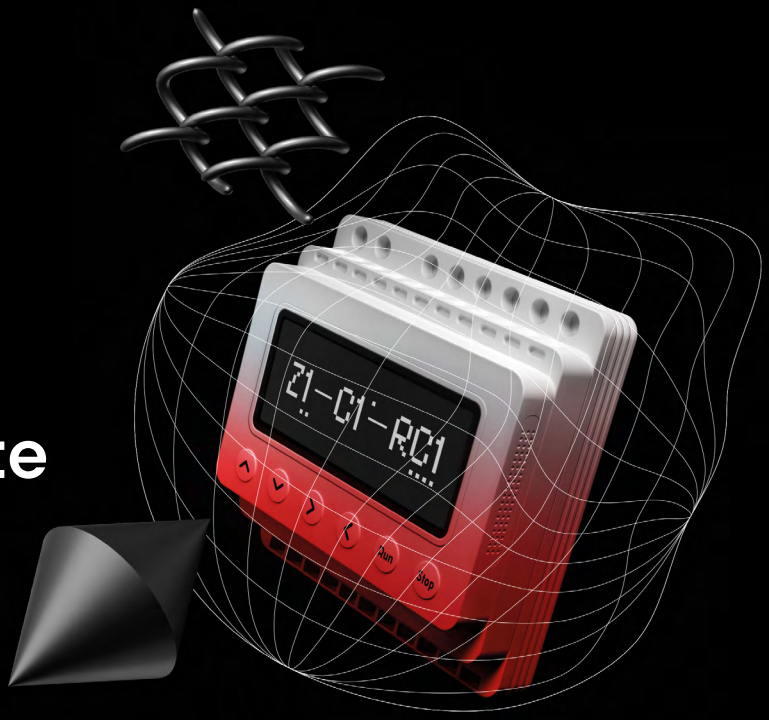
positive technologies

PT Industrial Cybersecurity Suite

The first integrated platform to protect industrial systems from cyberthreats



20% of attacks on industry bring production to a standstill

More than **80% of attacks** are carried out using malware

60% of manufacturing companies are unable to protect themselves from cyberattacks

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

- **Products:** MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox, and PT XDR work in combination to provide thorough security coverage for the entire organization, including ICS/SCADA systems.
- **Services:** A comprehensive package of services to analyze security measures in industrial systems, and PT ESC services to discover, investigate, and respond to complex incidents in ICS/SCADA systems.

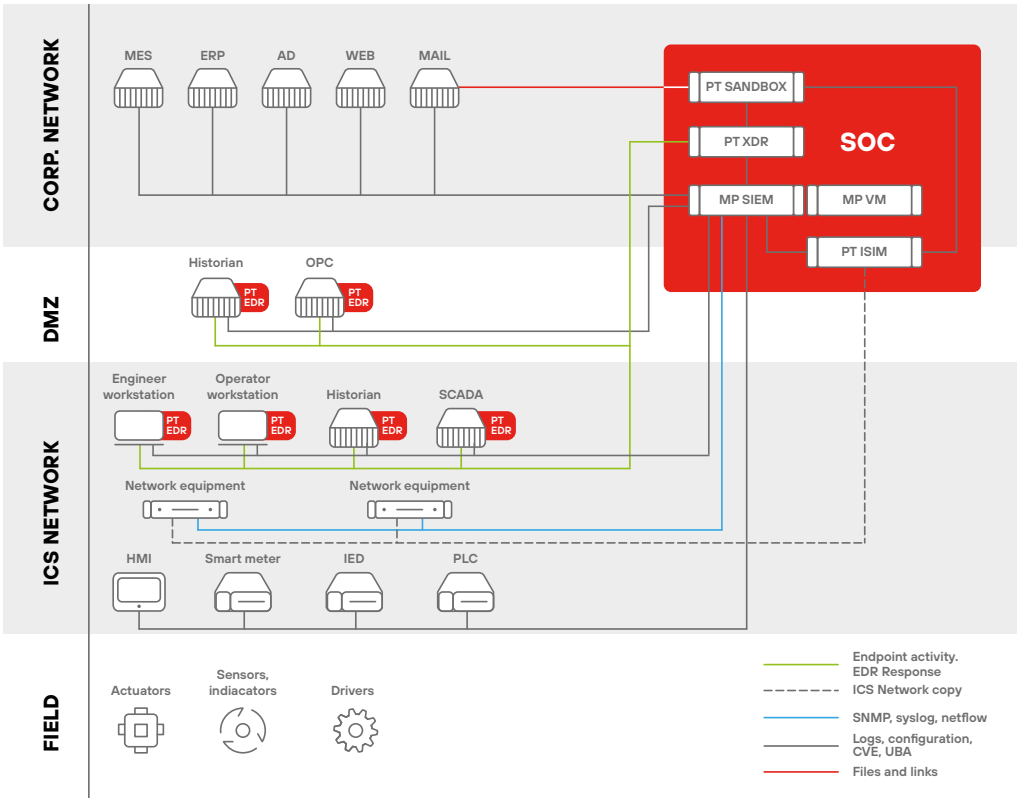
The solution

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 components

- **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.
- **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.
- **PT ISIM** performs deep analysis of ICS traffic with support for more than 120 network protocols. It provides threat hunting tools, automatically identifies attack vectors, and carries out retrospective network analysis. PT ISIM reports identified threats to MaxPatrol SIEM.
- **PT Sandbox** for industrial systems simulates the complete network environment, 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.
- **PT XDR** for industrial systems provides EDR agents specially adapted for operating in industrial environments. The EDR agents gather and analyze data from network endpoints to assist in hunting and neutralizing threats. PT XDR supports a wide range of popular operating systems. The EDR agents report suspected threats to PT Sandbox.

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. PT XDR 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 (MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox, and PT XDR EDR agents) and includes an in-depth 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 PT XDR provides EDR 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.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

Positive Technologies is a leading global provider of cybersecurity solutions. Over 2,300 organizations worldwide use technologies and services developed by our company. For more than 20 years, our mission has been to safeguard businesses and entire industries against the threat of cyberattacks.

Positive Technologies is the first and only cybersecurity company in Russia to go public on the Moscow Exchange (MOEX: POSI).

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