At-a-Glance: SigaML² New Solution Release

SIGA Multi-Level OT Cyber Process Resilience

SIGA is extending its current Level 0 OT cybersecurity detection solution (SigaGuard) to a Multi-Level OT cybersecurity solutions suite – **SigaML²** – for all Incident Response phases based on the NIST framework. The new products in the SigaML² include **SigaGuardX** – a real-time monitoring solution to detect, classify, and investigate suspicious OT cyber events in the exploitation phase and **SigaPAS** – a Process Anomaly Simulation tool for OT security teams to simulate cyberattacks at the process level.

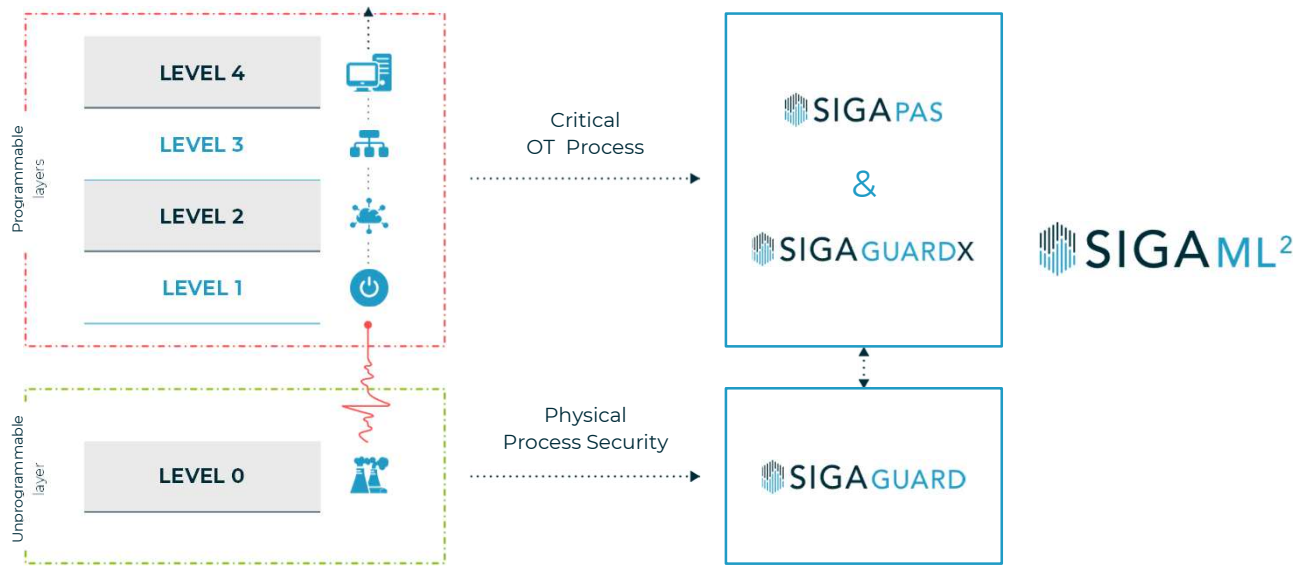
The Opportunity: Filling Critical Gaps in OT Cybersecurity Market

Augmenting Coverage of Current IDS Systems:
Traditional OT Intrusion Detection Systems (IDS) provide only partial insights into evolving threats, covering perhaps only 25% detection of potential OT cyberattack vectors.

Providing CISO Decision Support Tools for Incident Response:
Most existing solutions do not provide robust tools for managing cyber incidents once an attack occurs. This leaves OT security teams without reliable data to take decisions on containment, response, and recovery.

SIGA ML² addresses this gap with tools that cover not only detection but also providing real-time information to support critical decision-making during the Incident Response phase, offering visibility from the physical process level (Level 0) to Levels 1-4- PLCs, Control Software (HMI) etc.

SIGA ML² | Process Oriented, *M*ulti-*L*evel *ML* Approach



Why Now? Cyberattack and Regulatory Drivers

Regulatory Pressure & Compliance: Globally, regulations by NIST, EU (NIS2) and others are emerging to mandate OT cybersecurity protections and reporting requirements, often with significant penalties for non-compliance.

Rising Threat Landscape: Attacks on critical infrastructure are increasing in both volume and sophistication, making OT cybersecurity a priority for maintaining ongoing production and process resilience.

Tools for cyber-attack detection and Incident Response have gone from a "nice-to-have" to a "need-to-have." SIGA ML^2 delivers Multi-Level Machine Learning based cyber attacks detection to meet these rising challenges.

SIGA's Unique Value: Machine Learning and Multi-Level ICS Coverage

Process-Oriented OT Cybersecurity: Real-time visibility into the process level (Level 0), where many threats go undetected, ensuring that both cyber and operational teams have the information they need to respond effectively to attacks.

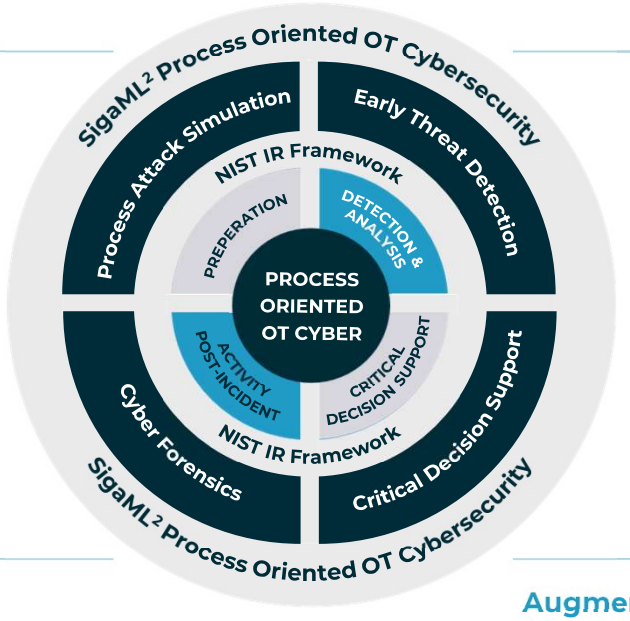
Advanced Machine Learning: SIGA applies Machine Learning (ML) and AI to data from all Levels (0-4) of the ICS, identifying suspicious asset behavior that is indicative of a potential cyberattack.

End-to-End Incident Response Management: SIGA supports critical decision-making for OT and cyber teams to manage cyberattacks effectively, including preparation, detection, containment and post-incident activities.

Training

An embedded OT cyber security simulation environment used to train teams in-house on realistic attack scenario and help them prepare and improve their cybersecurity skills

This knowledge is critical to the Forensics process and enables the prevention of future attacks and the development of procedures to prevent similar breaches.



Early Cyber Alerts

Advanced multi-level detection capabilities. Support Level 0 OT cyber security and provides immunity to "false data injection" scenario and enable "zero day" discovery for all attack expressions. Minimizes the attack identification time.

Provide accurate Level 0 data to help in the decision making during the containment phase. Help verify the process is restored to normal.

Augmenting Operational Data

About SIGA

SIGA provides a Process-Oriented OT Cybersecurity with real-time decision-making capabilities for managing critical Incident Response (IR) phases of an OT cyberattack – including Detection, Containment, Cyber-attack Forensics and OT cyber attacks simulation & IR training. Unlike other solutions, SIGA detects all expressions of a cyber-attack based on its unfiltered view of all Levels of Cyber OT, including Level Zero visibility.

Founded in 2014, SIGA has global customers in multiple sectors including Oil & Gas, Power Utilities, Data Centers and Water.

sygasec.com