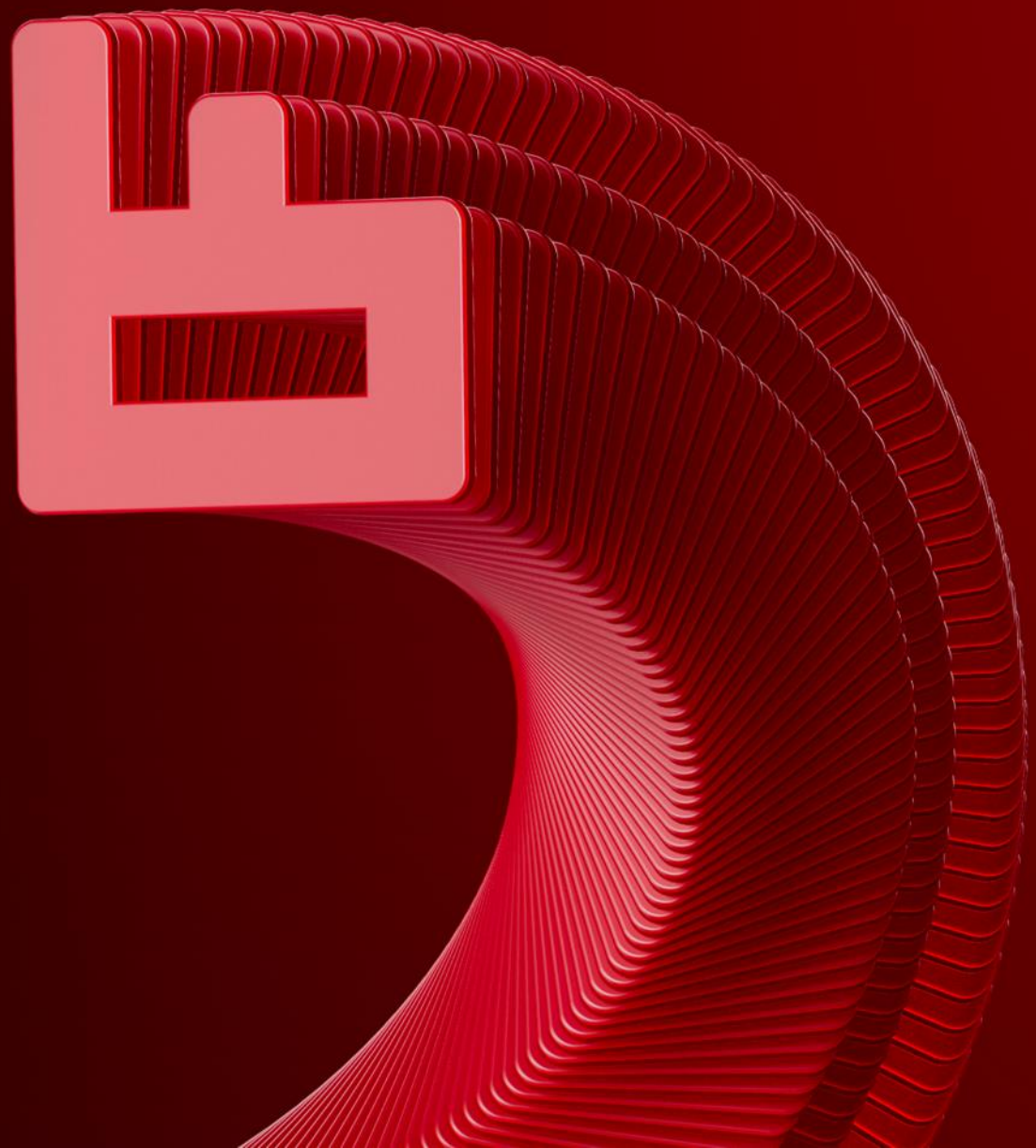
PT ISIM

Industrial Security Incident Manager



Practical cybersecurity solutions

20 years
of research
and development

2,000+ employees
including security engineers,
developers, analysts,
and other specialists

250+ experts
at our security
research center

200+
zero-day vulnerabilities
discovered
every year

250+
corporate
security audits
annually

50%
of all industrial and
telecom vulnerabilities
were discovered by our experts

- Products and solutions
- Security audits
- Incident investigation
- Threat research

More than 20 publications every year

- Quarterly reports on current cyberthreats and trends
- Forecasts
- Investigations into hacker group activities
- Industry-specific research

Analytical articles

Positive Technologies in industry

Oil and gas	SOCs in the top three oil and gas companies
Metallurgy	Three mining companies and two steel mills SOC at a major steel mill
Traditional generation	More than 60 power stations SOCs at two energy companies
Hydroelectric generation	More than 30 hydroelectric power stations SOCs at two generation companies
Electrical grids	More than 20 220/110 kW substations SOCs at three grid companies
Non-industrial engineering systems	Data center at a national telecom provider Large sports venue
Transport	More than 100 rail transport infrastructure facilities across the country

Industrial infrastructure vulnerabilities

Positive Technologies research shows an average of one to five major irregularities at industrial facilities:

- Off-design workstations with internet access
- Unsecured access points
- Remote access to the industrial network
- Unauthorized communication channels
- Lack of network segmentation and parasitic traffic
- Use of default passwords

Every irregularity carries cybersecurity risks

Some statistics from Positive Technologies

10%

of all successful cyber attacks in 2022 targeted industrial companies

96%

used social engineering and spread malware to gain access to the infrastructure

74%

of attacks are targeted campaigns, focusing on particular companies

in **57%**

attacks malware were used

34%

Of successful attacks used ransomware

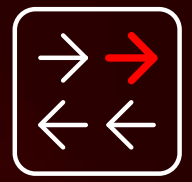
11%

companies’ CISO claim they can resist the attacks

Endpoint and perimeter protection isn't enough

Due to limited hardware resources, outdated operating systems, and proprietary technologies,

information security tools can't be installed on all devices



Inventory and tracking changes in large industrial ITinfrastructures are highly complex tasks

Enterprises aren't always aware of their assets

A large volume of communications remains within the OT network and doesn't pass through the firewall

Threats also need to be detected in network traffic

What's the solution?

Network Traffic Analysis (NTA)

NTA solutions focus on detecting attackers inside the network

They analyze traffic in detail and save an initial copy, allowing security teams to investigate incidents and reconstruct attack chains.

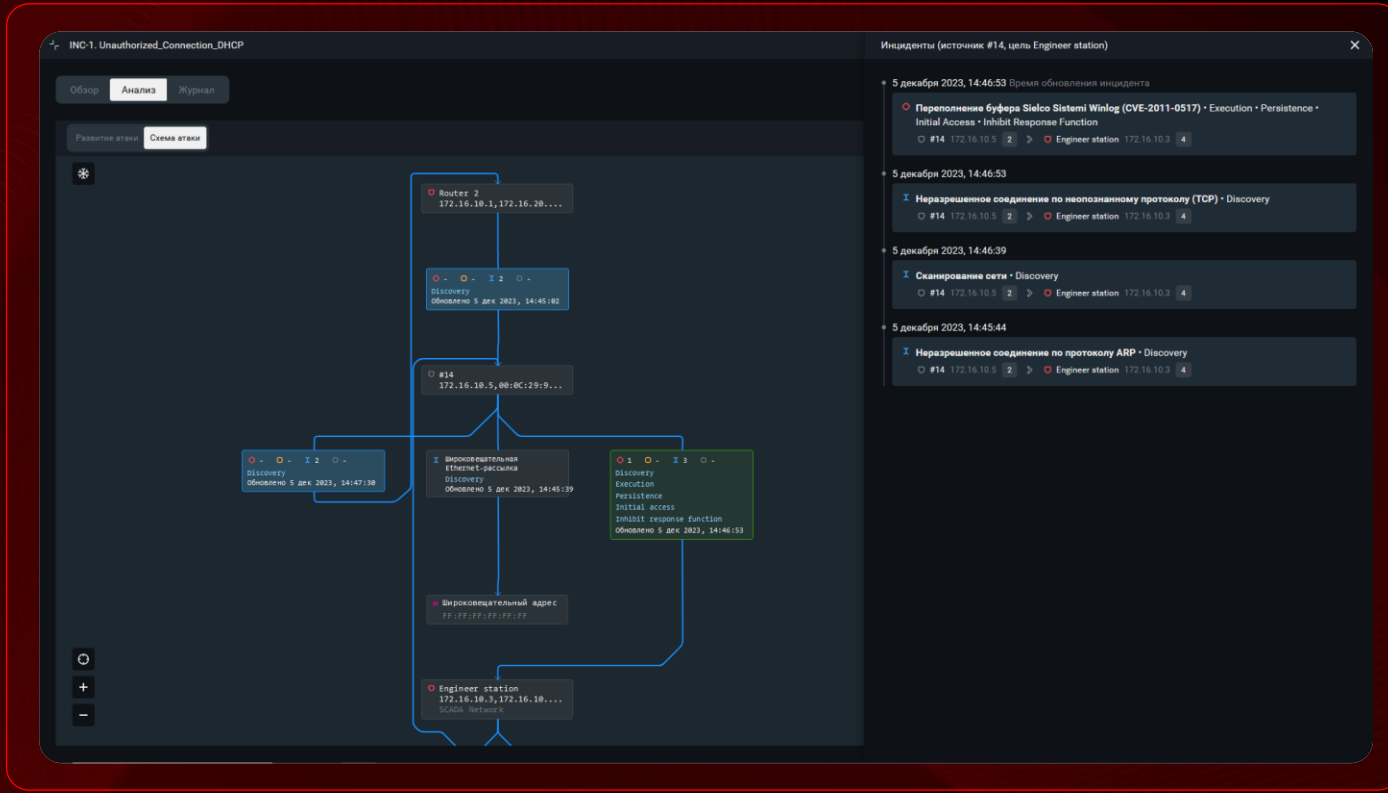
Without NTA, infosec specialists and IT administrators can't see security events in the industrial network

PT ISIM is your main tool to ensure the cyberresilience of industrial infrastructures

Industrial NTA

- Analyzes network-wide and industrial protocols on the perimeter and in the network.
- Detects attacks and potentially harmful actions.
- Provides information to investigate incidents

PT ISIM controls OT network security and helps detect cyberthreats to prevent damage to companies before it's too late



PT ISIM capabilities

OT network observability and change control

for greater infrastructural cyber resilience

- Provides OT infrastructure inventory and change control
- Detects dangerous process control commands

Security monitoring

to prevent dangerous process disruptions

- Detects OT traffic anomalies and security events
- Detects malware and forwards suspicious files for analysis

Threat detection and analysis

to protect the network and maintain industrial and business continuity

- Detects vulnerability exploitation and other malicious techniques
- Helps compliance

Who benefits from PT ISIM

Information security officers

Helps protect the company's critical infrastructure from current cyberthreats.

IT infrastructure maintenance officers

Helps ensure stable operation of the entire corporate IT infrastructure

Production continuity officers

Helps prevent emergencies and production stoppages

Applications

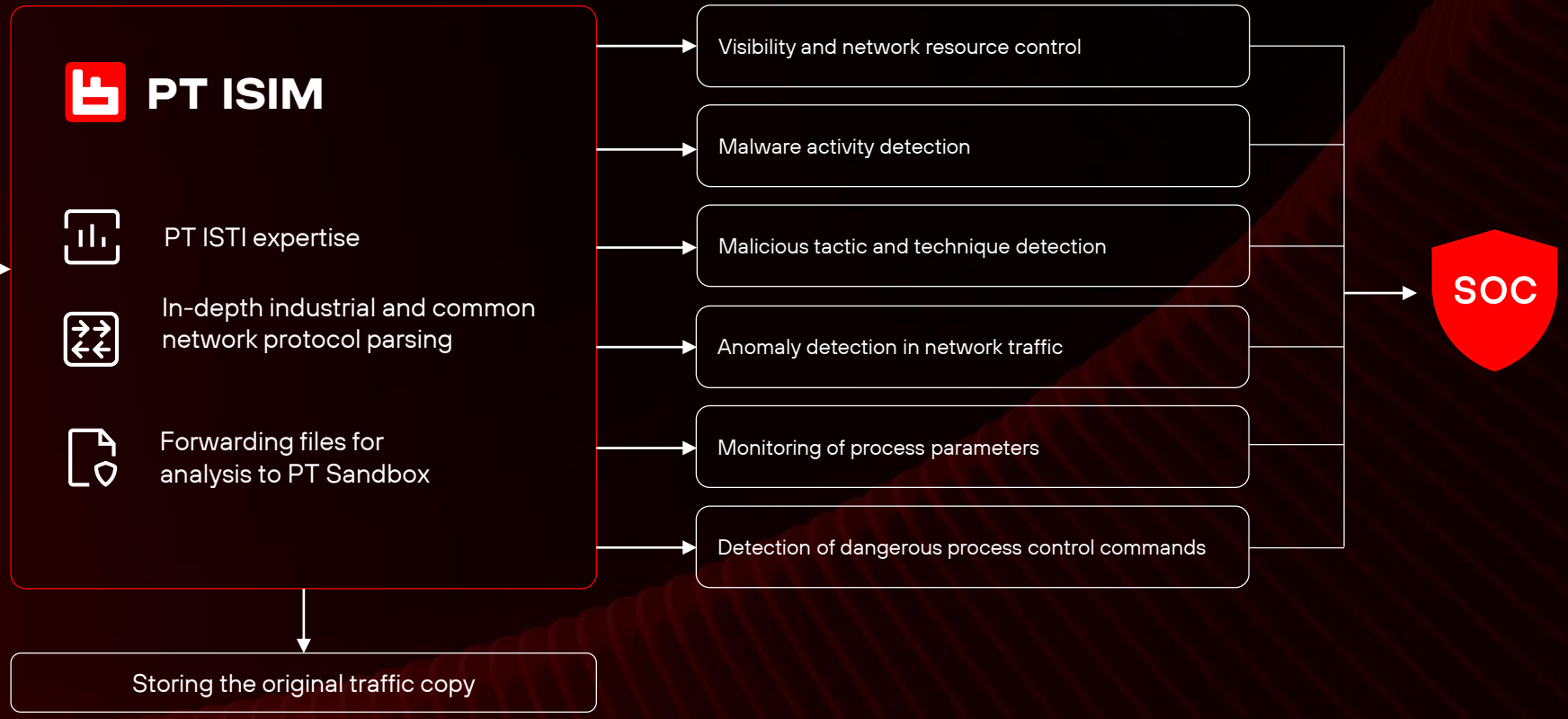
- Automated ICSs
- City and municipal utility infrastructure management systems
- Rail traffic control systems
- Distributed industrial infrastructure control systems
- Industrial Internet of Things systems
- DICOM-compatible systems and medical networks

How PT ISIM works

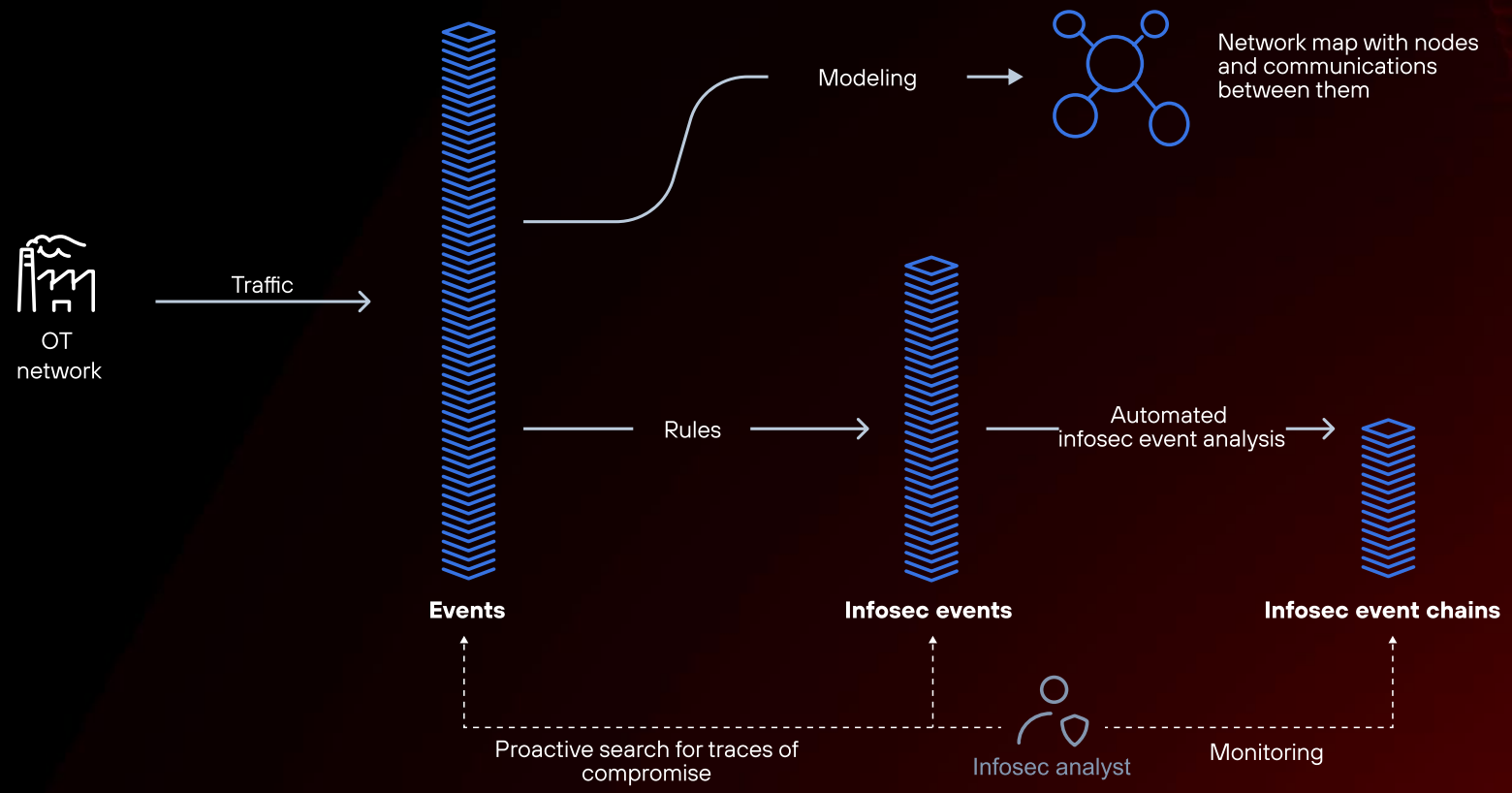
PT ISIM captures and parses network traffic (130+ protocols)

Traffic from the switch SPAN port

PT ISTI expertise helps with early detection of attacks on Windows and Linux, standard network equipment, and industrial devices. More than 8,000 rules and threat indicators



Traffic processing algorithm



1. A sensor collects traffic from the switch SPAN port. The initial copy of traffic is stored on the server in PCAP format

2. Normalized and filtered messages are checked for compliance with correlation rules

3. If a rule is triggered, an information security event is logged. Linked events are combined into chains for ease of investigation

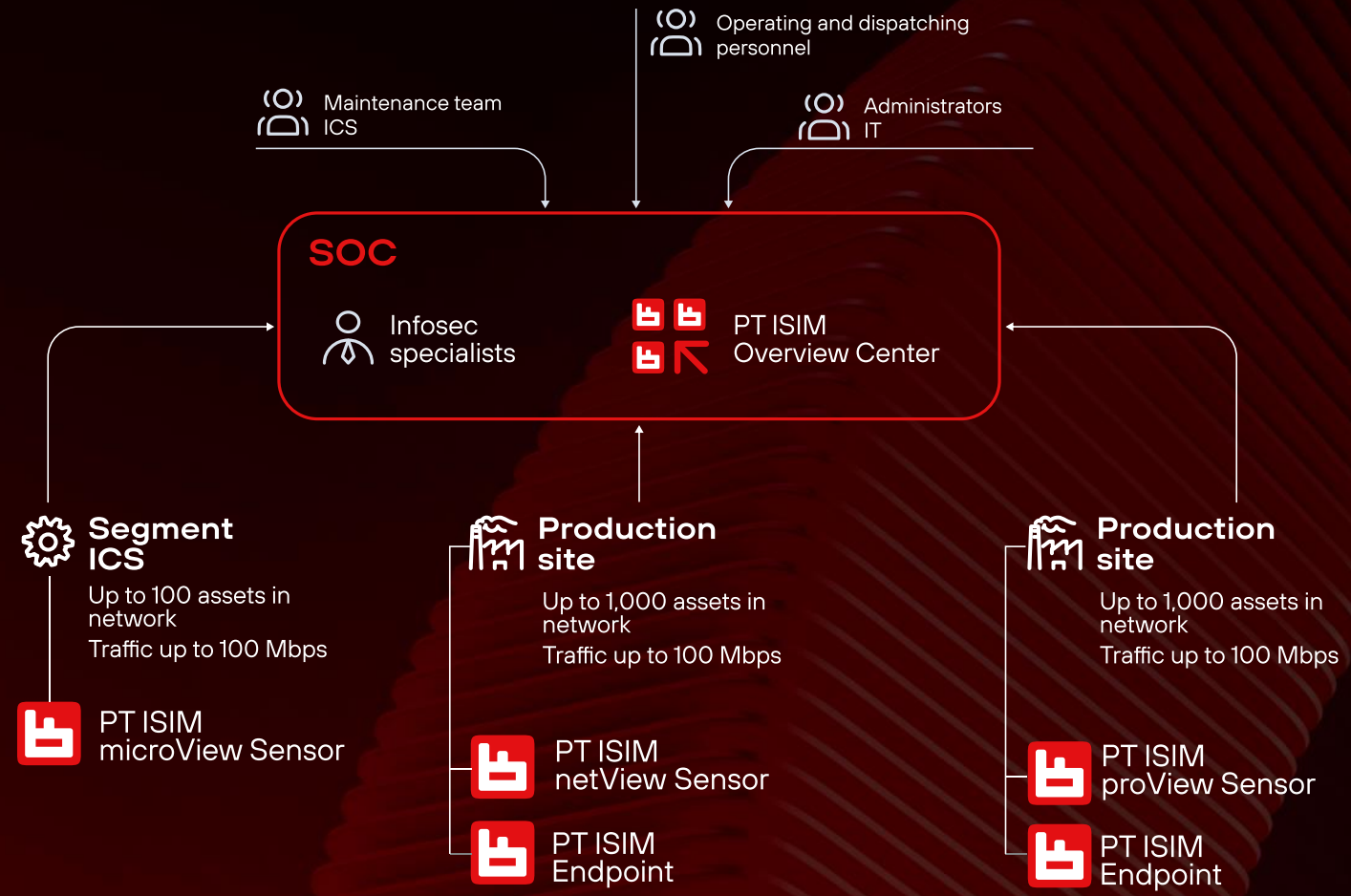
PT ISIM components

PT ISIM View Sensor

Installed at the level of the ICS network that hosts operator workstations and SCADA and PLC servers, PT ISIM View Sensors analyze and store network traffic.

PT ISIM Overview Center

Installed at SOCs or data centers, Overview Center is a management console that collects events from subordinate sensors and provides centralized configuration and update.

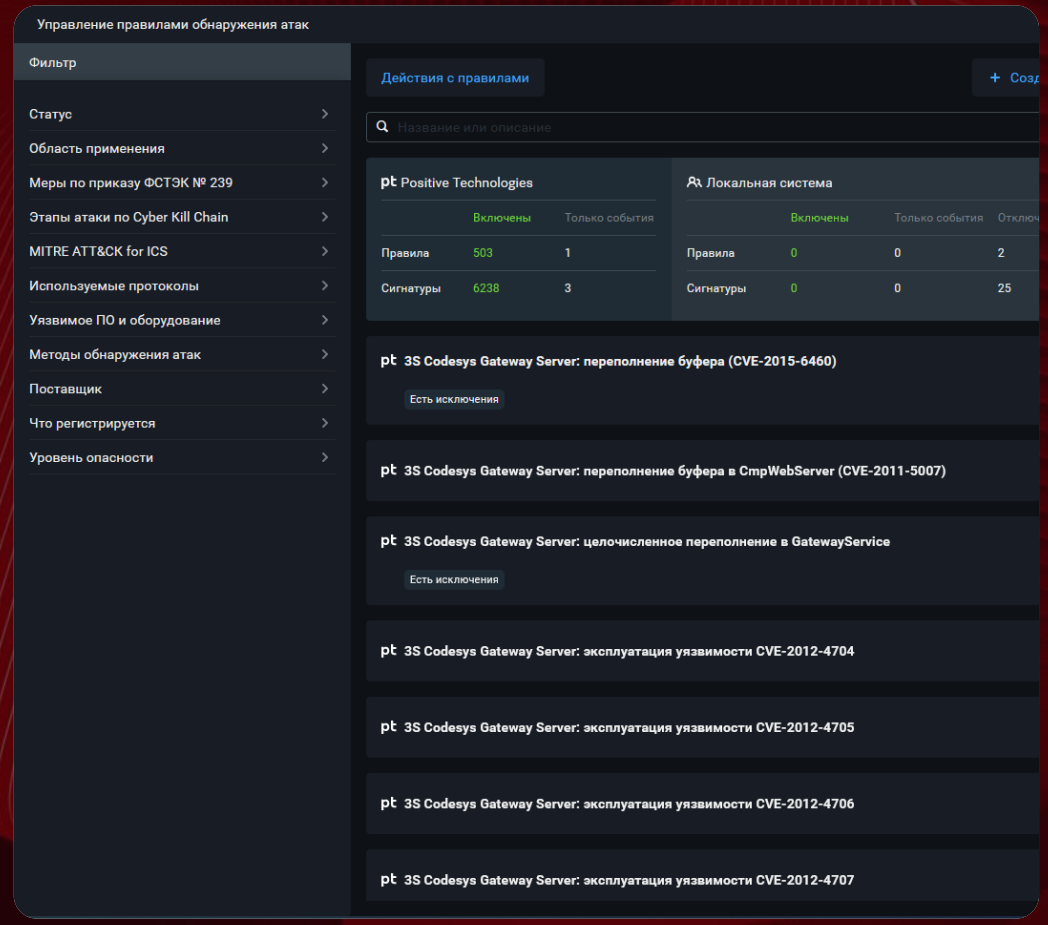


Technology expertise

8,000+

out-of-the-box industrial rules and threat indicators

Cover industrial software and hardware in Windows and Linux-powered infrastructures



Advantages of PT ISIM

1

Versatile product applicable to all major industries, IIoT, and medicine

PT ISIM parses more than 130 industrial and common network protocols, so it can be used in:

- Any industry: from heavy industry to engineering infrastructure facility management
- Industrial Internet of Things (IIoT) systems
- Intelligent medical systems transmitting data by the DICOM protocol

Advantages of PT ISIM

2

Engages all of an organization's technical departments in managing the security of business-critical systems

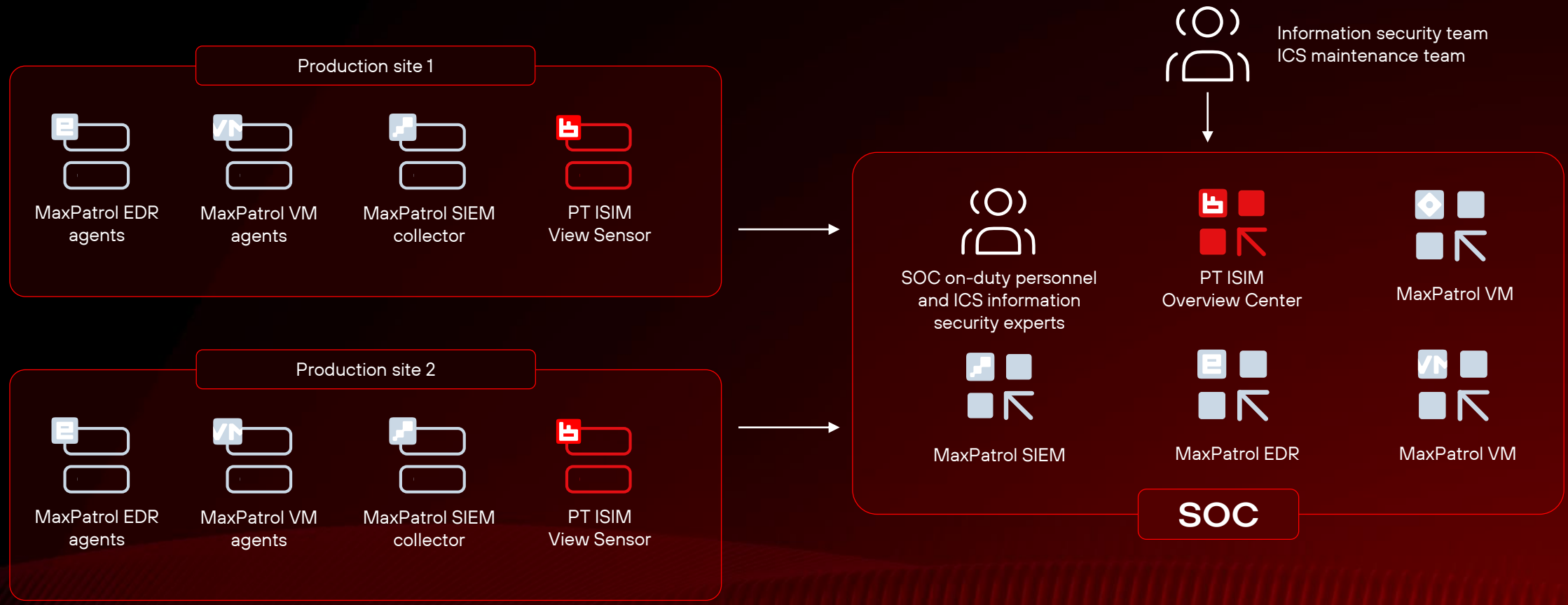
PT ISIM isn't just for infosec specialists. It provides a broad range of information and has tools for all of an organization's different technical departments:

- IT administrators
- ICS maintenance team
- Operators and dispatchers

PT ISIM is a component of PT ICS

PT ISIM	In-depth traffic analysis in industrial IT infrastructures, IIoT environments, and DICOM systems and networks
MaxPatrol SIEM	Collection and analysis of security events at the ICS application level: SCADA servers, controllers, and workstations.
MaxPatrol VM	Detection of vulnerabilities in industrial systems and remediation management
PT Sandbox	Behavioral analysis of files extracted by PT ISIM from network traffic and forwarded by MaxPatrol EDR from hosts
MaxPatrol EDR	Detection of targeted and complex threats at endpoints

Synergy of PT ICS component products



PT ISIM over time

PT ISIM 5.0

Endpoint security monitoring and a new interface

- Security monitoring on SCADA servers and workstation systems
- Collection of software security events
- Monitoring of process signals
- Updated dashboards and network scheme

Q2 2024 | Q3 2024 | Q4 2024 | Q1 2025 | Q2 2025 | Q3 2025 | Q4 2025

PT ISIM 4.5

New benefits for distributed production structures and MSSP

- Role-based model and multitenancy
- Single Sign-on (SSO) through the MaxPatrol platform
- PT ISTI updates through Overview Center

PT ISIM 5.* — 2025

Inventory and monitoring of OT network configurations

- Network inventory
- Incident response
- Vulnerability management

PT ISIM
Page on
ptsecurity.com

PT ICS
Join the PT ISIMTelegram
channel

Thank you!