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

Extended 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 l'unica 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

Identifica condizioni anomale tramite l'analisi comportamentale dei processi in esecuzione nei computer, del traffico di rete, dei log di sicurezza già disponibili nelle infrastrutture e grazie alla verifica d'integrità e disponibilità dei dispositivi OT.

Artificial Intelligence

Crea modelli comportamentali dinamici sulla base dei dati raccolti e li utilizza per identificare eventuali scostamenti.

Reaction

Le reazioni vengono eseguite dagli agent pre-istruiti con le azioni di contenimento e contrasto che gli esperti di Cyber Security eseguirebbero affrontando i vari tipi di incidente o comandando azioni sul sistema IT/OT stesso o guidando gli operatori umani con procedure operative manuali dettagliate. **Le regole di reaction (e detection) sono personalizzabili per singolo agent/endpoint e sistema OT, consentendo di ottenere la resilienza dei servizi IT/OT difesi.**

Investigation

Raccoglie informazioni, eventi e incidenti utili per la post-analysis degli esperti di cyber security.

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:

Come lavora Agger:

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

MODALITA PASSIVA:

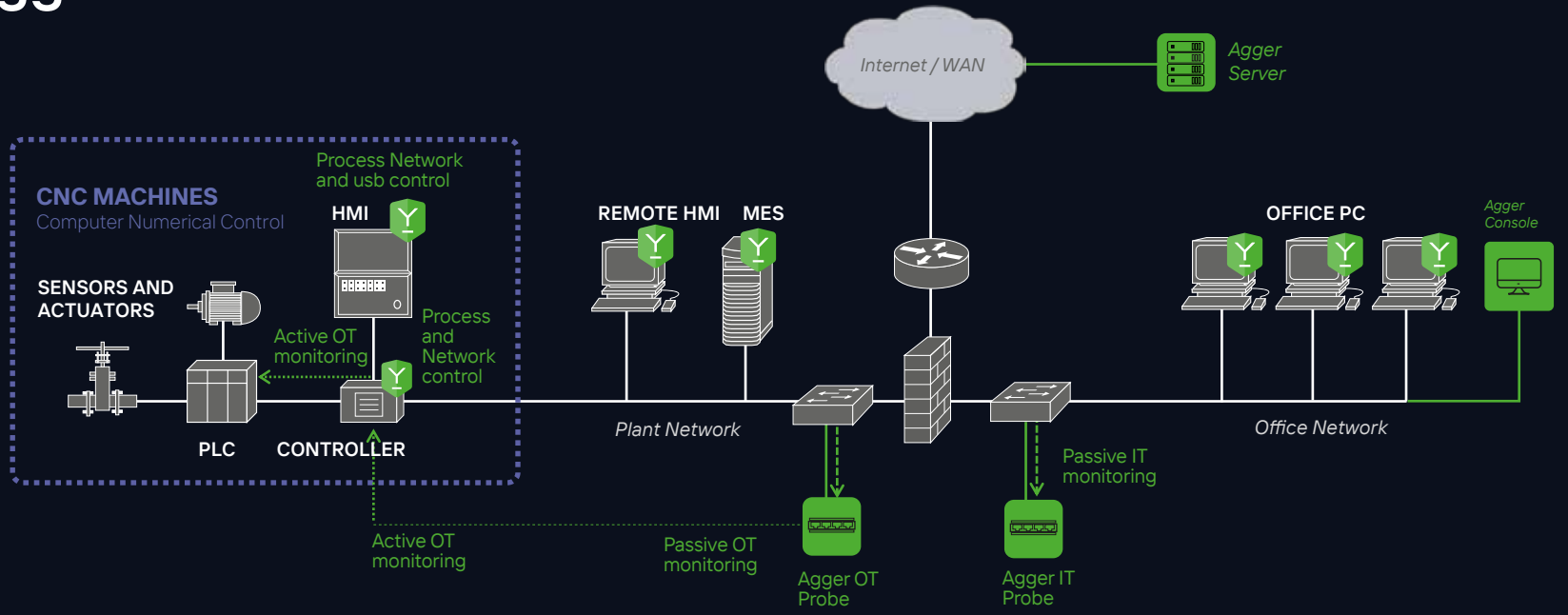
Basata sulla duplicazione e intercettazione del traffico di rete, viene utilizzata per ottenere informazioni sul comportamento, le prestazioni e la sicurezza di un dispositivo OT o di un intero sistema OT. Consente di raccogliere e analizzare le comunicazioni di rete di un sistema o dispositivo operazionale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

Agger Network Security è in grado di decodificare centinaia di protocolli OT standard (come ad esempio S7, MMS, DNP3,OPC, MODBUS, PROFINET) e può essere esteso con specifici plugin per protocolli custom.

MODALITA ATTIVA:

Monitoraggio realizzato tramite **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.

Agger OT Defence interroga attivamente i dispositivi OT collegati in rete, attraverso richieste periodiche su protocolli standard (come ad esempio S7, MMS, SNMP) e può essere esteso con specifici plugin per protocolli custom.



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 all'istante 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.

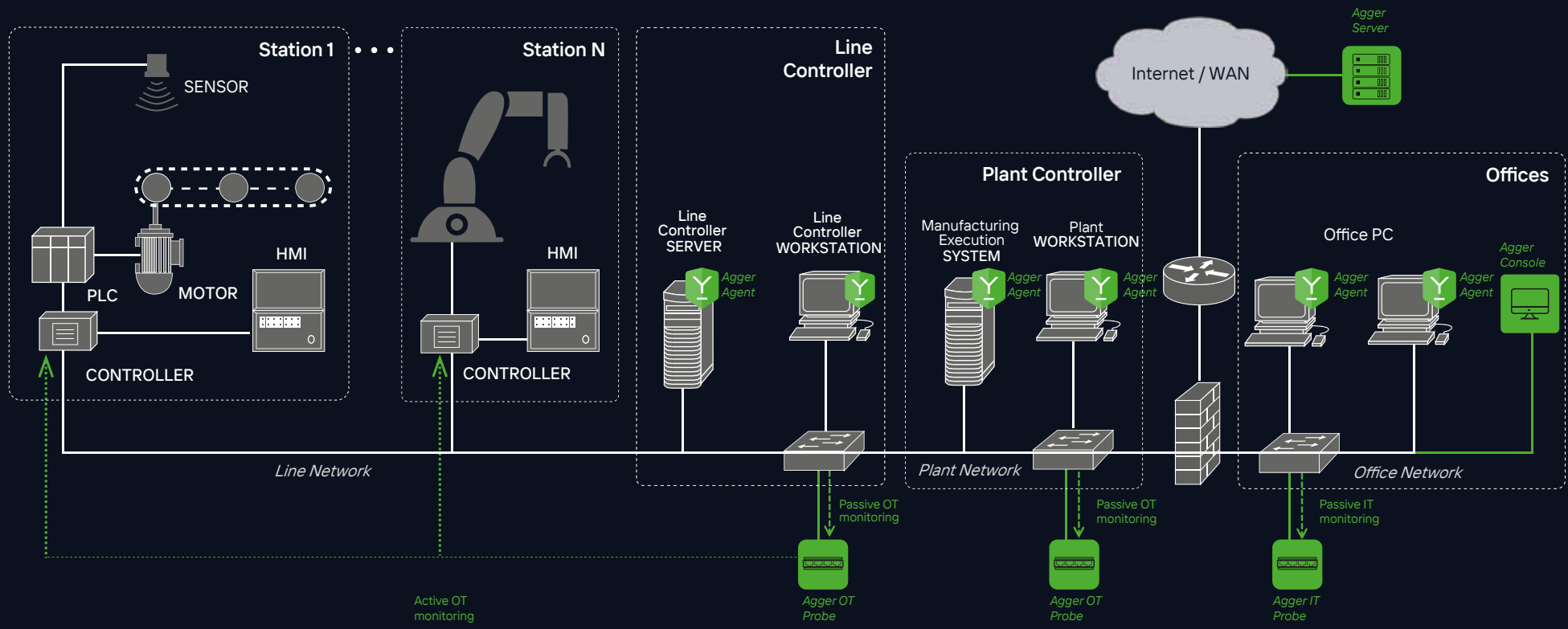
Possibilità di assegnare tag (colore e testo) agli endpoint e agli apparati agentless per attribuire informazioni come la posizione fisica del device, il servizio a cui appartiene, il fornitore che lo gestisce, ecc.

LINEE DI PRODUZIONE

La crescente convergenza tra IT e OT ha portato significativi vantaggi operativi eeconomici, ma ha inevitabilmente 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 ha ancora sviluppato 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.

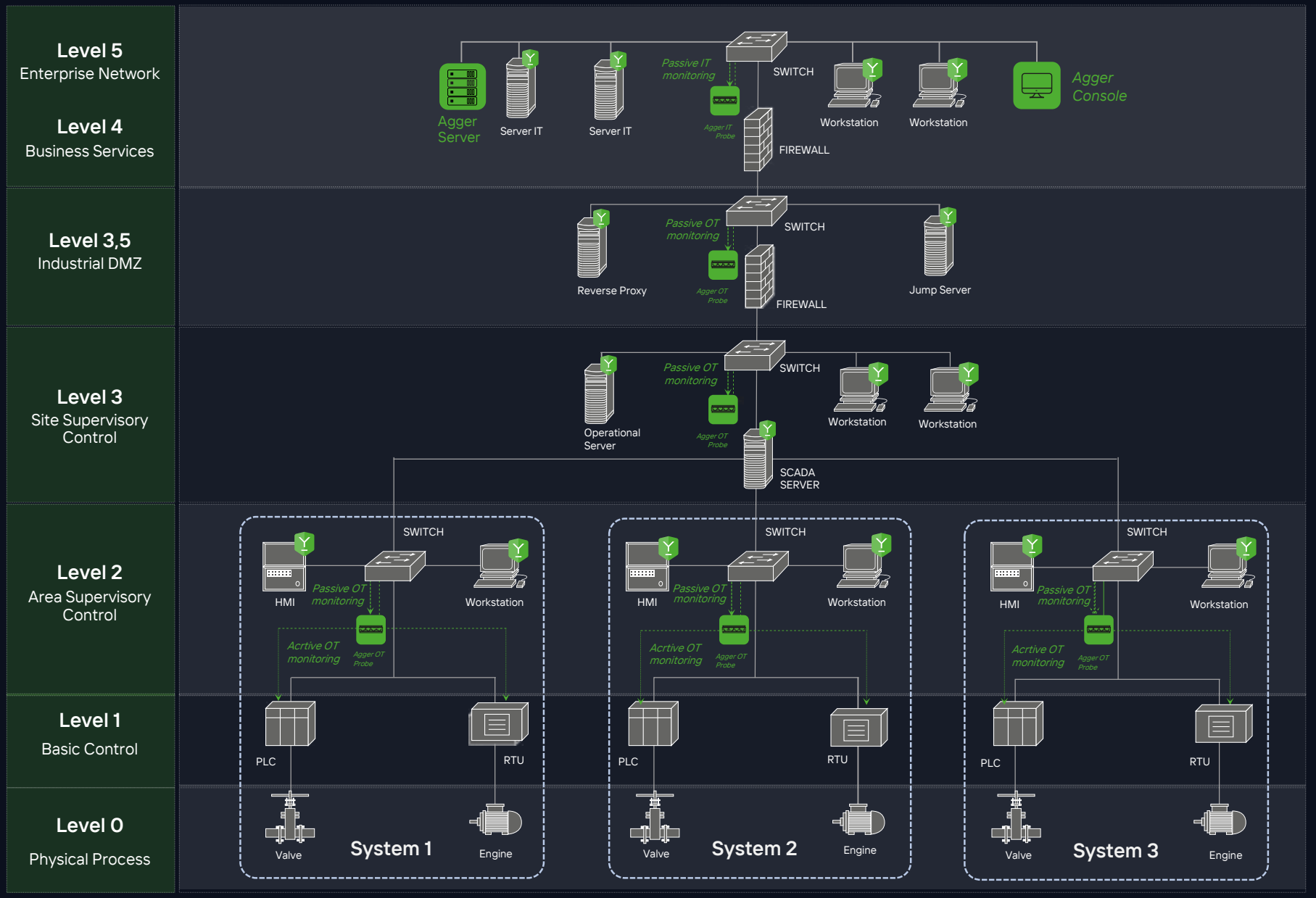


PURDUE MODEL

Purdue Enterprise Reference Architecture

IT
Facciamo monitoraggio passivo del traffico IT.
Installiamo agent su client e server e interroghiamo attivamente apparati di network.

OT
Facciamo analisi passiva del traffico e interrogazione attiva degli apparati OT.
Installiamo agent su computer di controllo e HMI.



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

CYBERSECURITY MADE IN EUROPE

marketing@gyala.com
gyala.com in Gyala