Services +

ICSGuard

A Host Intrusion Detection System for HPCi Controller

DIGITAL

gepowerconversion.com

ICSGuard

ICSGuard, is an integrated health and security monitor for the controller, equipped with machine learning capabilities. ICSGuard will serve as a Host Intrusion Detection System (HIDS) Controllers.

Key Features

ROBUSTNESS & SCALABILITY

- Full featured, domain agnostic HIDS for HPCi controllers
- Scalable from small to large OT networks
- Fills the gap in the detection chain providing protection on the process control network

GRAPHICAL USER INTERFACE:

- Provides a comprehensive dashboard to monitor the controller status, alert history, recent alerts, and acknowledgment status
- Features a detailed display that shows alerts in real time as detected by the algorithm
- Provides the ability to visualize and maintain an asset inventory of the HPCI devices deployed in the OT network

MACHINE LEARNING

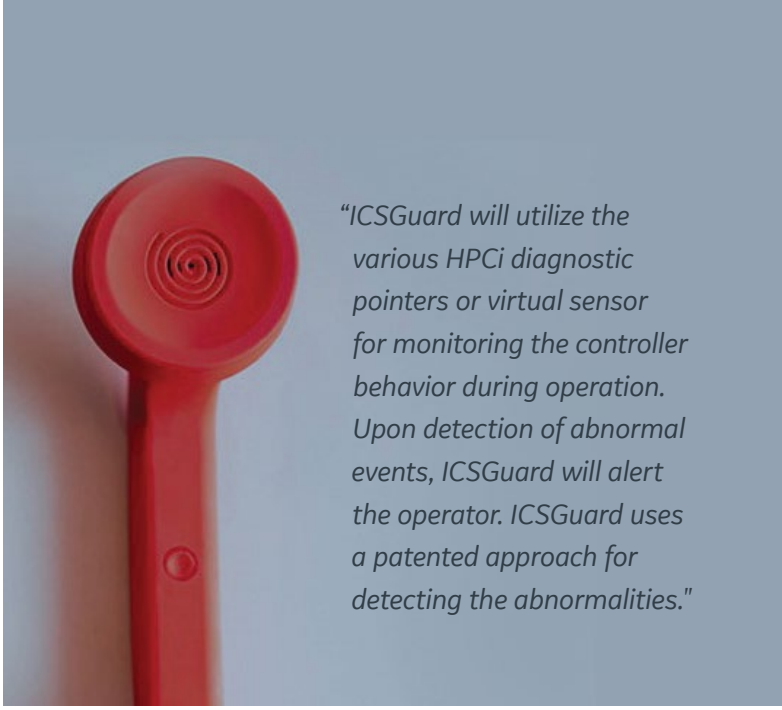
- Advanced machine learning capabilities for detecting control system abnormalities and security breaches
- ML performance feedback display provides the ability to monitor the performance of the ML models

REPORTING

- Ability to generate an executive event report summarizing all detected events in an easy-to-read format
- ICSGuard intrusion reports provide details on the leading forms of attack and provides a timeline of how attacks have progressed over time including any patterns detected

INTEGRATION

- Integrates directly with GEPCs “Security Management Suite” for user account management
- Integrates directly with GEPCs Data Historian or 3rd party syslog server for historizing events
- Integrates with a centralized SIEM solution



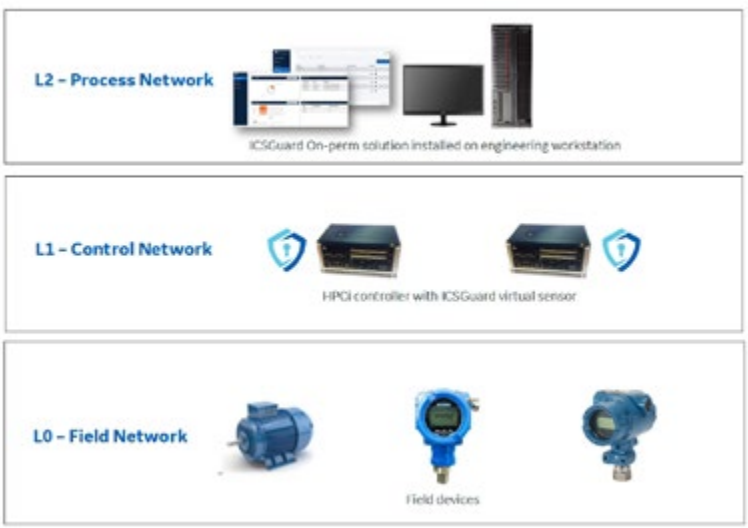
“ICSGuard will utilize the various HPCi diagnostic pointers or virtual sensor for monitoring the controller behavior during operation. Upon detection of abnormal events, ICSGuard will alert the operator. ICSGuard uses a patented approach for detecting the abnormalities."

Compliance

- ICSGuard meets the SL1 requirements of ISA/IEC 62443-4-2
- Complies to alert HIDS requirements of NIST 800-94
- Developed in compliance with ISA/IEC 62443-4-1 and thus providing “software development and lifecycle assurance” (SDLA)
- Role based access control is compliant to IEC62351-8

Deployment Architecture

ICSGuard operates in the process control layer as shown in the Purdue image below. As the HIDS for the controllers, ICSGuard monitors their behaviour for anomalies. ICSGuard can also be integrated to a centralized security incident and event management solution (SIEM).



Detection Capabilities

Cyber-attack detection

ICSGuard is able to detect attacks from both external and internal sources. It provides protection against various threat sources such as:

ACCESS CONTROL MONITORING

User login: Any user login needs to be monitored for potential inadequate intrusion by the plant authority

Multiple login failure: ICS Guard detects multiple failed controller login attempts. As this could be a sign of a brute force attack, dictionary attack or a rainbow table attack. The algorithm flags this as an alert for further investigation.

DEVICE MONITORING

SSH session initiated: ICSGuard detects SSH user logins on operational controllers. Since this is not expected on an operating plant, the algorithm will flag an alert.

An unknown command to the controller via secure socket shell (COTS) will be flagged as an alert.

NETWORK MONITORING

DoS attack detection: ICSGuard can detect a DoS attack or a broadcast storm onto the controller. It utilizes the virtual sensor values to detect the incoming storm. ICSGuard will continue to create alerts untill the DoS attack is eliminated from the network.

CONTROLLER MEMORY MONITORING

Memory leak prediction/detection: A memory leak is an unintentional form of memory consumption where an allocated memory block is not released after use. Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial-of-service attack (by crashing the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

ICSGuard predicts the memory leak in advance, additionally it can also detect a leak in progress.

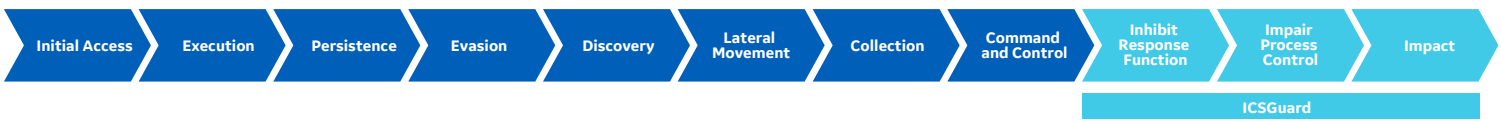
CONTROLLER TASK MONITORING

Task overrun detection: In operations, task overrun occurs due to various reasons such as increased network traffic, communication failure, etc. An attacker can also cause a critical task to overrun to disrupt the plant operation. ICSGuard can detect such overrun immediately and alert the plant authority for further investigation.

Task suspension detection: In operations, task suspension is uncommon. But a threat actor can gain access to a controller and can potentially suspend a critical task to disrupt the site operations. ICSGuard can detect such threats immediately using virtual sensor technology.

Compatibility Matrix	Sys_HPCi 7.1.x	Sys_HPCi 7.2.x	Sys_HPCi 8.1.x
Features			
Access Control Monitoring			X
Device Monitoring			X
Network Monitoring	X	X	X
Controller Memory Monitoring	X	X	X
Controller Task Monitoring			X
Configuration Monitoring			X
Basic Asset Information	X	X	X
Enhanced Asset Information			X

How ICSGuard is different from a NIDS ?



- A network-based intrusion detection system (NIDS) detects malicious traffic on a network.
- As per the MITRE ATT&CK framework shown above, several tactics and techniques are used to attack a control system.
- Typically NIDS are able to detect attacks early in the attack chain. Once the attacker has reached the "inhibit response state" it is almost impossible for a NIDS to detect them.
- ICSGuard is designed to fill this gap in the detection chain. ICSGuard is an important part of a defence in depth architecture, protecting the heart of the control system.
- ICSGuard performs prediction and detection of attacks and faults based on behavioral analysis of the controller by using patented machine learning algorithm.

Conceived for Operators

GE Power Conversion's Digital Suite is built on GE's industry wide expertise in IT, OT (operating technology) and IIoT (the industrial internet of things). Above all we believe it should be intuitive, visual and customized for your operational needs. Featuring simple, clear interfaces it provides organizations of all sizes with access to GE's powerful data analytics, made accessible and usable by providing better intel and situational awareness. Genuine performance improvements are within reach, to help your organizations work with increased efficiency and profitability.

About GE's Power Conversion Business

GE's Power Conversion business applies the science and systems of power conversion to help drive the electric transformation of the world's energy infrastructure. It does so by making and delivering advanced motor, drive and control technologies that evolve today's industrial processes for a cleaner, more productive future. Serving specialized sectors such as energy, marine, renewables and industry through customized solutions and advanced technologies, GE's Power Conversion business works with customers to increase efficiency.

To find out more:
contactus.powerconversion@ge.com

DIGITAL

GEA35227 02/2023