



Industrial Cybersecurity (PT ICS)

By Positive Technologies



**Operational Technology,
exists practically in every industry
in some way or another**

**and OT needs to be
protected**

**Perhaps the OT needs it
above all!**

Agenda:

1. Russian regulation for OT Security
2. Threats are both external & internal
3. PT ICS – our portfolio for OT Security
4. References

1. Russian regulation for OT Security

CII / Critical Information Infrastructure



Federal Law #187-FZ

SETS THE RULES AND OBLIGATIONS FOR COMPANIES TO ASSESS AND **CATEGORIZE IT & OT** INFRASTRUCTURES (SIGNIFICANT CATEGORY #1, #2, #3 OR NON-SIGNIFICANT)

Executive Order 127-PP and FSTEC FORM #236

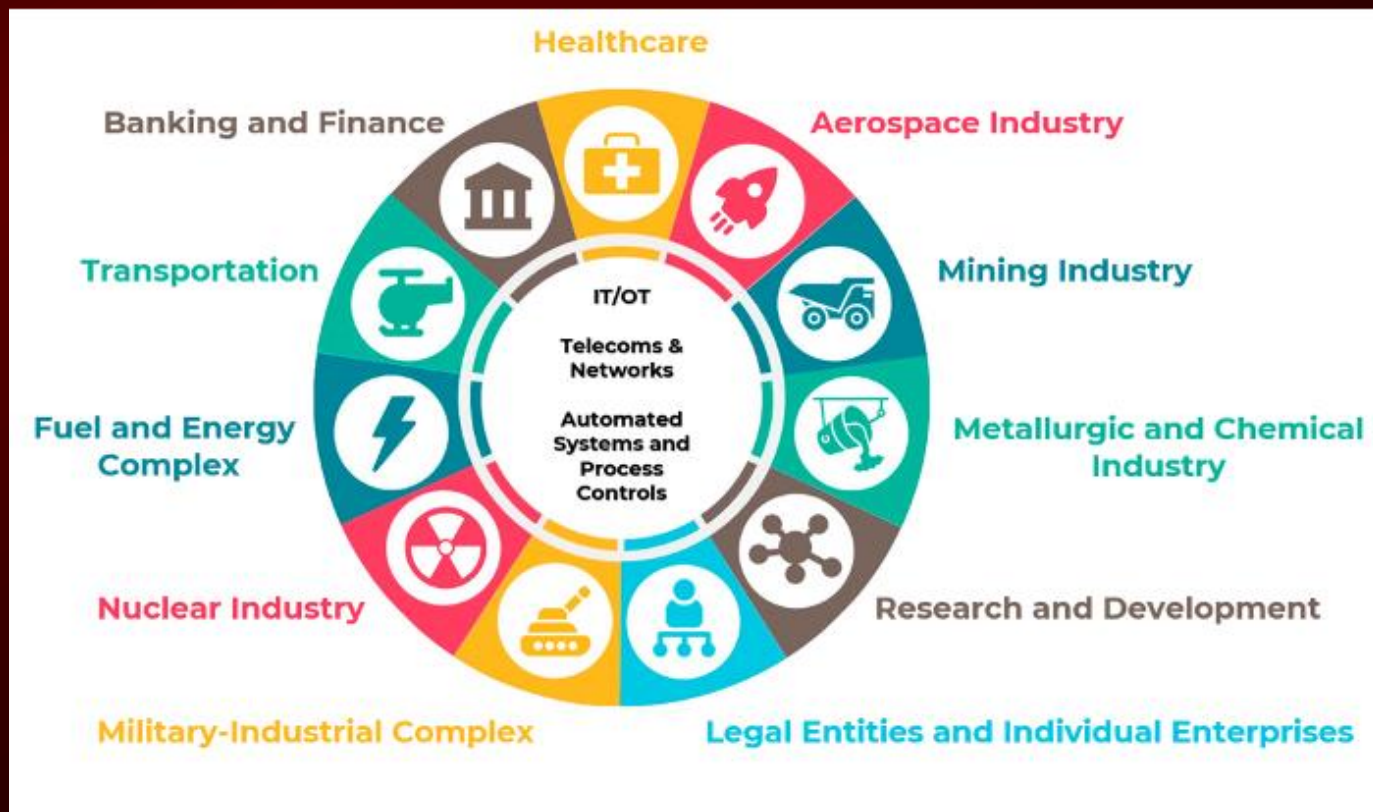
THE RULES HOW TO ASSESS THE SYSTEMS AND WHAT TO CONSIDER TO CHOOSE CATEGORY.

FSTEC ORDER #239

LIST OF CONTROLS AND MEASURES THAT MUST BE DEPLOYED BY CRITICAL INFRASTRUCTURE OWNER, FOR EACH CATEGORY (SIGNIFICANT CATEGORY #1, #2, #3)

Cyber Security with the only goal to prove compliance with this regulations is "paper" security

CII / Critical Information Infrastructure



Согласовано
Заместитель директора
Федеральной службы
по техническому
и экспортному контролю

В.С. Лютин
В.С. Лютин

Утверждено

Заместитель Министра
промышленности
и торговли Российской Федерации

СЕРИЯ ДН № 00000000000000000000

Сертификат: 01044330200

СОГЛАСОВАНО Заместителя директора Федеральной службы по техническому и экспортному контролю		УТВЕРЖДЕНО Заместителя Министра промышленности и торговли Российской Федерации	
 В.С.Лутин		 В.В.Шин	
+21+ января 2024 г.		+21+ января 2024 г.	
ПЕРЕЧЕНЬ типовых объектов критической информационной инфраструктуры Российской Федерации, финансируемых в области металлургической промышленности			
№ п/п	Наименование типового объекта критической информационной инфраструктуры (ИИС, ИТКС, АСУ)	Осуществляемые критические процессы типовых отраслевых объектов КИИ	ОКЕИД
1	Система управления технологическим процессом подготовки сырья	Выполнение работ по разведке и добыче; Выполнение работ по производству металлов.	22.10 Деятельность по извлечению и обогащению 20.10 Производство промышленных газов 20.10 Производство чугуна, стали и ферросплавов 24.10.1 Производство основных чугунов из жидкого чугуна 24.10.11 Производство чугуна 24.10.12 Производство ферросплавов 24.10.13 Производство чугуна проката 24.10.14 Производство стали в грубой и чистой форме
2	Система управления технологическим процессом хранения сырья или продукции	Обеспечение хранения металлов, сырья или продуктов, требующих особых условий хранения и транспортировки в условиях металлов, производство чугуна (жидкого), производство и выделение металлов, извращение и выделение металлов, извращение сталей, из	

For key industries there is a comprehensive list of typical systems that must be classified as critical in T&D, power generation, chemical, O&G, metal & mining and other industries. They are maintained by Ministry of Energy and Ministry of Industry of Russia

Our industrial installed base



Oil and gas



Three SOC in the **three** largest oil and gas companies

Metal & mining



Three mining enterprises and **two** steel mills
One SOC in one of the largest steel mills

Power generation



60+ power stations
Two SOC in **two** energy companies

Hydropower



30+ hydroelectricity plants
Two SOC in **two** power-generating companies

T&D



20+ 220/110 kV substations
Three SOC in **three** electric grid companies

Non-industrial facilities



One data center in a national telecom provider
One large sports arena

Transportation

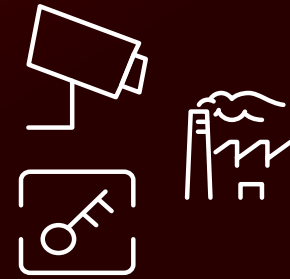


100+ railway stations across the country

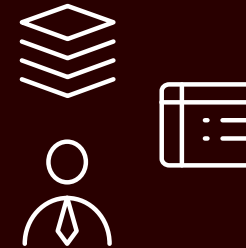
Measures and Controls

FSTEC Order #239 – mandate:

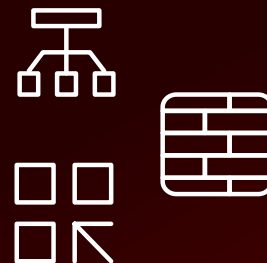
- ✓ A list of **BASIC** measures and controls for Significant Systems of CII (i.e. firewall, backup, EPP/anti-virus, IPS, SIEM, VM etc.)
- ✓ They are *necessary* but not always *sufficient* for particular company
- ✓ Real measures can be derived from practical threat model with consideration of **non-tolerable events** (or *negative consequences* developed by FSTEC)



**Physical
controls**



**Administrative
controls**



**Technical
controls**

2. Threats are both external & internal

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

Securing perimeter is not enough



HOW FAST

2 days

to penetrate into the perimeter based on our pentests

30 mins

record time to hack the perimeter

HOW LONG

200 days

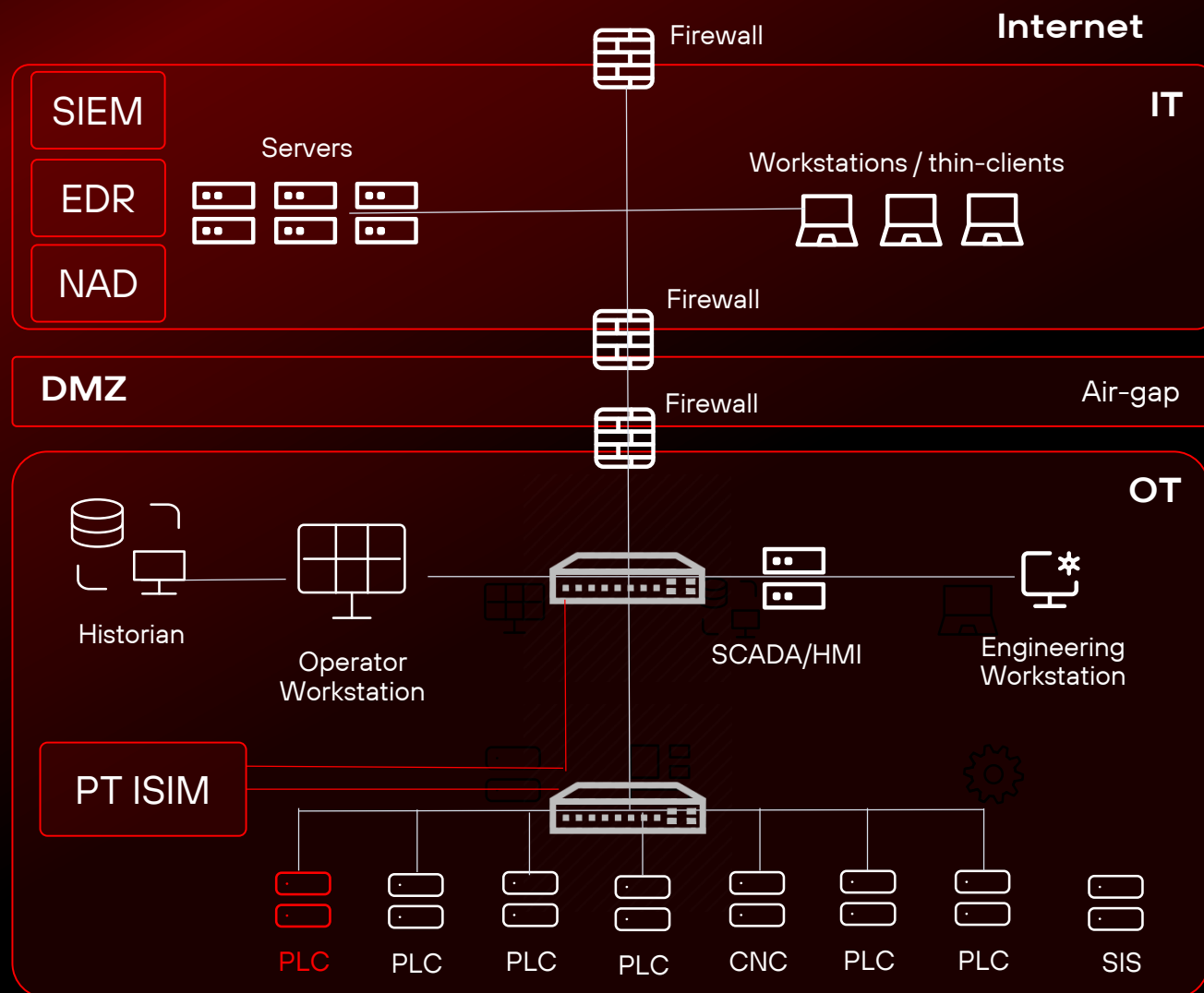
2000–2022

In average the hacker stays unseen (based on our researches)

11 years

record time to stay inside the infrastructure

Challenges in OT



Weak and default passwords

Lack of network segmentation

Outdated software and firmware

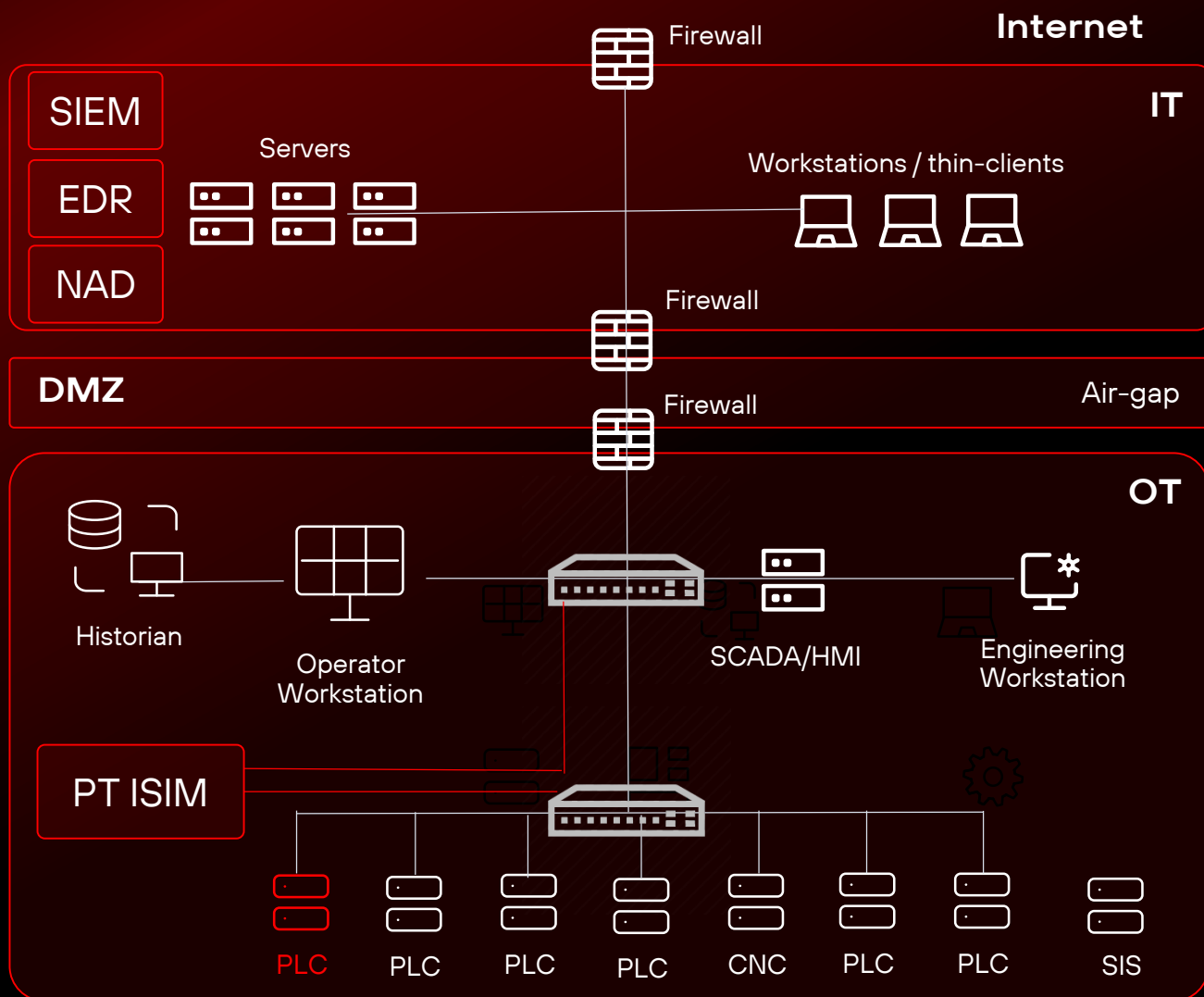
Hidden IT assets (computers, networks)

Limited changes in maintenance windows

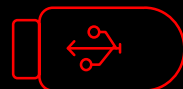
Dependency on OEM / vendors

HR: skills, resources, workforce

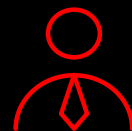
Who's got access to OT network?



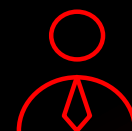
Hackers, hacktivists or APT groups?



Unauthorized 3G modems?



Your own personnel with legitimate access?



3rd parties (OEM, contractors) with remote and legitimate access?

A few examples of real incidents



Threats are not only hackers and ransomware

Oil refinery

Defueling from a reservoir large amount of petrol.

Evidence of the fraud were cleaned up in the SCADA logs

Financial losses

Nuclear power plant

Several types of malware were detected **in the network** traffic of a fully air-gapped radiation monitoring system

Potential deny of service with unpredictable consequences

Household waste processing center

Illegal delivery of household waste. Access to waste control system. Unauthorized unloading of waste

Financial losses

Oil pipeline system

Theft of unaccounted volumes of crude oil from the pipeline system. Decanting oil to sell it on the black market

Financial losses

Iron and steel works

An employee switched off SIS and remotely manipulated a trestle crane. As a result - one man found dead.

**Financial losses
Occupational fatality**

OT security monitoring



Positive Technologies expertise in PT ICS

	PLC	Network devices	Work-stations	Servers
Application layer				
User operations layer	Operations and Control			
	Configuration			
	Maintenance			
	Admin			
Application software layer	PLC project	Config files	Communication software	
			Engineering software	
			SCADA software	
			PLC project	
System layer	Firmware	Firmware	OS RDBMS	OS RDBMS Virtualization Domain Controller
Network layer		Traffic NetFlow		

Dangerous commands and control operations
Suspicious service commands and operations
PLC and SCADA project changes
Historian data modification or deletion
Manipulation with SCADA user settings
Suppression of traces of illegitimate actions

**Complete
OT security monitoring
with PT ICS**

Malware detection
Intrusion detection
Privilege escalation detection
Network anomaly detection
System configuration change detection

**Common IT &
security monitoring**

Key points:

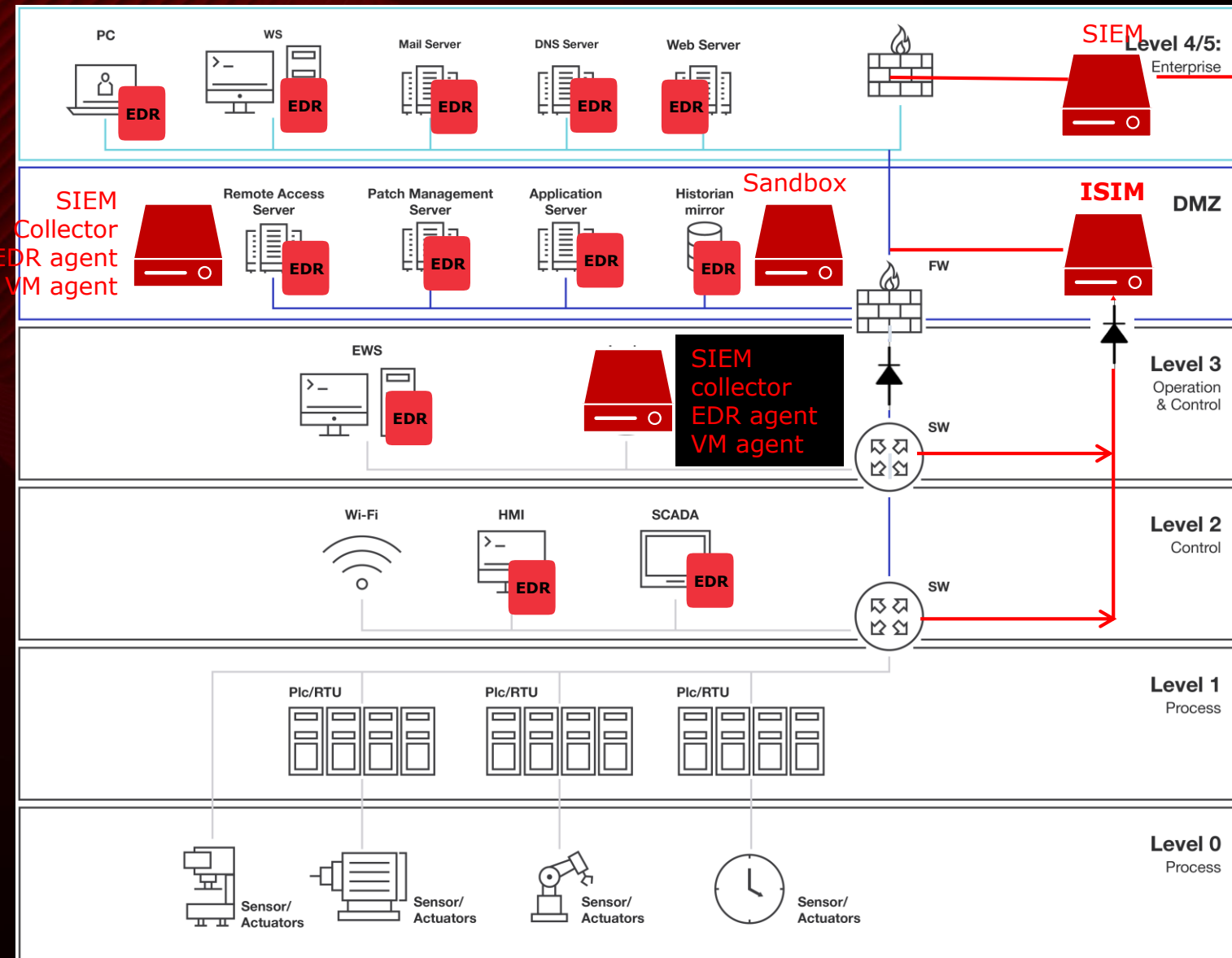


Architecture with 1 data diode

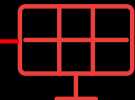


Key points:

- ISIM does not need agents, it's standalone and independent NTA
- ISIM receives just a copy of the OT traffic (from SPAN)
- ISIM installed in the IT network or in the DMZ
- From the OT network to ISIM the SPAN traffic is forwarded via a data diode
- ISIM has full visibility of the OT traffic yet stays accessible from the SOC



SOC



Security workstations



Incident management



Asset management, vulnerability and patch management



24/7



IT & OT

3. PT ICS – our portfolio for OT Security

PT Industrial Cybersecurity Suite



Comprehensive solution for OT security:



- **PT ISIM:** traffic analysis (NTA) and threat detection in ICS (OT) networks
- **MaxPatrol SIEM:** monitors information security in large hierarchical infrastructures + industrial content
- **MaxPatrol VM:** security asset management and vulnerability management process + industrial content
- **MaxPatrol EDR:** autonomous host agent to detect complex and targeted attacks
- **PT Sandbox:** network sandbox for detecting complex targeted malware attacks + industrial content



One for all industries: O&G, power & utilities, transportation, metal & mining, manufacture, healthcare, buildings



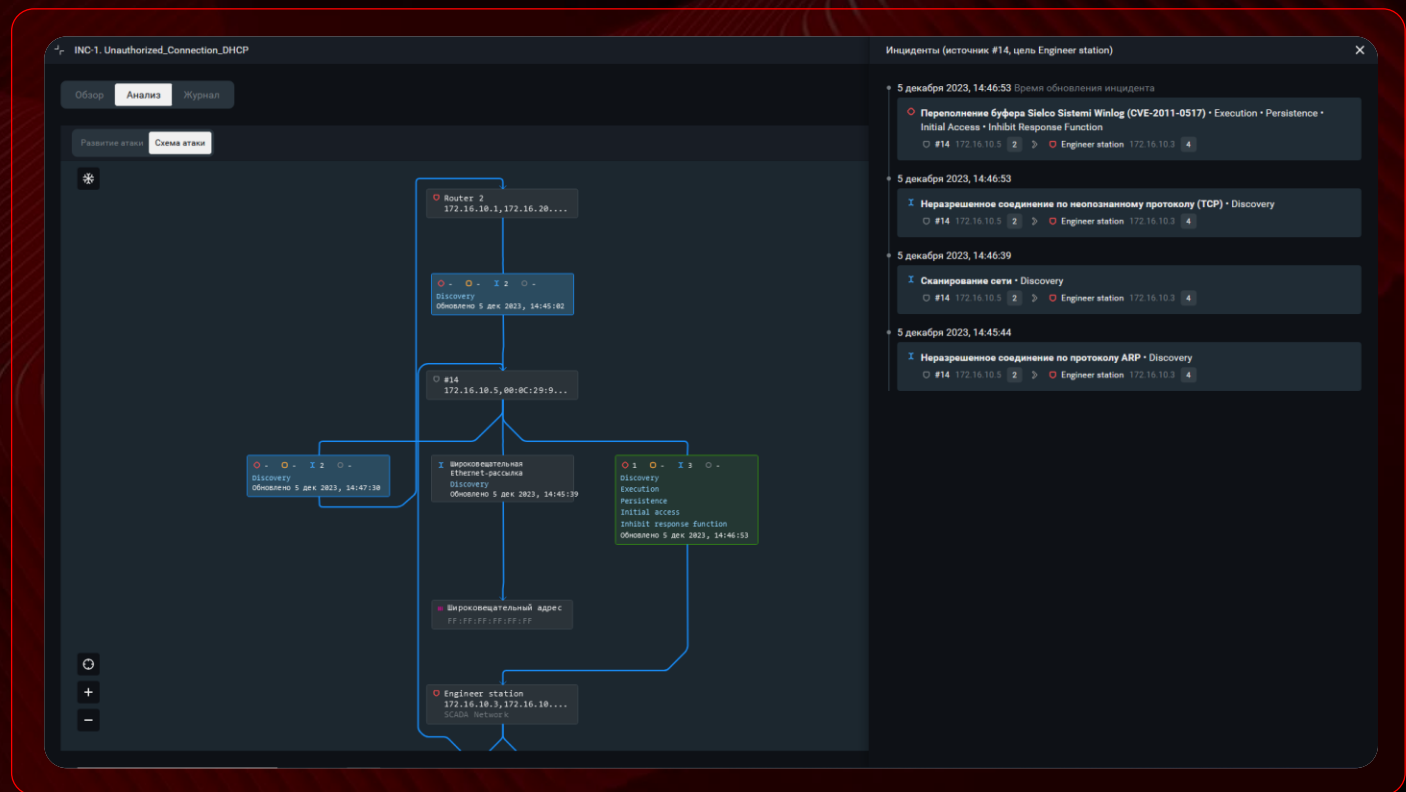
Single products ecosystem
for securing both IT and OT infrastructures

PT ISIM – the key solution for OT resilience through continuous monitoring

PT ISIM — OT traffic analysis (NTA)

- DPI for common & industrial network traffic inside the OT perimeter
- Detects threats, malware and dangerous control commands
- Accumulates raw data for forensic and investigation

**Continuous monitoring,
threat analysis and
control of OT infra**



CISA & NSA Top-10 Cybersecurity Misconfigurations*



1. Default config of software and apps
2. Improper separation of user/admin privileges
3. **Insufficient internal network monitoring**
4. Lack of network segmentation
5. Poor patch management
- ...

Any corporate network is **vulnerable** to attacks, even if the perimeter is well secured.

The actions of an attacker who has already penetrated the perimeter and is "noisy" in the network **are not usually visible to perimeter protection tools** (firewalls and IDS)

It is vital to control **both external and internal traffic**

PT ISIM – key component in OT ^{pt}



> Know Your Infrastructure:

- (**asset management**), visibility of the OT infrastructure
- (**security monitoring**), anomaly and threat detection
- (**control**), threat analysis and investigation

CISO

Secure critical infrastructure
Cybersecurity Resilience Aspects

CIO/IT

Resilience of IT&OT
infrastructure

CTO/OT

Assure resilient operations.
Business Continuity
Management

PT ISIM – off-the-shelf product

with rich expertise

PT ISIM analyzes OT traffic (130+ protocols)

SPAN-port

Database "PT ISTI" inside PT ISIM includes more than 8000 rules, signatures and treat indicators for 130+ network protocols. Updated regularly



PT ISIM



Expertise (PT ISTI)



DPI for industrial and common network protocols



File extraction for analysis in PT Sandbox

Raw traffic storage

Visibility and integrity control (new assets)

Malware detection

Hacker tactics and technics detection

Network anomalies detection

Operational parameters monitoring

Dangerous OT commands detection

SOC

MaxPatrol SIEM & SCADA software



SIEM that does work in OT environments

Detects incidents with a unique approach that keeps IT infrastructure transparent and leverages deep expertise to discover threats.

Can be deployed in OT segment to collect events from SCADA.

Technological expertise cases

- Remote SCADA management
- An attacker reprograms a PLC
- An attacker spoofs a SCADA project
- An attacker logs in to SCADA and can send commands from it
- An attacker makes a PLC unavailable for operators
- An attacker spoofs data seen by SCADA
- An attacker makes SCADA unavailable for operators
- An attacker steals data from SCADA

[Product booklet](#)

7 packs

of industrial expertise is already available for MaxPatrol SIEM

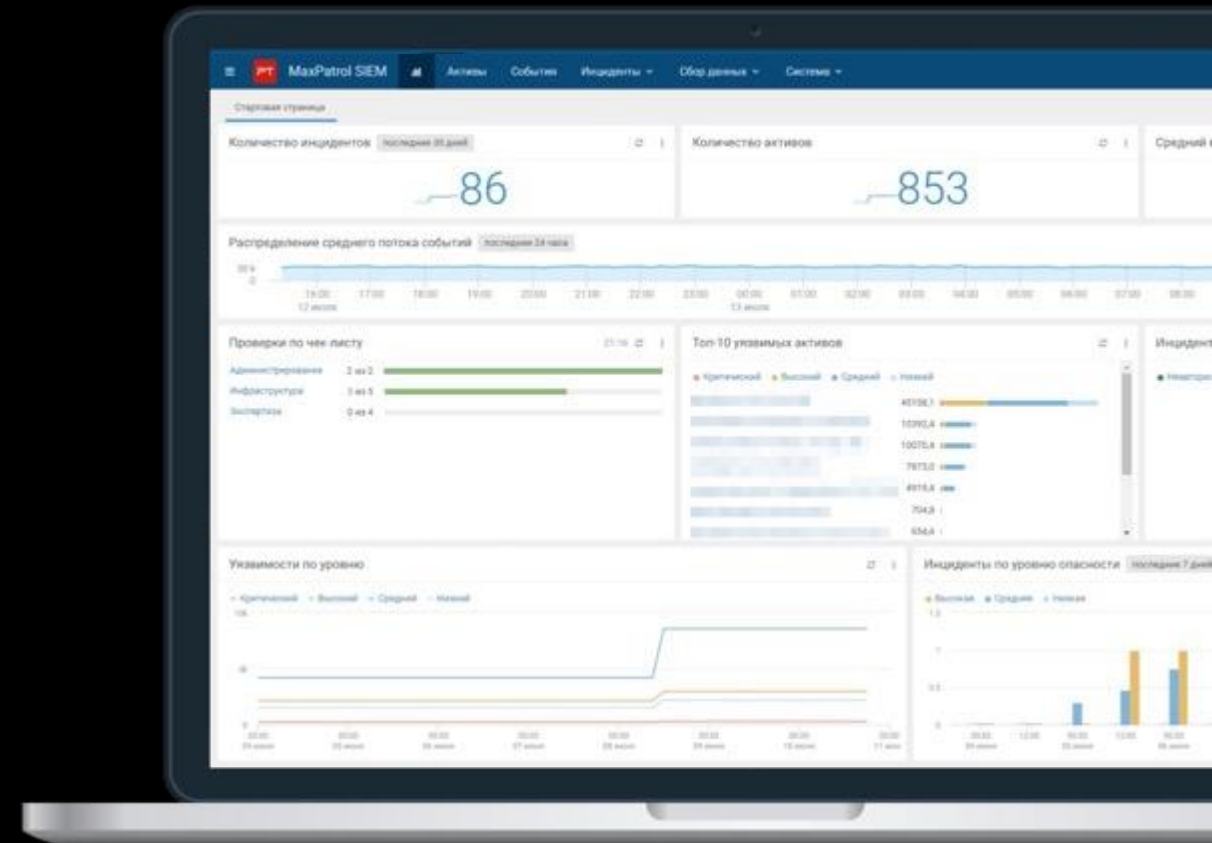
+3 packs

will be released by end of 2024



Off-the-shelf

faster project implementation



+ more in roadmap for continuous enrichment²⁴ of the OT expertise

MaxPatrol VM SCADA software



Next-generation vulnerability management system

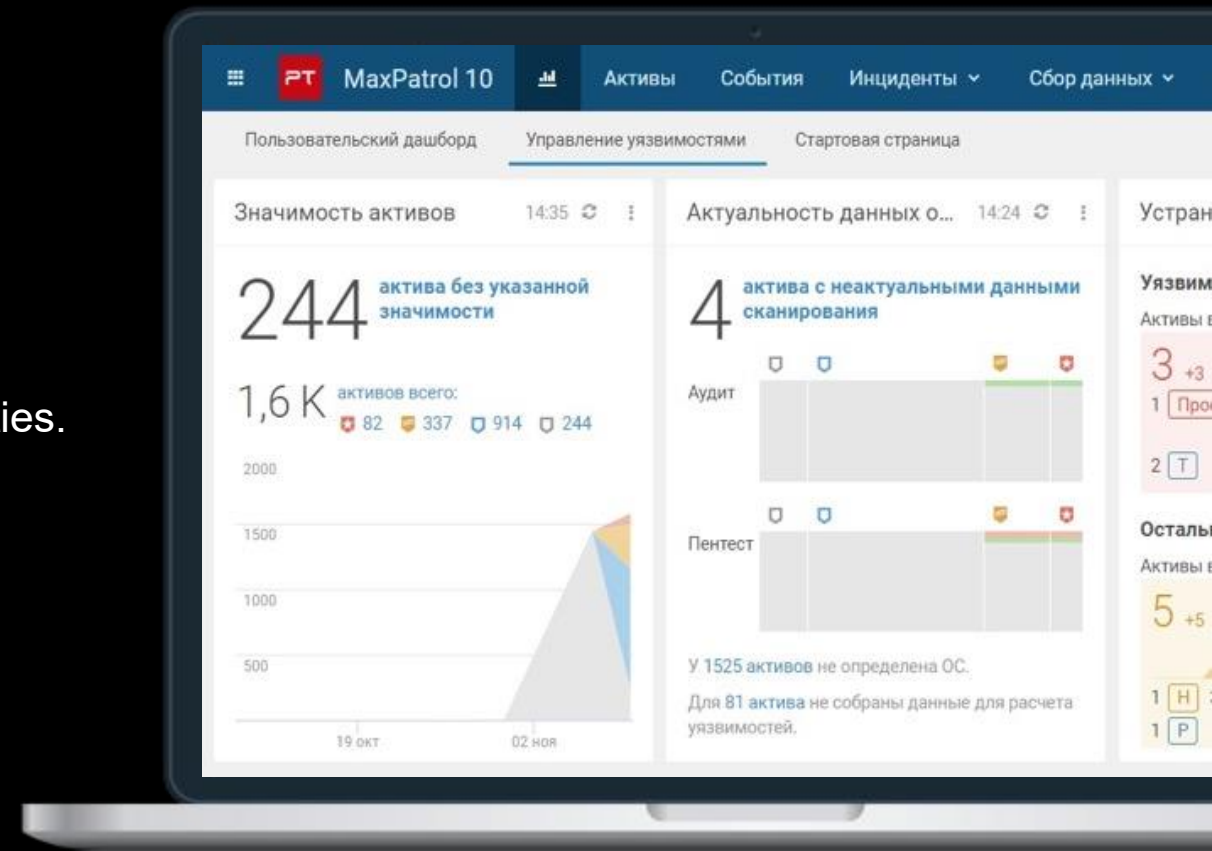
- Helps build a fully-fledged vulnerability management process that involves cyber security and IT specialists.
- Monitors the security of IT infrastructure at all times and helps to properly prioritize work on vulnerabilities.
- Includes industrial agents and expertise:
 - SCADA and firmware scanners
 - Vulnerability detection robots

[Product booklet](#)

3 packs

of industrial expertise is already available for MaxPatrol VM

+ more in roadmap for continuous enrichment of the OT expertise



PT Sandbox tailored for SCADA



Advanced sandbox

with customizable virtual environments. Detects sophisticated cyberthreats.
Applies machine learning technologies as well as static and dynamic methods

You received a malware by email. It's not a regular malware, but... something industrial

Could this be the beginning of a targeted attack?

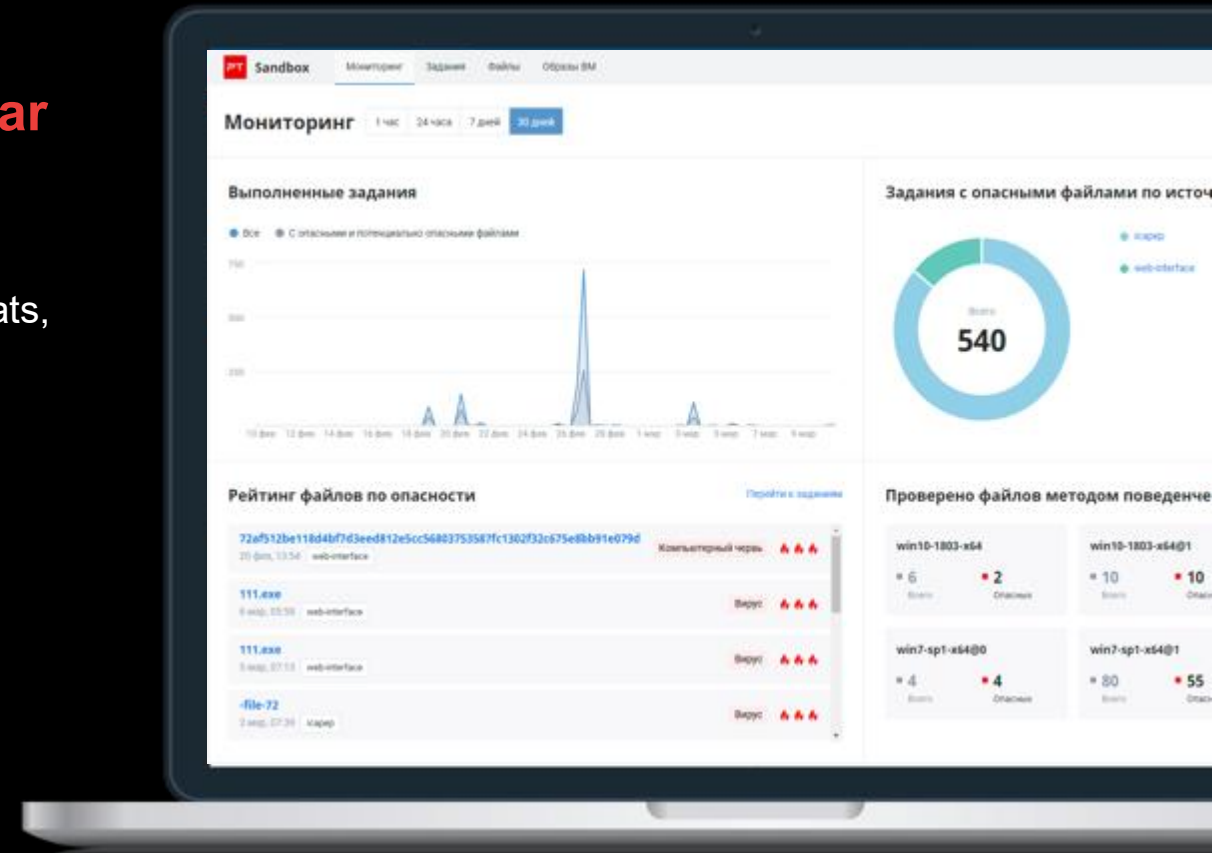
Protects against targeted and mass malware attacks and zero-day threats, and detects both common malware (encryption malware, ransomware, spyware, remote control utilities, and loaders) and sophisticated hacker tools, such as rootkits and bootkits

What is important for OT

Emulation of technological environments

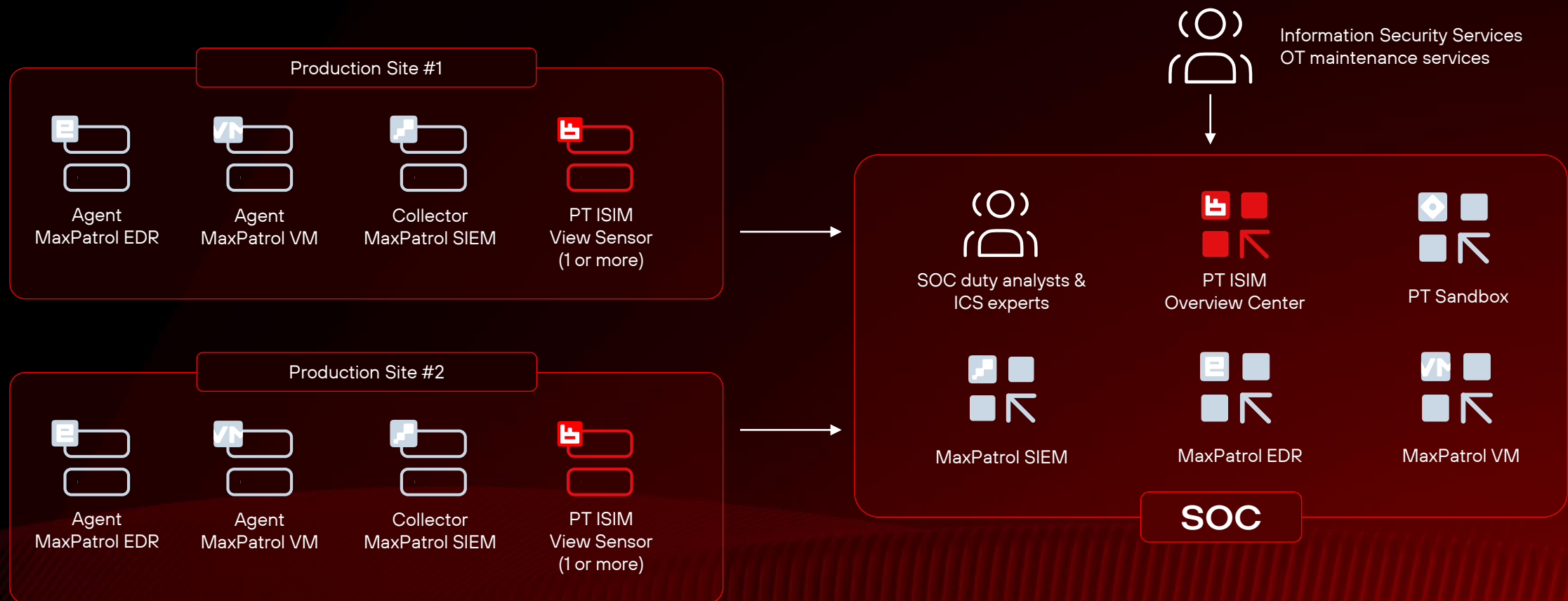
Detection of SCADA- and firmware-specific malware

[Product booklet](#)



Components of PT ICS

in geographically distributed deployment



4. References

Reference project: power generation



Company & industry: a large private power generation holding in Russia

Project size: 50+ Thermal Power Plants, Hydro Power Plants, Solar Power Plants, hundreds of boiler stations

Project: Cyber Attack Defense Center for the whole holding

Goals & objectives: defense of critical infrastructure; digital transformation

Products: MaxPatrol Platform (SIEM, VM, EDR) + PT ISIM + PT Sandbox & PT AF

Project timeline: Phase I – 2020-2022 (completed), Phase II & III - 2023-2025 (in progress)

Achievements: thanks to this project the company managed to secure the IT and OT infrastructure from the massive attacks started in March 2022 and continuing nowadays. Project kicked-off digital transformation of the whole holding, and development of company-wide security standards and practices



40 000
employees



14M
households



160k
companies

Reference project: transportation



Company & industry: the largest railroad company in Russia

Project size: 100+ railroad stations

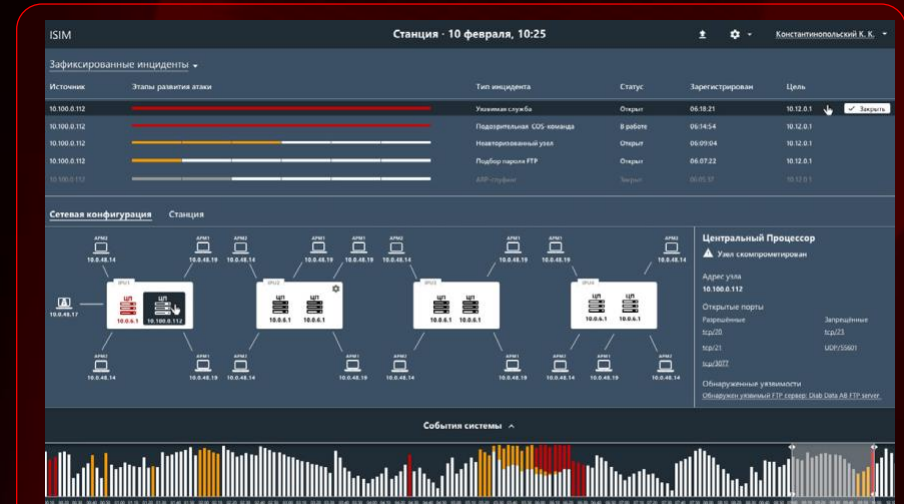
Project: security control for Bombardier computer-based interlocking systems based on EBILock 950 controllers

Goals & objectives: integrity control of the interlocking systems, threats detection

Products: PT ISIM

Project timeline: 1st deployments in 2016. Continuous roll-out across whole country

Achievements: Bombardier proprietary protocols supported in PT ISIM to control normal operations inside the railroad interlocking system



Reference project: ore mining and concentrating plant



Company & industry: one of the largest private iron ore refineries

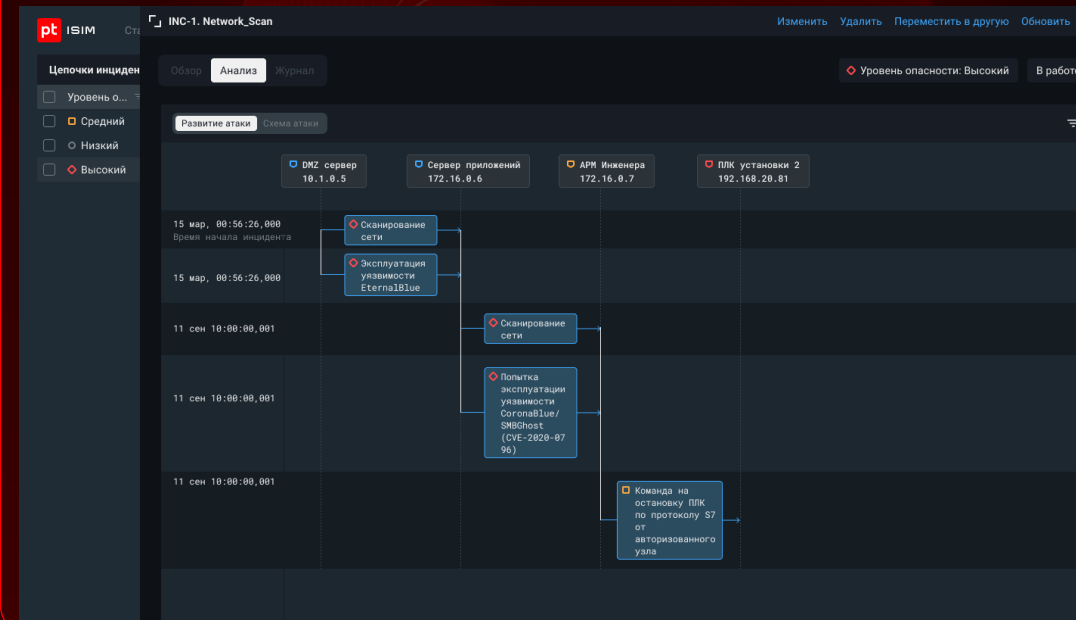
Project size: several production sites, including most automated production lines (based on Siemens WinCC)

Project: monitoring and control of traffic & events from OT environment (separation, jaw crusher, floating, etc.)

Goals & objectives: critical infrastructure defense

Products: PT ISIM and MaxPatrol SIEM

Achievements: the customer is now confident that the remote production infrastructure is well secured. All security incidents are monitored and investigated in a timely manner





PT ISIM

Web-page
ptsecurity.com



PT ICS

Thank you!

Cyber threats for OT segment in 2023

from Positive Technology



10%

of all successful attacks were targeted on industrial companies

Each 3rd

attack led to non-tolerable event – business or operations interruption

80%

Attacks in Middle East were targeted APT attacks

>30%

Is share of industrial companies in targeted attacks

88%

Attacks in Middle East were detected in Saudi Arabia

Sources

<https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/>
<https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/>
<https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-chetvertaya/>
<https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/>
<https://www.ptsecurity.com/ww-en/analytics/apt-groups-in-the-middle-east/>

Cyberattack Hits Iran's Major Steel Companies in Iran (2022)



Cyberattack Hits Iran's Major Steel Companies

Monday, 06/27/2022

Conflict - Military

Iran

see in the video, this cyberattack has been carried out carefully so to protect innocen

A screengrab from the footage of Khuzestan Steel Company's CCTV that was released by the Predatory Sparrow hacker group

A hacking group called Predatory Sparrow targeted Monday three of Iran's major steel plants by a cyberattack, purportedly forcing one of them to halt production.

The group said that it hacked **Mobarakeh Steel Company** in the central Esfahan province, **Khuzestan Steel Company** in southwestern Iran near Ahvaz, and **Hormozgan Steel Company** in the south.

Khuzestan Steel Company – Iran's second biggest after Mobarakeh -- had to stop work until further notice "due to technical problems" following the attack, which is one of the biggest on the country's strategic industrial sector in recent years.

He claimed the cyberattack was unsuccessful and no structural damage to production lines happened, thanks to "timely measures and vigilance."

Another Iranian news channel, Jamaran, said the attack failed and no machines were harmed because the factory happened to be non-operational at the time due to an electricity outage.

[See more details](#)

Inactive malware found at 2 petrochemical plants in Iran (2016)



The official said the malware at the two plants was inactive and had not played a role in the fires.

In periodical inspection of petrochemical units, a type of industrial malware was detected and the necessary defensive measures were taken,” Gholamreza Jalali, head of Iran’s civilian defense, was quoted as saying by the state news agency IRNA.