECTION & REACTION AUTOMATICHE

ESTESA THREAT INTELLIGENCE

PREVIENE | IDENTIFICA | GESTISCE

TEMPO MEDIO DI REAZIONE
ZERO SECONDI

UN AGGER PER OGNI MERCATO:

- DEFENCE CYBER RESILIENCE
- UTILITIES CYBER RESILIENCE
- HEALTH CYBER RESILIENCE
- INDUSTRIAL CYBER RESILIENCE
- NAVAL CYBER RESILIENCE

Come lavora Agger:

Installiamo Agent e sonde oppure agiamo in **modalità agentless**.

MODALITA PASSIVA:

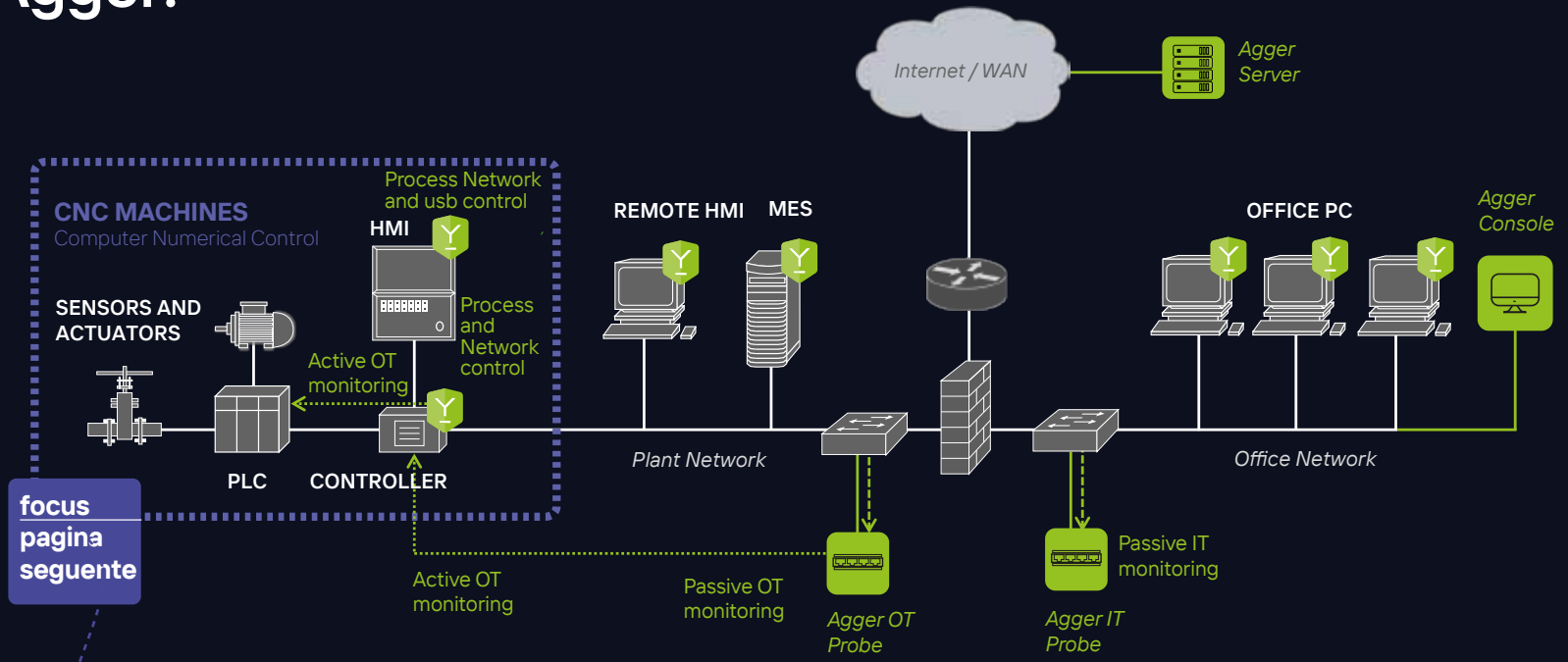
Basata sulla duplicazione e intercettazione del traffico di rete, e utilizzata per ottenere informazioni sul comportamento, le prestazioni e la sicurezza di un dispositivo OT o di un intero sistema OT. Consente di raccogliere e analizzare le comunicazioni di rete di un sistema o dispositivo operazionale (OT) **senza interferire con il suo funzionamento normale.**

Attualmente Agger utilizza il modulo NTA per l'analisi passiva, includendo al suo interno controlli per vari protocolli OT (S7,MMs, DNP3,..) e sviluppa ad hoc eventuali ulteriori protocolli necessari.

MODALITA ATTIVA:

Monitoraggio realizzato attraverso l'interazione diretta con il dispositivo OT, utilizzando le interfacce e i protocolli che il device espone sulla rete. Acquisendo molte più informazioni, consente di rilevare potenziali alterazioni delle configurazioni interne realizzate direttamente sul dispositivo fisico.

Attualmente Agger utilizza il componente Agentless Device Monitoring (ADM) per interrogare attivamente i dispositivi OT collegati in rete, attraverso richieste periodiche sui protocolli S7, Manufacturing Messaging System, SNMP. ecc.



NB

- **Configurazione di regole custom di detection e reaction sia per gruppi di agent che per singolo endpoint:** Consente di avere una gestione personalizzata degli incidenti in funzione del ruolo operativo degli asset impattati. Il set di possibili reazioni è estremamante ampio. Possono essere create complesse sequenze di azioni da eseguire in realtime sulla macchina che ha generato l'incidente, su quelle che appartengono allo stesso servizio potenzialmente a rischio, o su tutta l'infrastruttura IT o OT.
- Raccolta di informazioni sullo stato del sistema nell'istante in cui avviene un incidente, resa disponibile all'analista insieme alle regole applicate per contenerlo. Consente di verificare lo stato del sistema al momento dell'incidente: processi in esecuzione; connessioni di rete; utenti loggati; tabelle di routing; stato servizi; modifica delle configurazioni del task manager, di utenti e gruppi, delle configurazioni di rete, dei software installati, ecc.
- Possibilità di assegnare tag (colore e testo) agli endpoint e agli apparati agentless per attribuire informazioni quali ad es. la posizione fisica del device, il servizio a cui appartiene, il fornitore che lo gestisce, ecc.

COMPUTER NUMERICAL CONTROL MACHINE

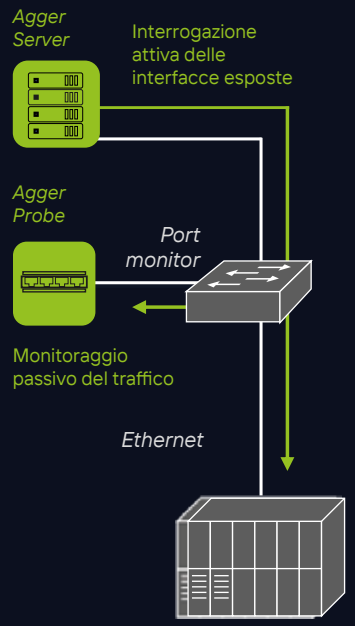
La soluzione per gli impianti industriali:

La crescente convergenza tra IT e OT ha portato significativi vantaggi operativi ed economici, ma ha inevitabilmente anche ampliato il perimetro di vulnerabilità delle infrastrutture e delle aziende interconnettendo due mondi storicamente e culturalmente precedentemente separati. L'incremento della frequenza di attacchi a infrastrutture critiche e siti industriali ha **evidenziato le debolezze strutturali del mondo OT** che, non essendo finora mai stato esposto a tali minacce, non ha sviluppato nuove soluzioni intrinsecamente sicure by design.

Per garantire la continuità e l'integrità dei processi produttivi, aumentandone la resilienza contro le minacce cyber, **è fondamentale adottare un approccio olistico che integri aspetti tecnologici e procedurali.**

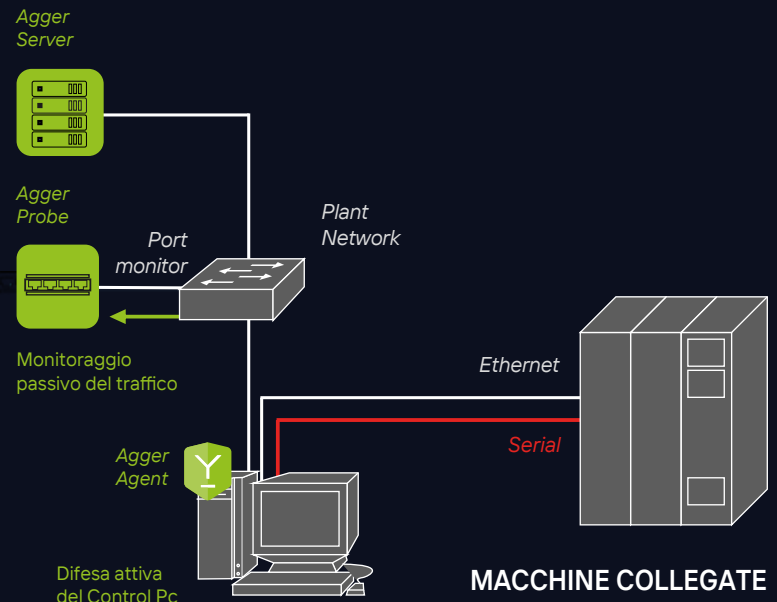
Gyala ha sviluppato un processo di messa in sicurezza degli impianti industriali, attraverso soluzioni dedicate alle varie tipologie di macchine e linee di produzione, che consente la piena compliance ai requisiti del Regolamento Europeo Macchine Sicure e del Framework Nazionale di Cybersecurity.

Tipologia 1



MACCHINE direttamente collegati alla rete

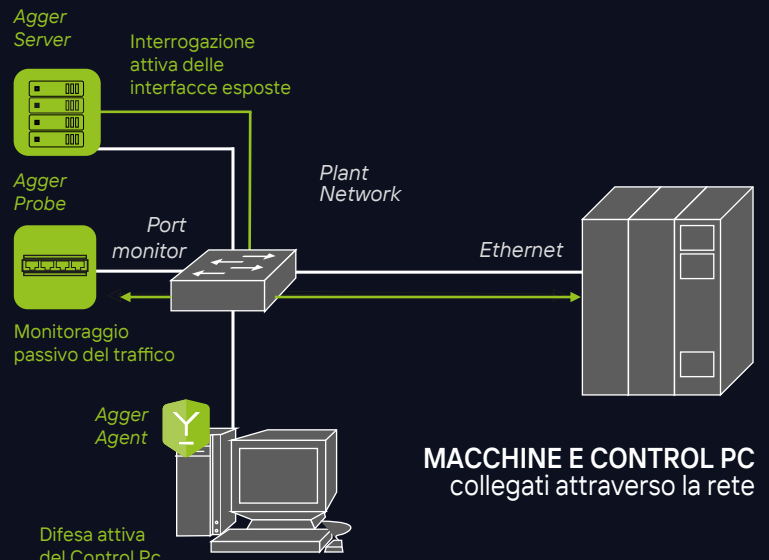
Tipologia 2



CONTROL PC

MACCHINE COLLEGATE ad un Control PC in rete

Tipologia 3



CONTROL PC

MACCHINE E CONTROL PC collegati attraverso la rete

AGGER INDUSTRIAL RESILIENCE È PENSATO PER:

CISO, Tecnici IT, Tecnici di linee di produzione industriali.

Completamente integrabile

Consente di ottenere la massima protezione senza interferire o limitare la continuità e l'integrità dei processi produttivi.

Regole custom detection e reaction

Possibilità di creare regole di detection e reaction sia a livello centralizzato che a livello di singolo agent per ottenere la resilienza dei servizi erogati da tutti i sistemi anche legacy.

Compliance

Compliance ai requisiti del Regolamento Europeo Macchine Sicure e del Framework Nazionale di Cyber Security.

Regolamento macchine

2023/1230

Il nuovo regolamento macchine richiede che i sistemi di sicurezza delle macchine siano progettati in modo da evitare che attacchi cyber possano causare comportamenti pericolosi.

L'Industrial Cyber Security è un elemento essenziale dal design della macchina a tutto il suo ciclo di vita.

Entro il

2027

Data di applicazione

Assicura la conformità al *regolamento macchine* con Agger industrial Resilience

AGGER
Powered by Gyala

INDUSTRIAL CYBER RESILIENCE

Gyala,
Al sicuro. **Sempre.**

Agger, Soluzione Custom Made

Agger, la nostra soluzione di **Cyber Security all-in-one** interamente modulabile e personalizzabile, offre supervisione e reazione automatica per ogni tipo di rischio, grazie a un sofisticato sistema AI di derivazione militare, che garantisce stabilità e resilienza degli ambienti IT e OT.

Innovazione Made in Italy

Gyala coniuga **l'approccio "agile"** tipico di una startup innovativa con il consolidato **know-how maturato** dai 3 Founder nella gestione di progetti di Cyber Protection di infrastrutture critiche, sviluppati grazie al PNRM, con il Ministero della Difesa e ora sul mercato grazie ai principali System Integrator nazionali.

Sviluppiamo soluzioni all'avanguardia di Automatic Defense per proteggere le risorse strategiche IT e OT di aziende pubbliche e private dagli attacchi informatici.

Gyala, il tuo Technology Partner

Grazie alla nostra **pluriennale esperienza in ambito di Difesa,** affrontiamo con competenza e **con la massima efficienza** le sfide crescenti del panorama della cybersecurity.

Ci avvaliamo di un ecosistema di system integrator, advisor company e solution provider che integrano la nostra soluzione all'interno dell'infrastruttura del cliente.

ISO 9001:2015
ISO IEC 27001

INDUSTRIA 4.0

marketing@gyala.com
gyala.com in Gyala