positive technologies

PT INDUSTRIAL CYBERSECURITY SUITE

INTEGRATED PLATFORM TO PROTECT INDUSTRIAL SYSTEMS FROM CYBERTHREATS

The degree of automation in industry is constantly increasing. The same IT components are employed in business management and on production lines. For attackers, there is no real difference between attacking the corporate network or the industrial control network. The attack methods and scenarios are identical in either case. However, industrial automation systems are often less protected than corporate IT systems. **PT Industrial Cybersecurity Suite** (PT ICS) can help bridge that gap.

PT ICS helps identify and respond to the early stages of an attack in an industrial environment. The platform provides comprehensive security for industrial systems, covering everything from network hosts to individual devices.

PT ICS combines multiple Positive Technologies products and services into a single, integrated security solution

Products: PT ISIM, MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, and MP EDR work in combination to provide thorough security coverage for the entire organization, including ICS/SCADA systems.

Services: A comprehensive package of both offensive and defensive services for ICS/SCADA systems, including OT security assessment, audit and compliance as well as incident response and investigations.

PT Industrial Cybersecurity Suite components

PT ISIM

performs deep analysis of ICS traffic with support for more than 130 network protocols. It provides threat unting tools, automatically identifies attack vectors, and carries out retrospective network analysis. PT ISIM reports identified threats to MaxPatrol SIEM.

MaxPatrol VM

for industrial systems provides vulnerability management for the entire organization. It analyzes automation network components, checks for vulnerabilities in them, and oversees the elimination of any discovered threats. MaxPatrol VM integrates with MaxPatrol SIEM, and both products are managed via a single interface.

MaxPatrol SIEM

for industrial systems is the cornerstone of the PT ICS platform. It monitors the activity of software applications and the behavior of users at network endpoints to identify security incidents, and provides tools to manage detected anomalies. MaxPatrol SIEM comes with out-of-the-box support for ICS/SCADA components from global manufacturers.

PT Sandbox

for industrial systems simulates the complete network nvironment, mirroring all software and deception mechanisms in order to discover unknown ICS/SCADA malware in files and links. All objects discovered by PT ISIM are sent to PT Sandbox for static and dynamic analysis.

MaxPatrol EDR

for industrial systems provides EDR agents that gather and analyze data from network endpoints to assist in hunting and neutralizing threats.

What you get

- **One solution for all industries:** O&G, power & utilities, transportation, metal & mining, manufacture, healthcare, constructions.
- **One ecosystem** for IT and OT infrastructures.

PT Industrial Cybersecurity Suite

3 SOCs **in the three largest oil and gas companies**

3 **mining enterprises and two steel mills**

One SOC in one of the largest steel mills

60+ **power stations**

Two SOCs in two energy companies

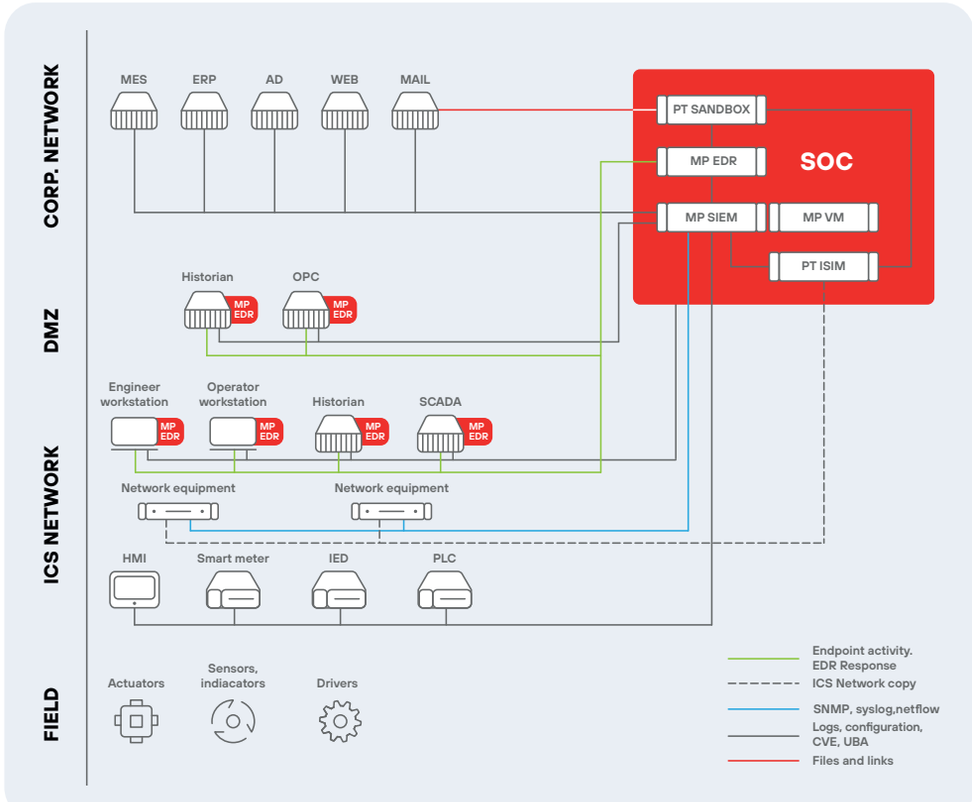
50+ **hydroelectricity plants**

Two SOCs in two powergenerating companies

30+ **220/110 kV substations**

Three SOCs in three electric grid companies

How it works



All products in the PT ICS platform are installed in the industrial control network. MaxPatrol SIEM gathers and analyzes ICS/SCADA component logs. MaxPatrol VM receives information about the ICS/SCADA network topology and identifies vulnerabilities. PT ISIM analyses industrial equipment network traffic. PT Sandbox analyzes files and links that are transmitted in emails and network traffic, and stored in network directories, and on ICS/SCADA network endpoints. MP EDR provides tools for automatic and selective responses to threats. All these tools work in unison to identify and eliminate threats at any stage of an attack.

Advantages

The first integrated platform to protect industrial systems from cyberthreats

The platform consists of five Positive Technologies products (PT ISIM, MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, and MP EDR agents) and includes an indepth audit of the ICS/SCADA system. PT ICS integrates these products into a single platform to provide comprehensive protection for your entire organization.

Attackers have nowhere to hide

Security systems built with PT ICS can detect attacks at any stage of execution and prevent business damage. In the event of an attack, the individual products that comprise PT ICS enable SOC analysts to determine what stage the attack is at and predict the attackers' next moves. PT Sandbox blocks malware in email, while MP EDR provides agents that enable a selective response to suspicious events on network endpoints.

Optimal implementation of security tools

PT ICS provides full coverage for both corporate and ICS/SCADA networks in a single platform. The audit included in the package enhances the SOC team's ability to detect and respond to threats, and reduces the overall number of security tools required in the system.

Fully autonomous

PT ICS is an entirely on-premise solution; all data is analyzed internally without ever leaving the enterprise network.

Learn more about

PT INDUSTRIAL CYBERSECURITY SUITE

Positive Technologies provides result-driven cybersecurity solutions, safeguarding businesses, governments, and global events like the Olympic games, FISU, and the FIFA World Cup from devastating attacks.

global.ptsecurity.com

info@ptsecurity.com