Logsign

Advanced OT-IT Threat Detection with Logsign Next-Gen SIEM

Datasheet

Advanced OT - IT Threat Detection

Logsign SIEM guarantees full control and security on the OT-IT network with its Correlation, Security Analytics features and Big Data embedded infrastructure by allowing security analysts to easily monitor assets on the network.

How does Logsign SIEM ensure visibility, security and control on your IT and OT systems?

Logsign protects all industrial systems from complicated attacks that cause irretrievable damage to technologies (IT) and operational technologies (OT).
It provides:

A Scalable SIEM Solution: All corporate and industrial cyber security shareholders receive a scalable SIEM solution that eliminates the security concerns between the IT and OT. It uses Open API and detects the threat by integrating with the cyber defense products developed by security producers. It also offers strong Correlation skills that enable institutions to be proactive against cyber threats. By providing a strong platform for security and compatibility management on the industrial process control networks, Logsign offers an advanced cSOC software platform.

Supportive Technologies: Logsign SIEM combines the necessary technologies such as security gap evaluation and unauthorized access detection to support the physical and infrastructural requirements of industrial applications. Its simple and understandable user interface and dashboard screens facilitate the planning and application of a complete solution.

A Modular Detection and Response Platform: The modular detection and response platform Logsign SIEM offers prevents attacks on critical control systems. It broadens this protection by leveraging its scalable and expandable infrastructure with the attack detection signatures of firewall producers (Palo alto, Checkpoint, FortiGate) peculiar to OT systems, and by getting support from ICS equipment producers with regards to tight integration and legal compliance frameworks.

Comprehensive Protection: Logsign SIEM delivers complete visibility, security and control for industrial networks. It enables the security professionals to effectively detect and reduce the threats against the security, reliability, and continuity of industrial processes.

When Planning, Designing, Managing and Improving Cyber Threat Monitoring Infrastructure, aim to achieve the following goals:

- React to attacks and conduct legal analysis
- Improve attack detection and prevention skills
- Leverage global cyber intelligence services to proactively anticipate new potential attacks
- Continuously monitor and analyze network infrastructure
- Enable advanced security automation, perception, and visibility
- Increase control of the distributed processes
- Improve compliance with legal requirements and monitoring
- Respond faster when incidents occur and improve corporate performance
- Create better decision-making processes based on more detailed information
- Reduce reaction times to proactive maintenance and unforeseen malfunctions
- Increase information flow to shareholders

How to Design a Proactive Cyber Security Infrastructure on OT-IT Systems with Logsign SIEM in 11 Steps

1. Use an SMS & E-mail alert system to warn users when a suspicious incident/threat or a hardware change/error is detected on the OT system.
2. Perform a detailed investigation of the security gaps in the OT network traffic and the traffic formed with the cyber threat intelligence service against the operational threats.
3. Conduct effective threat detection with detailed association on the packages received from the OT Communication Protocols (Modbus/Profibus).
4. Direct the suspicious traffic detected by Logsign SIEM to the Palo alto – FortiGate - Checkpoint Firewall tools when requested, and act.
5. Detect the operating hours, IP addresses and countries of the tools used by the attackers.
6. Analyze the capability of the SCADA communication protocols used in the sector Modbus, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, OPC, ProfNet, and S7 (Siemens).
7. Investigate the traffic between IT-OT and protect from the threats coming from the IT network.
8. Investigate the traffic on the OT network using deep package analysis focusing on content details against the security gaps and operational threats.
9. Obtain the momentary incidents from the Windows XP – Windows 7 OT-ICS terminals with the Logsign Client agent.
10. Use the MITRE ATT&CK Open Source Cyber Attack Technical Tactics and Procedures to perform attack analysis and prevention actions.
11. Support the notification and incident response processes when an anomaly or threat is detected or suspicious fingerprints are observed on the L3 layer by supporting the enterprise NIDS/NIPS structures.

About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

0 850 660 0 850

Info Security Products Guide 2020 GLOBAL EXCELLENCE BRONZE

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE SILVER

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD

CYBER DEFENSE GLOBAL AWARDS CYBER DEFENSE MAGAZINE 2018 WINNER