AGGER
Powered by Gyala

NAVAL
CYBER RESILIENCE

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

GYALA
Cyber Security

AGGER
Powered by Gyala

NAVAL
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

NAVAL
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.

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:

MODALITA 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.**

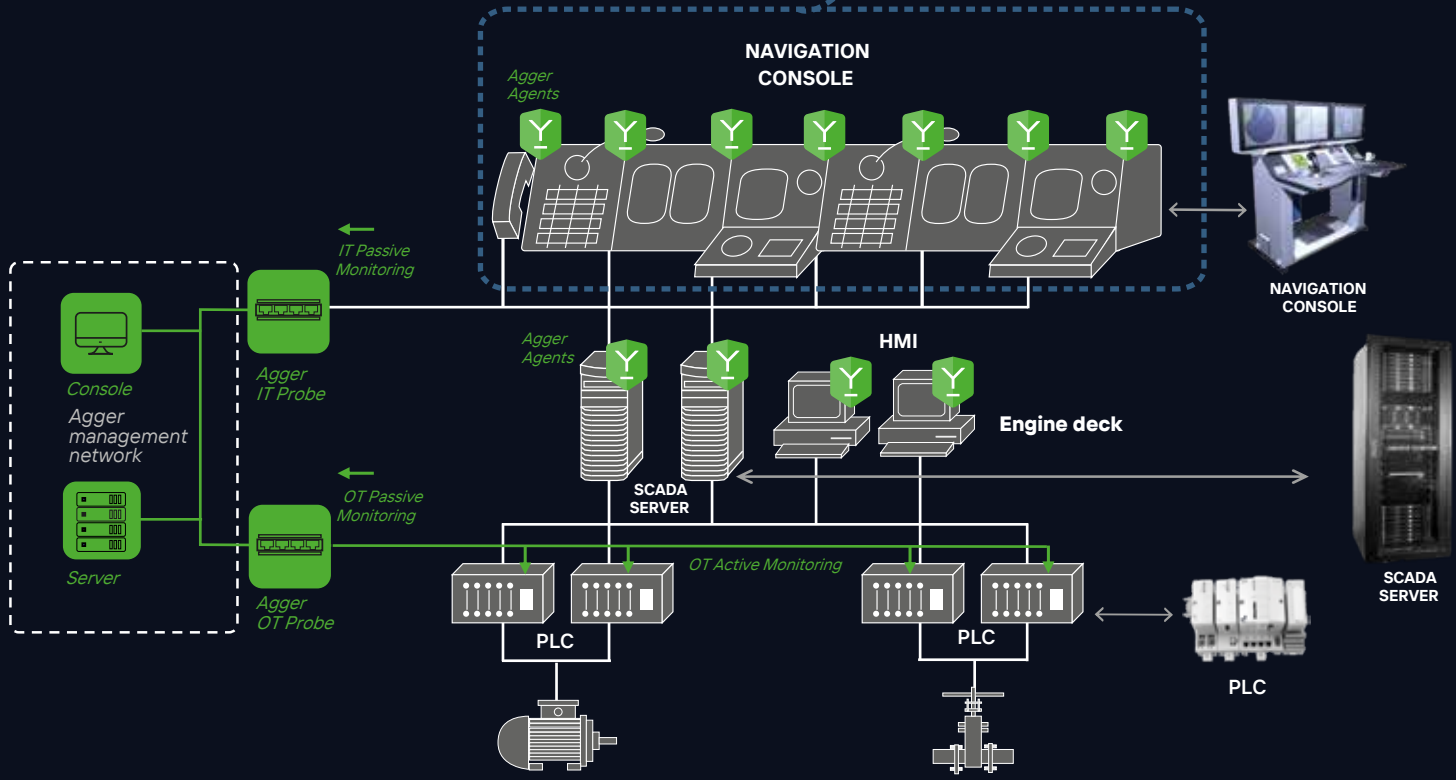
Agger Network Security è in grado di decodificare centinaia di protocolli OT standard (come ad esempio S7, MMS, DNP3,OPC, MODBUS, PROFINET) e può essere esteso con specifici plugin per protocolli custom.

MODALITA 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



Dal 1 Luglio
2024
Obbligatori

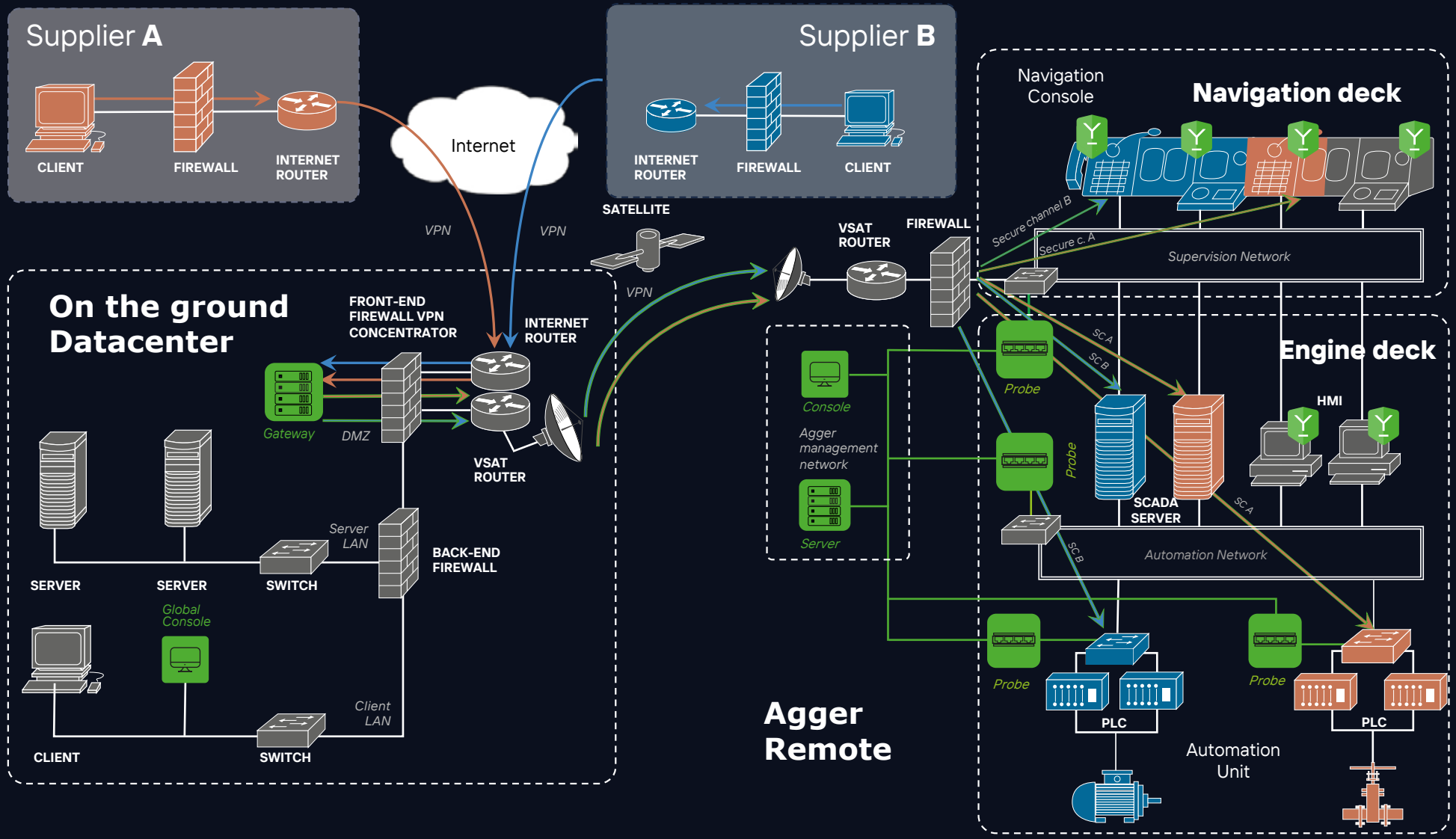
Standard IACS

International Association of Classification Societies

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 che verranno ordinate dal 1 luglio 2024 e sono suggerite come linee guida per le precedenti.**

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

Assicura la conformità agli standard con Agger Naval Resilience



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 i canali di comunicazione sicuri e segregati attraverso i servizi satellitari verso ogni nave. La console del centro di controllo consente di definire semplici policy 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 **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

COMPLIANT
AGLI STANDARD
IACS
UR-E26 e UR-E27

CYBERSECURITY
MADE IN EUROPE

marketing@gyala.com
gyala.com in Gyala