PRODUCT DESCRIPTION

Positive Technologies
Industrial Security
Incident Manager

PT ISIM

ptsecurity.com

Scope of application

- Automatized ICSs
- Control systems for urban engineering infrastructures
- Automated control systems for critical infrastructure facilities
- Engineering infrastructure control systems at data analysis centers, business centers, and malls
- Industrial plants and facilities with distributed infrastructure

4,000+
rules for detecting industrial cyberthreats

Key benefits and capabilities

PT Industrial Security Incident Manager is a refined tool for conducting uninterrupted traffic analysis within company networks.

PT ISIM is designed for use in security operations centers (SOCs), where cybersecurity incidents are addressed.

With PT ISIM, SOC specialists have the tools they need to effectively monitor the security of industrial control systems (ICSs).

- **Quick deployment and enhanced security.** PT ISIM is equipped with passive monitoring architecture and self-learning capabilities. Integration into active ICS networks can be accomplished in a minimal timeframe.
- **Detection of cybersecurity noncompliance.** PT ISIM will detect infractions of cybersecurity regulations and deviations from company standards before they become problematic.
- **Simple integration with existing processes.** PT ISIM comes with all the necessary mechanisms for integration into pre-implemented security solutions, as well as to expand those systems' functionality. With detailed, high-level record keeping, communication of individual events and incidents at the level of the SOC (to SIEM and other systems), and capabilities for investigation of detected incidents, system integration is simple and secure.
- **Inventory and monitoring of system integrity.** PT ISIM compiles an automatic inventory of network elements, including ICS components, and constantly monitors network integrity.
- **Incident visualization.** Convenient graphic tools combine network topology and production workflow for an eagle-eye view of security. Security incidents can be visualized at the level of business logic.
- **Site-specific flexibility.** PT ISIM provides the flexibility necessary to monitor threats and attack vectors specific to a given site. Data from ICS audits guarantee optimal configuration of monitoring mechanisms.
- **Fit for an industrial setting.** Physical conditions in industrial settings can be far from gentle. PT ISIM components are selected with industry specifics in mind, so they can withstand demanding conditions without missing a beat.

PT Industrial Security Threat Indicators

PT ISIM detects security violations using a unique database of industrial cyberthreats, PT Industrial Threat Indicators (PT ISTI). Thanks to PT ISTI, PT ISIM can detect potential attacks on software or on ICS equipment (scanning of ICS network nodes, vulnerability exploitation), while the attacks are still in their preparatory stage. It can also identify system configuration errors (for instance, weak passwords or deactivated encryption settings), detect potentially unsafe network

practices (for instance, outdated protocols), and bring attention to undocumented (and unsafe) commands used to manage ICS equipment (PLCs, industrial switchboards, and terminals).

The threat database also enables PT ISIM to detect potential vulnerabilities in ICS networks, including those that could be exploited by ransomware viruses such as WannaCry or Petya, or by other damaging software, like Trisis/Triton. It also allows for the detection of cryptocurrency mining within a network.

Positive Technologies experts frequently update PT ISTI with new signature methods and rules for detection of attacks made on industrial equipment and software. The database consists of vulnerabilities and weak points in ICS security that have been located by specialists in the course of security analyses and state-of-the-art studies conducted on cyberthreats.

PT ISIM can be updated automatically or manually. The database contains several thousand signature methods and rules for detecting attacks on common systems including ABB, Emerson, Hirschman, Schneider Electric, Siemens, and Yokogawa.

Goal and aims

PT ISIM improves the security, accessibility, and consistency of technological processes via network traffic analysis and preventative detection of attacks aimed at ICSs.

PT ISIM netView Sensor can be deployed and used without any specialized skills or training

System deployment goals

- Uninterrupted ICS cybersecurity analysis
- Control over personnel and customer actions
- Detection of cybersecurity compromise and ICS attacks
- Detection of incidents and notification of individuals responsible for cybersecurity
- Creation of a trusted data source for thorough investigations into cybersecurity compromise incidents
- Incident analysis including discovery of true causes and impact assessment
- Recommendations for mitigation and prevention of incidents
- Ensuring compliance with regulatory guidelines (including FSTEC orders 31 and 239, critical information infrastructure law 187-F3, and coordination with GosSOPKA centers)

1 hour

is all the time it takes to launch PT ISIM netView Sensor in an active ICS segment using automatic configuration

Technical solutions

- A copy of ICS traffic data is transmitted via a unidirectional data diode and undergoes constant processing
- Event analysis at the level of communication protocols, including industrial protocols (Siemens S7, IEC104, DIGSI, GOOSE/MMS, Schneider Electric UMAS, CIP, Yokogawa, PROFINET DCP, SPA-Bus, EKRA, OPC, Modbus and others)
- Automatic ICS network scheme visualization
- Identification of unauthorized connections to the ICS network
- Detection of potential threats and direct attack attempts
- Discovery of unauthorized changes to technological parameters
- Network access control to PLC settings (reading and editing of microprograms and PLC projects)
- Detection of unauthorized PLC access and manipulation
- Detection of complex, time-spaced ICS attacks (attack chains)
- Generation of cybersecurity incidents taking into account the technological process logic
- Visualization of the mnemonic scheme of the technological process and indication of components whose operation is disrupted by cybersecurity incidents
- Compilation of incident reports and reports on ICS security status, and transfer of reports to external systems (SIEM, GosSOPKA)

80%

of relevant threats to ICS can be detected by PT ISIM netView Sensor «straight out of the box,» without the time-consuming configuration required by most similar solutions

Scalability

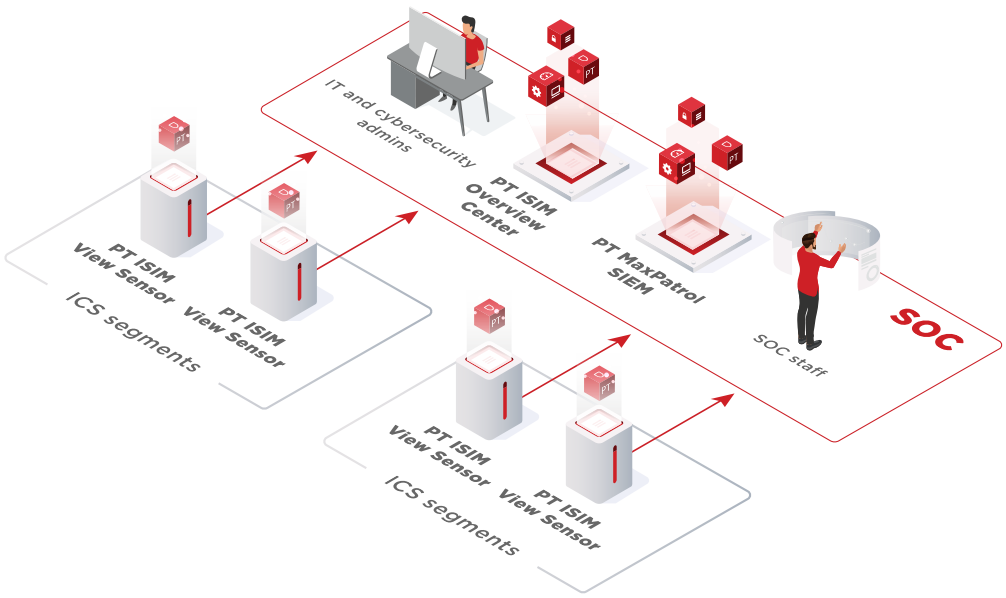
PT ISIM solutions can be easily scaled to meet specific requirements and demands. PT ISIM components can be integrated gradually, meaning a large, sudden investment won't be needed for a full system overhaul. PT ISIM netView Sensor, the most basic version of the network sensor, is simple to install and ideal for initial integration and daily use. In the long-term, PT ISIM licensing options allow for increased system functionality without having to update equipment. The number of components that can be included in a PT ISIM system is unlimited. When initially being rolled out, the system can be applied exclusively to critical areas, then expanded to all processes with time.

System components. Functions and technical specifications

PT ISIM is an integrated set of components, including network traffic analysis servers (sensors), business analytics servers, and SOCs. Working together, these components identify critical incidents and communicate them to staff at industrial facilities.

- Full-function PT ISIM View sensors and interface-free PT ISIM sensors are used to collect and analyze traffic at the level of the ICS network segment that is being defended (where operator workstations, SCADA severs, and PLCs are located). They receive a copy of traffic data from a router mirror (Mirror/SPAN) port or a TAP device.
- he PT ISIM Overview Center component centralizes sensor management. It collects information on registered incidents, ensures centralized configuration, and updates connected sensor components. PT ISIM can also send information about events and incidents directly to SIEMs (for instance, MaxPatrol SIEM).
- All PT ISIM components run on Debian OS and communicate with one another via HTTPS. Access via Secure Shell protocol might be required for initial installation and configuration.

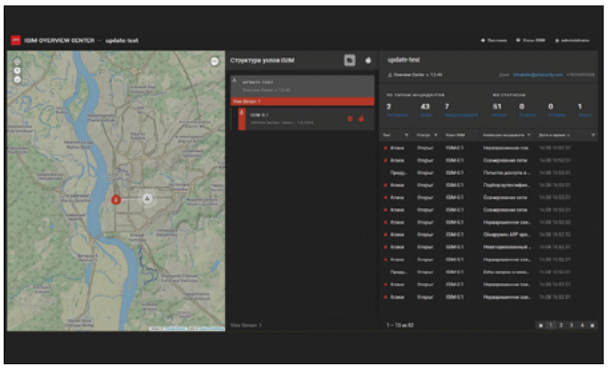
Complex solution based on PT ISIM, PT MaxPatrol SIEM, and MaxPatrol 8 is a perfect match for an industrial company's SOC



Sample of system architecture with View Sensors and Overview Center management servers

PT ISIM system components

Component	Functions and essential capabilities
PT ISIM View Sensor	▪ ICS segment traffic analysis ▪ Process events in real time. ▪ Support industrial and IT protocols (DPI). ▪ Automatic identification of ICS network nodes (inventory) ▪ Visualize industrial network topology. ▪ Intelligent detection of infractions (unauthorized manipulation of ICS components and exploitation of vulnerabilities) ▪ Event analysis accounting for business logic ▪ Powerful retrospective analysis of events
PT ISIM Overview Center	▪ Centralized management of PT ISIM sensors (updates, diagnostics) ▪ Consolidated information on confirmed cybersecurity incidents
PT ISIM View Point и PT ISIM Sensor	▪ Traffic analysis and incident detection in distributed, underloaded ICSs ▪ Initial traffic analysis is carried out with inexpensive, simple PT ISIM sensors placed at remote stations ▪ Traffic analysis results and visual data undergo high-level processing, centralized in the PT ISIM View Point console



PT ISIM Overview Center sensor control screen

PT ISIM netView Sensor compiled analytics screen

Additional external components

The following additional components can be used to connect PT ISIM sensors:

- A unidirectional diode that guarantees one-way transmission of data from the router SPAN port to the PT ISIM sensor
- An aggregating device, lowering the number of PT ISIM sensors needed to aggregate traffic from a series of router SPAN ports
- A regenerating unit, which replicates traffic from one SPAN port to other monitoring device ports
- A TAP device, which receives a copy of the traffic in the absence of a SPAN port

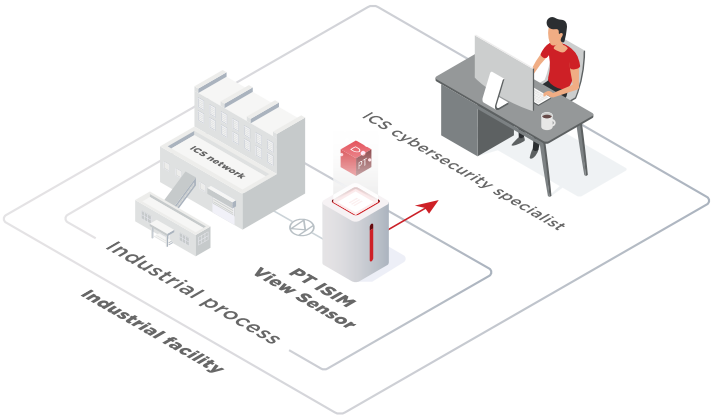
Sensor versions

Feature	PT ISIM Sensor	PT ISIM netView Sensor	PT ISIM proView Sensor
Safe and fast integration with ICS network	+	+	+
Incident management UI*	-	+	+
Automatic mapping of ICS network nodes	+	+	+
Automatic mapping of ICS network communications	+	+	+
Visualization of the ICS network scheme	+	+	+
Real-time monitoring of node connections to ICS network	+	+	+
Support for industrial protocols (DPI)	+	+	+
Event search and filtering tools	+	+	+
Detection of exploitation of vulnerabilities in ICS software and hardware	+	+	+
Network communication integrity control	+	+	+
Visualization of incidents on the ICS network scheme	+	+	+
Automatic generation of white lists of network connections	+	+	+
Automatic generation of white lists of network nodes	+	+	+
Control of white lists of network connections	+	+	+
Control of white lists of ICS network nodes	+	+	+
Logging and storage of ICS network traffic	+	+	+
Traffic and incident data export	+	+	+
Inventory of ICS network nodes	+	+	+
Retrospective event analysis	+	+	+
Detection of network anomalies	+	+	+
Automatic learning mode	+	+	+
Critical parameters control	-	-	+
Incident visualization on an industrial process scheme	-	-	+
Tools for creating and customizing own analysis rules	-	-	+
Tools for creating graphical mnemonic schemes	-	-	+
Export to external systems (for example, SIEM)	+	+	+
Integrated database of industrial cyberthreats PT ISTI	+	+	+
Export to PT ISIM Overview Center	+	+	+
Management via PT ISIM ViewPoint	up to 30 sensors	-	-

* PT ISIM Sensor does not include a user interface. PT ISIM View Point is needed to control and update this sensor type

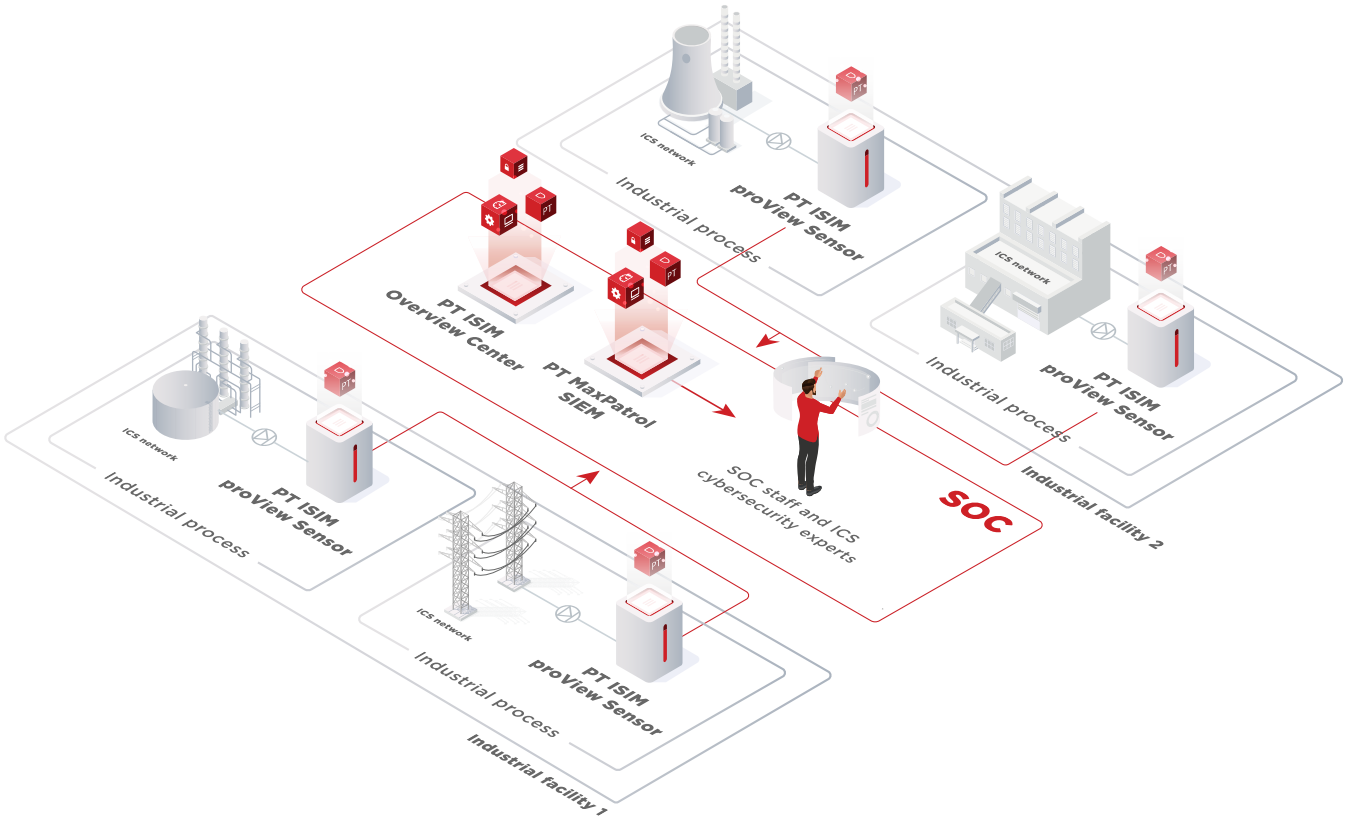
Sample scenarios

Scenario 1. Automatized management with minimal expense



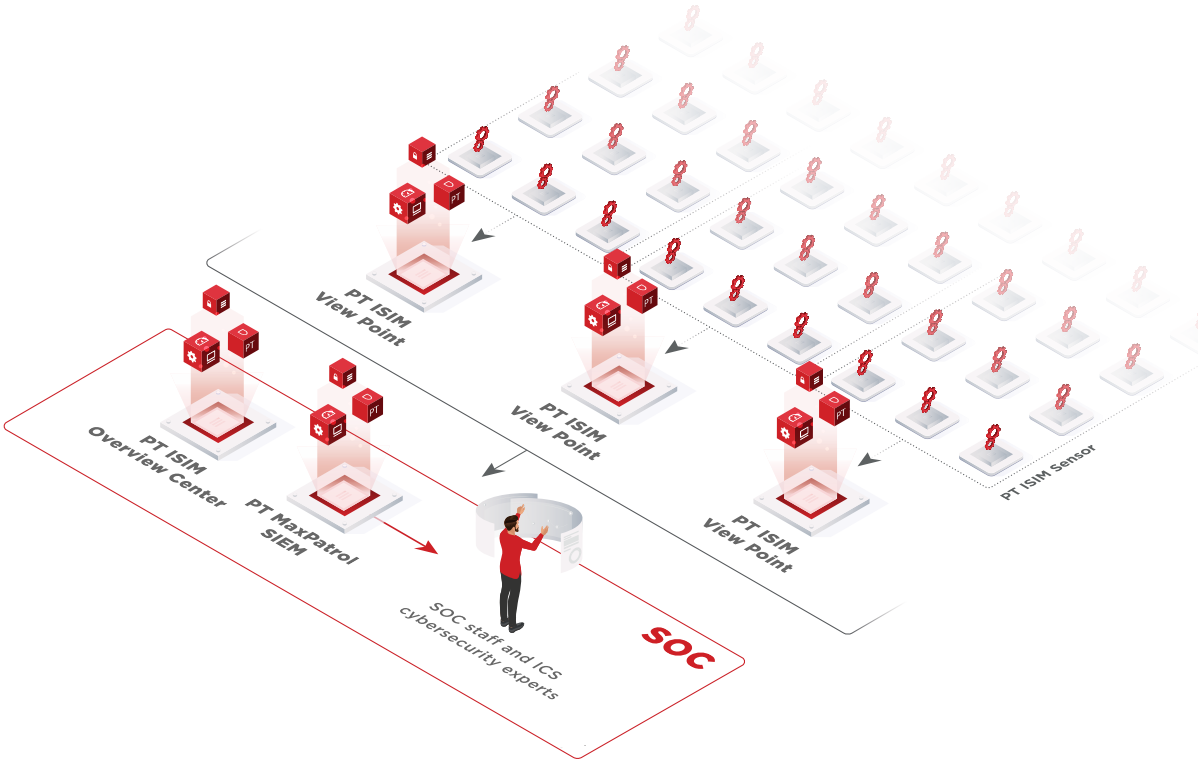
- A minimal set of components are installed on each defended platform (PT ISIM netView Sensor and, if necessary, a unidirectional data diode), allowing for the client's security specialists to conduct monitoring.
- No need for lengthy initial analyses of ICS networks and processes.
- Each sensor is managed individually.
- Minimal deployment, no specialist knowledge is required.
- Ideal for protecting small infrastructures as well as for gradual scaling of solutions at large facilities with distributed infrastructure.

Scenario 2. Maximal coverage and centralized management



- ICS components and segments must undergo a security analysis to optimize monitoring systems.
- With PT ISIM proView Sensor, attack vectors found in security analyses can be accounted for in monitoring system configurations. Security specialists can then react quickly and effectively against complex cyberattacks that are specific to their given ICS, including zero-day attacks.
- An SOC is organized to process incidents.
- PT ISIM Overview Center provides centralized management of PT ISIM components.
- Incidents are processed in the centralized SIEM system.

Scenario 3. Distributed infrastructure with a high proportion of underloaded segments



- Cost-efficient, compact PT ISIM Sensors without user interface are deployed in the networks of remote and underloaded ICS segments.
- PT ISIM View Point servers are deployed in consolidated areas and in SOCs, enabling sensor control and access to traffic analysis results.
- Incidents are processed in a centralized SIEM system.

Notes

Specification

	PT ISIM View Sensor	PT ISIM Overview Center	PT ISIM Sensor	PT ISIM View Point
CPU	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T	Intel Core™ i7-9700T, 2,0–4,3 GHz, 12M cache, 8C/8T	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T
RAM	2x16 Gb DDR4	2x16 Gb DDR4	16 Gb DDR4	2x16 Gb DDR4
Storage	2x480 GB SSD	2x480 GB SSD	1 TB M.2 SSD	2x480 GB SSD
Network connections	6x10/100/1000 Mbps, RJ45;	2x10/100/1000 Mbps, RJ45;	1 x 1Gb/s RJ-45 USB-Eth 1Gb/s external adapter (additional equipment)	2x10/100/1000 Mbps, RJ45;
Supply	1x220V AC	1x220V AC	1x 220V AC	1x220V AC

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.

PT ISIM DS_A4.ENG.0003.01