AGGER
Powered by Gyala

# IT/OT/IOT CYBER RESILIENCE

**Automatic and customizable 24/7 Detection and Reaction at the endpoint level**

Agger is the only Italian company specialized in cybersecurity that, thanks to advanced military-grade artificial intelligence algorithms, is able to automatically prevent, detect and manage threats and anomalies 24/7, maximizing IT/OT resilience of the infrastructures.

## 5 Modules:

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

## 4 Funzionalità
**in un'unica piattaforma**

### Detection
Continuous monitoring of endpoints, networks, and OT systems using unique AI algorithms to detect anomalies in process and network behavior in real time.

### Reaction
Real-time, automatic, and customizable responses to threats, adapted to the specific infrastructure.

### Artificial Intelligence
Uses military-grade AI algorithms for supervision and automated reaction, capable of identifying and managing any threat or anomaly.

### Investigation
Agger gathers and synthesizes behavioral data from your infrastructure, making it available for expert post-analysis.

# ONE PLATFORM FOR ALL NEEDS

### ADVANCED RULE IMPLEMENTATION
Starting from Agger version 3.0, detection rules are expressed in Sigma, Yara, and Suricata formats. This makes the detection engine even more flexible, powerful, and granular. The use of these expressive formats improves threat detection and significantly reduces false positives.

### TAG SYSTEM:
The tagging system allows to freely classify endpoints and devices, facilitating incident analysis, identification of critical services and risk management. Tags improve visibility, operational response and impact calculation.

### INCIDENT SECTION
Agents collect and send events, commands, and system telemetry, enabling detailed analysis, kill chain reconstruction, and threat hunting. Direct control over endpoints supports effective incident response.

### ABILITY TO PERFORM COMPLEX QUERIES
All events, incidents, rules, and centrally collected information on host status, IoT devices, and network traffic can be queried with ease. Users can conduct simple text searches or use Query Domain-Specific Language (OpenSearch DSL) for more precise and faster results.

### COMPLETE CONTROL BY INTERFACE
The console provides complete visibility into the operating system: processes, services, connections, users, patches and configurations are monitored in real time. Every change is tracked in the change log, with direct control over the network, firewall and resources.

### FULL VISIBILITY INTO NETWORK TRAFFIC
Improved visibility into network traffic: Logs include comprehensive interpretations of Application Layer 7 protocols, aggregate data into dashboards, and enable AI-driven behavioral models, improving infrastructure understanding and reducing false positives.

### OT/IOT SECTION:
The OT/IoT section allows discovery of PLCs, network devices, medical equipment, CNC machines, sensors, and ECUs and enables real-time monitoring of their integrity and availability. Operators can define specific commands per OT/IoT device and send them directly from the console.

### REACTION AND DETECTION RULES CUSTOMIZATION:
Reaction (and detection) rules **are customizable for single agent**/endpoint and OT system.

## IT/OT CYBER RESILIENCE

### Endpoint Detection
- Detection on IT, OT, and network endpoints
- Behavioral analysis of running processes

### Installation
- Cloud
- On-premise
- Segregated networks

### Incident Management
- Unified interface for managing IT/OT incidents
- Application of global and/or custom rules
- Incident history and correlation

### Reaction
- Predefined reactions based on playbooks
- Custom reactions at the endpoint level
- Centralized custom reactions

### Analysis
- Global Threat Intelligence integration
- Correlation of all IT, OT, and network security events

### Risk Management
- Correlation between IT/OT devices and business services
- Assessment of incident impact on service continuity

### Network Detection:
- Deep content analysis at the application layer
- Behavioral modeling of network activity
- Incident detection and blocking

### Anomaly Detection
- Medium-term data acquisition
- Behavioral analysis of IoT and OT devices
- Anomaly detection based on operational states

### Compliance
- NIS / NIS2
- DORA
- AGID Guidelines
- CER (Legislative Decree 134)
- NIST Zero Trust Architecture
- EU Machinery Regulation

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

### Log Collection
- Platform log analysis
- Integration of 3rd-party log sources
- Event correlation

### Discovery
- Active discovery of IT/OT devices
- Passive network-based discovery with probes

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