

AGGER
Powered by Gyala

NAVAL
CYBER RESILIENCE

Automated Cyber Resilience **IT/OT/IoT** per il settore **Navale**

GYALA
Cyber Security

AGGER
Powered by Gyala

5 Moduli

Endpoint Detection and Response

Network Security Appliance

Risk Management Tool

Correlation Module

OT Defence

Agger è la piattaforma di Cyber Automated Resilience **100% Made in Italy** progettata per proteggere infrastrutture IT, OT e IoT. Integra detection, analisi comportamentale e reaction automatica in un'unica architettura modulare e personalizzabile, riducendo il tempo di esposizione alle minacce e aumentando la resilienza dei servizi.

L'automazione e la personalizzazione delle regole di Detection & Reaction arrivano fino al singolo agent o endpoint.

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

Applica automaticamente azioni di contenimento e contrasto attraverso playbook personalizzabili. Le reaction possono essere definite a livello di singolo agent, endpoint o sistema OT e possono agire direttamente sui sistemi o guidare l'operatore attraverso procedure dedicate.

Investigation

Raccoglie e correla eventi, incidenti e informazioni di contesto, mettendo a disposizione degli analisti gli elementi necessari per investigazione, threat hunting e post-analysis.

AGGER
Powered by Gyala

Cyber Resilience IT/OT/IoT

AUTOMATICA. PERSONALIZZABILE. IN TEMPO REALE.

DIFESA PER TUTTI I SISTEMI IT/OT
ANCHE LEGACY

INSTALLAZIONE
- CLOUD
- ON PREMISES
- RETI SEGREGATE

<1 SECONDO
TEMPO MEDIO
DI REAZIONE

INTEGRABILE CON SERVIZI GESTITI
(ES. SOC, SIEM)
LADDOVE GIÀ PRESENTI

Tempo medio di reazione **zero secondi**

DETECTION & REACTION
AUTOMATICHE E PERSONALIZZABILI

anche per singolo agent o endpoint

Recognized by Gartner®

SAMPLE VENDOR

2024
Emerging Tech:
AI in CPS Security

2026
Hype Cycle™ for
CPS Security

2026
Hype Cycle™ for
Zero-Trust Technology

All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner's business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties merchantability or fitness for a particular purpose.

Come lavora Agger:

Installiamo Agent e sonde oppure agiamo in modalità agentless.

Riusciamo infatti a **aggirare il problema della impossibilità di installare agent software sulla logica programmabile degli apparati OT grazie a una sofisticata tecnica di interrogazione** dei device implementata in modalità agentless.

Agger è in grado di monitorare gli apparati OT in:

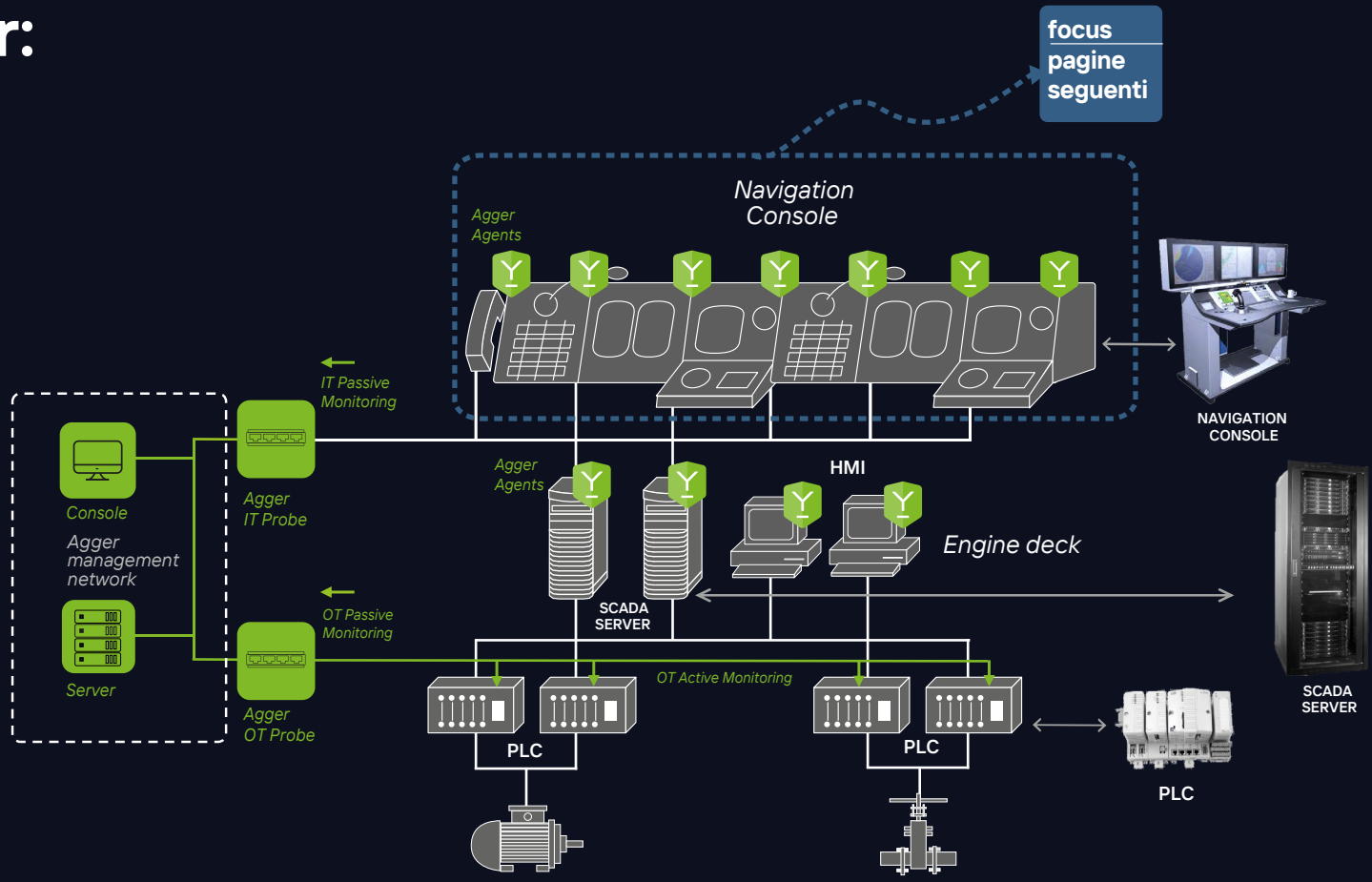
MODALITÀ PASSIVA
Basata sulla duplicazione e intercettazione del traffico di rete e utilizzata per ottenere informazioni sul comportamento, le prestazioni e la sicurezza dei dispositivi OT. Consente di raccogliere e analizzare le comunicazioni di rete di un sistema o dispositivo OT **senza interferire 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.

MODALITÀ ATTIVA
Realizzata attraverso l'interazione diretta con il dispositivo OT, utilizzando le interfacce e i protocolli che il device espone sulla rete. Ottenendo 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.

focus pagine seguenti



Standard IACS

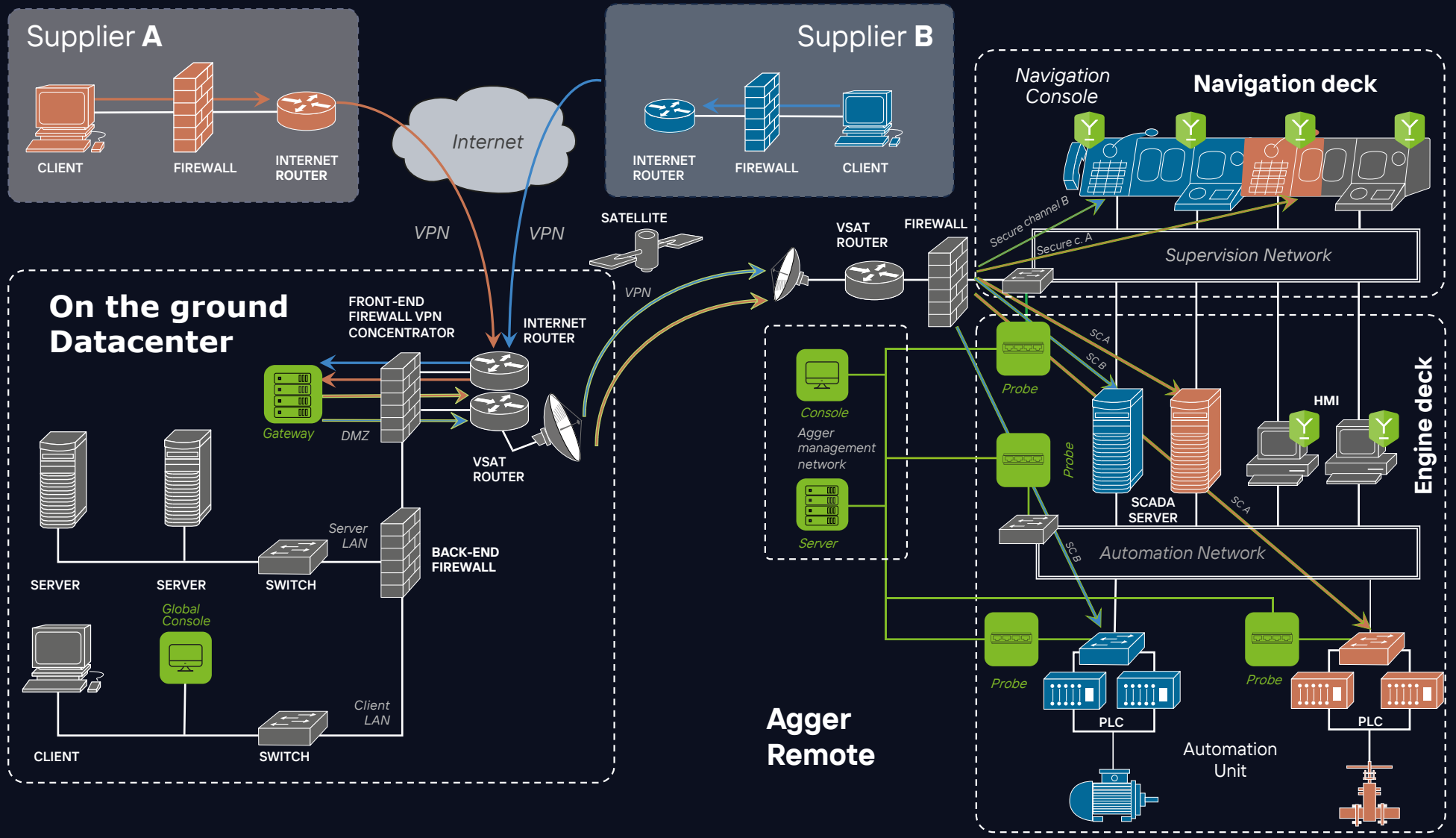
Dal 1 Luglio
2024
Obbligatori

International Association of Classification Societies

Assicura la conformità agli standard con Agger Naval Resilience

Gli standard UR-E26 "Cyber resilience of ships – Rev.1 Nov 20232" e UR-E27 "Cyber resilience of on-board systems and equipment – Rev.1 Sep 2023" **sono obbligatori per le navi ordinate dal 1 luglio 2024 e sono linee guida suggerite per le navi ordinate precedentemente.**

Il primo standard fornisce i requisiti per la cybersecurity della nave nel loro insieme, mentre il secondo per i singoli sottosistemi.



SHIP MANAGEMENT SYSTEM

Obiettivo: La resilienza delle infrastrutture IT/OT di bordo di una nave, consentendo un accesso sicuro e controllato dei fornitori di servizi di diagnostica e manutenzione da remoto.

Agger fornisce un **Secure Gateway** a terra che verifica l'accesso dei fornitori e abilita canali di comunicazione sicuri e segregati attraverso i servizi satellitari e verso ogni nave. La console del centro di controllo consente di definire policy semplici che consentono a un fornitore di accedere solo a predefiniti apparati dei sotto sistemi di bordo di una specifica nave in una prestabilita finestra temporale. Il Secure Gateway **registra tutte le sessioni dei fornitori e controlla in tempo reale che non vengano eseguite operazioni che violano le policy di sicurezza.**

Gyala, al sicuro. **Sempre.**

Agger, Soluzione Custom Made

Agger, la nostra **soluzione di cybersecurity** 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/OT/IoT**. Nata nel settore militare, oggi è anche a difesa delle infrastrutture civili.

Innovazione Made in Italy

Gyala è una **deep tech italiana** di Cyber Automated Security, nata per difendere ambienti critici, industriali e regolamentati, dalla **consolidata esperienza** dei 3 founder nella gestione di progetti di Cyber Protection di **infrastrutture critiche**, sviluppati con il Ministero della Difesa e con i principali System Integrator nazionali.

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

Gyala, il tuo Technology Partner

La **pluriennale esperienza in ambito di Difesa**, ci permette di affrontare **con efficienza** le sfide crescenti di cybersecurity.

Tecnologia abilitatrice per la compliance con le principali Normative come: **NIS2 · Framework Nazionale per la Cybersecurity · Regolamento Macchine (UE) 2023/1230 · DORA · IACS UR E26/E27 · IEC 62443 · Cyber Resilience Act.**

ISO 9001:2015
ISO IEC 27001

CYBERSECURITY™
MADE IN EUROPE

SCOPRI AGGER PER IL TUO SETTORE:
Consulta le soluzioni dedicate a Defence, Industrial, Naval, Health, Finance, Utilities, PA, PMI ed Enterprise.
Scarica le brochure.



marketing@gyala.com
gyala.com