positive technologies

PT Industrial Security Incident Manager

PT ISIM ensures OT network security and provides monitoring capabilities for OT and IIoT infrastructures of Industrial and Building facilities

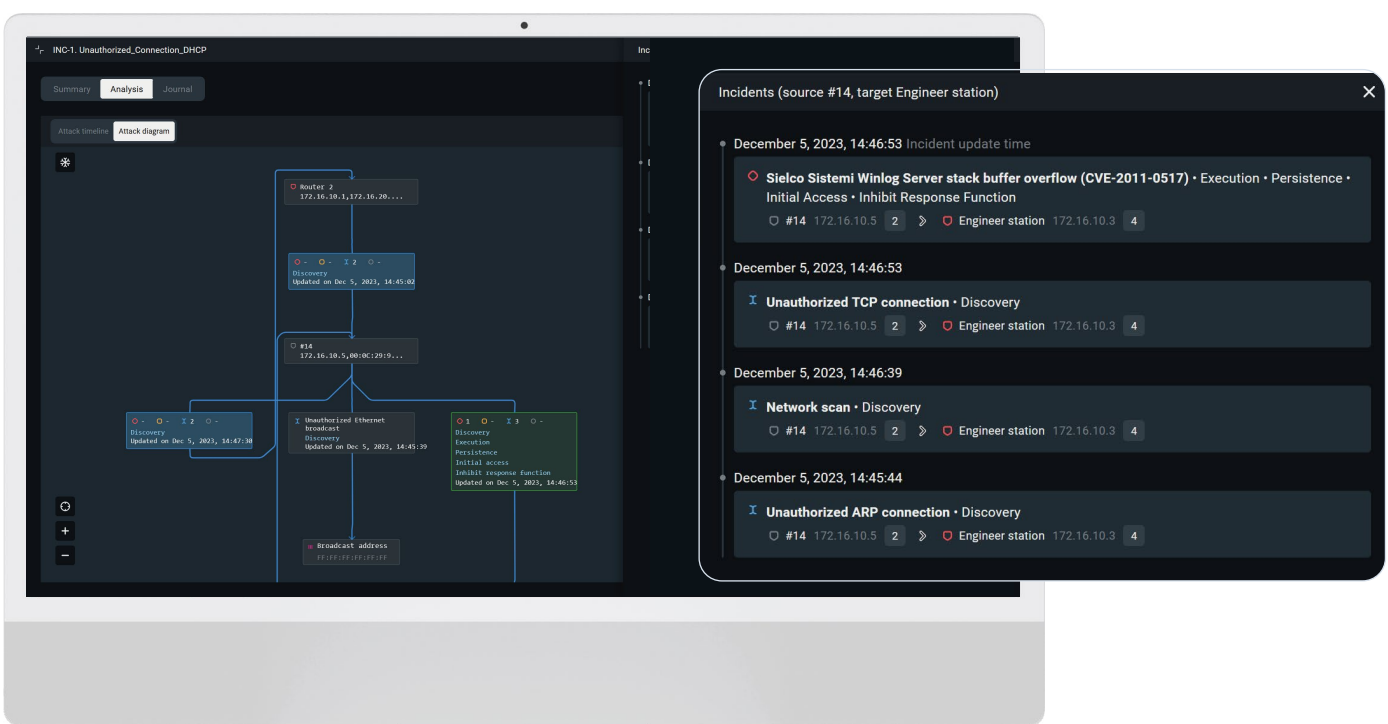
PT Industrial Security Incident Manager

is an in-depth traffic analysis system for the OT networks with rigorous traffic inspection for both common and specific industrial network protocols. Looking at the traffic both on perimeter and inside the industrial control network, PT ISIM detects malicious operations that may deem dangerous for operational processes and provides necessary artefacts for security incidents investigations.

PT ISIM relies on its own database of industrial cyberthreats - PT Industrial Security Threat Indicators (PT ISTI). Available out of the box this rich expertise helps start monitoring and threat detection without time-consuming configuration of a network sensor.

Value proposition

- PT ISIM detects more than 130 network protocols and can be used in any industrial infrastructure or in IIOT environments, with Building Management Systems and healthcare DICOM-based equipment;
- PT ISIM controls all communications inside the OT network and detects anomalies, threats, flaws in OT configuration and even dangerous control commands – critical for any industrial company
- PT ISIM unveils hidden IT assets inside the OT infrastructure. Clear understanding of the OT network structure is essential for ensuring robust OT operations



Use cases

- OT network inventory and new assets detection
- Anomaly detection, malicious and dangerous commands
- Malware detection with export of suspicious files for thorough statistical and behavioral analysis in PT Sandbox
- Vulnerabilities exploitation and other adversary techniques
- Compliance with regulatory requirements

Industries

- Industrial Control Systems (ICS)
- Critical Infrastructure systems
- Building Management Systems (BMS)
- Rail transport control systems
- Distributed industrial companies
- Industrial IOT
- DICOM-compatible healthcare equipment and systems

Who benefits from PT ISIM?

PT ISIM engages all technical services and departments who can benefit from observability and predictability of OT infrastructure and security monitoring:

- security personnel – can secure critical OT infrastructures from actual cyberthreats
- OT maintenance personnel – can ensure resilience of the OT infrastructure and uninterrupted operation of critical processes
- OT managers and dispatch personnel – can safely operate the plant and achieve production KPI with cyber risks sufficiently mitigated

How it works

PT ISIM takes a copy of the OT network traffic from a SPAN port of an industrial switch, crunches all captured packets and communications, visualizes network topology with all hosts and network communications. If malicious operations or anomalies found PT ISIM generates an alert and saves raw traffic for further investigation. PT ISIM can then inform the north-bonding SIEM system in the SOC, for example, MaxPatrol SIEM.

8000+

rules and industrial threat indicators are available "out of the box" and applicable for Windows and Linux infrastructures.

PT ISIM

Components

PT ISIM View Sensors – network sensors

Key components of the system that capture and store OT network traffic. Sensors are deployed inside the OT infrastructure and connected to the OT network with PLCs, SCADA servers, engineering and operator workstations.

PT ISIM Overview Center – management console

Unified interface for centralized monitoring, management and upgrade of multiple connected ISIM View Sensors. Usually deployed at the level of SOC or data center. Overview Center receives incidents from all connected Sensors.