AGGER
Powered by Gyala

CYBER RESILIENCE IT/OT/IOT

Detection e Reaction 24/7 automatica e personalizzabile a livello di singolo end-point

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 informatica, massimizzando la IT/OT resilience dell'infrastruttura.

5 Moduli:

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

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 di'integrità e disponibilità dei dispositivi OT.

Reaction

Le reazioni vengono eseguite da agent pre-istruiti con le azioni di contenimento e contrasto che gli esperti cyber eseguirebbero per i 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.**

Artificial Intelligence

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

Investigation

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

UNA PIATTAFORMA CHE RISPONDE A TUTTE LE NECESSITÀ

INSERIMENTO DI REGOLE AVANZATO:

Le regole di detection in formati Sigma, Yara e Suricata aumentano flessibilità e precisione, migliorando l'identificazione delle minacce e riducendo i falsi positivi grazie a una maggiore espressività nella descrizione dei comportamenti sospetti.

QUERY COMPLESSE:

Tutti gli eventi, incidenti e dati di rete possono essere interrogati con ricerche testuali su ogni campo o con query avanzate in DSL (OpenSearch), migliorando l'analisi con precisione, velocità e capacità di esplorare informazioni complesse.

PIENA VISIBILITÀ TRAFFICO DI RETE:

La visibilità sul traffico di rete è stata ampliata: log dettagliati fino al layer 7 alimentano dashboard analitiche e modelli AI per l'anomaly detection, migliorando la comprensione operativa e riducendo drasticamente i falsi positivi.

TAG SYSTEM:

Il sistema di tagging consente di classificare liberamente endpoint e device, facilitando l'analisi degli incidenti, l'identificazione dei servizi critici e la gestione del rischio. I tag migliorano visibilità, risposta operativa e calcolo dell'impatto.

CONTROLLO TOTALE DA INTERFACCIA:

La console offre visibilità completa sul sistema operativo: processi, servizi, connessioni, utenti, patch e configurazioni sono monitorati in tempo reale. Ogni modifica è tracciata nel change log, con controllo diretto su rete, firewall e risorse.

SEZIONE OT/IOT:

È possibile effettuare la Discovery e monitorare in tempo reale dispositivi OT/IoT come PLC, sensori e macchine CNC, verificandone integrità e disponibilità. È possibile inviare comandi personalizzati ai dispositivi remoti dall'interfaccia Console.

SEZIONE INCIDENTI:

Gli agent raccolgono e inviano eventi, comandi e telemetrie di sistema, permettendo analisi dettagliate, ricostruzione della kill chain e attività di threat hunting. Il controllo diretto sugli endpoint supporta una risposta efficace agli incidenti.

CUSTOMIZZAZIONE REACTION E DETECTION:

Le regole di reaction (e detection) sono **personalizzabili per singolo agent**/endpoint e sistema OT**.**

IT/OT CYBER RESILIENCE

Endpoint Detection

Rilevamento su end point IT e OT e Network
Analisi comportamentale dei processi in esecuzione

Installation

Cloud
On premises
Reti segregate

Incident Management

Gestione degli incidenti IT/OT da un'unica interfaccia
Applicazione delle regole globali e/o personalizzate
Storico degli incidenti e correlazione tra gli stessi

Reaction

Reazioni preconfigurate in base a playbook
Reazioni personalizzate su singolo end point
Reazioni personalizzate centralizzate

Analysis

- Globale Threat Intelligence
- Correlazione degli eventi di sicurezza IT/OT e Network

Risk Management

Relazione tra device e servizi IT e OT
Valutazione dell'impatto degli incidenti sui servizi

Network Detection:

Analisi del contenuto a livello applicativo
Creazione di modelli comportamentali
Identificazione e blocco di incidenti

Anomaly Detection

Acquisizione dati a medio termine
Analisi comportamentale dei dispositivi IoT e OT
Identificazione di anomalie in funzione degli stati operativi

Compliance

- NIS/NIS2
- DORA
- AGID
- CER (DL n.134)
- Zero Trust NIST
- Regolamento Macchine

Framework:

- MITRE ATT&CK Framework
- IEC 62433 Framework
- NIST Cybersecurity Framework

Log Collection

Analisi dei log piattaforma
Ricezione log da sistemi terzi
Correlazione

Discovery

Ricerca attiva apparati IT/OT
Discovery passiva con sonde di rete

more info: marketing@gyala.com - www.gyala.com