What is critical infrastructure?

Critical infrastructure consists of systems that manage technological processes in industries that are of strategic importance for the global economy, government institutions and society.

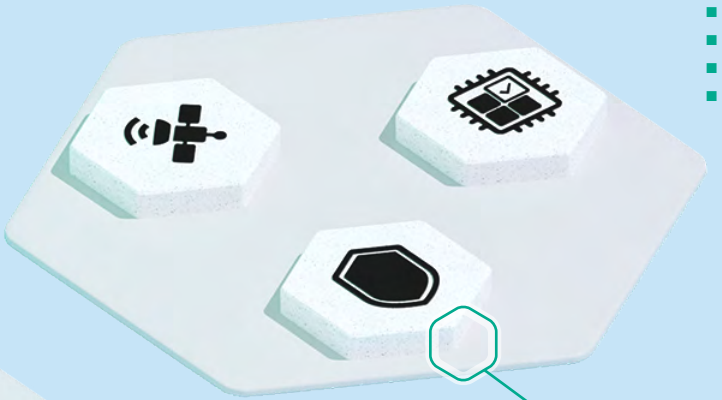
Critical infrastructure in industry

Heavy industry

- Fuel extraction
- Electricity production and supply
- Mining industry
- Metallurgy
- Chemical industry
- Automotive production
- Mechanical engineering
- Production of construction materials
- Pulp and paper industry

Light industry and social infrastructure

- Logistics and transport
- Food industry
- Pharmaceuticals
- Housing and utility facilities



Critical manufacturing

- Defense industry
- Rocket and space industry
- Production of microchips and electronics

How we protect critical infrastructure and industrial enterprises

Ensuring industrial cybersecurity

Objective

Eliminate cyber-incidents at our customers' industrial facilities

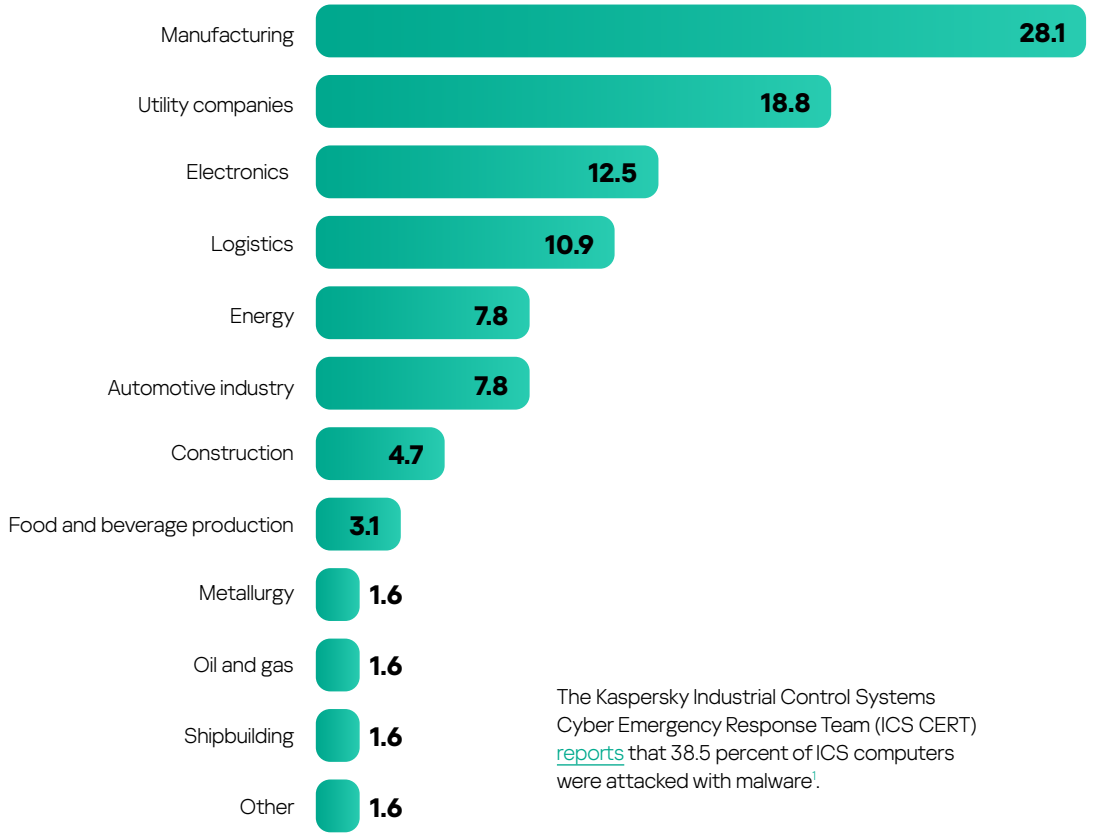
Today, industrial cybersecurity is a technology that promotes the sustainable development of enterprises. Our solutions can be used to protect companies from any industry and with any level of digitalization, whether they use conventional or cutting-edge computer equipment.

Our brief overview of main industrial cybersecurity incidents in the second half of 2023 showed companies in the manufacturing sector accounted for the vast majority of enterprises that came under attack.

Breaches of critical infrastructure in 2022–2023

- ThyssenKrupp had to suspend the production of automotive parts due to a cyberattack.
- Battery manufacturer Varta suspended production at all enterprises after its IT systems were hacked.
- Hackers took control of the IT system at a pumping station of the Municipal Water Authority of Aliquippa, which provides water supply services in the U.S. state of Pennsylvania.
- A cyberattack on the global container terminal operator DP World led to major disruptions at Australia's international ports.
- Nearly 2 million Texans experienced water outages due to a cyberattack on their water utility NTMWD.
- The hacktivist group SiegedSec hacked into and stole confidential data from the Idaho National Laboratory, a nuclear research center of the U.S. Department of Energy.

Industries most susceptible to cyberattacks in the second half of 2023



The Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS CERT) reports that 38.5 percent of ICS computers were attacked with malware[1].

Our contribution to minimizing risks and reducing damage from cyberattacks on manufacturing enterprises

We help customers save money with our solutions

Cyberattacks can lead to the disruption or complete shutdown of processes and services, which can diminish a company's economic performance. This can be avoided with the use of our products to protect critical infrastructure and industrial enterprises. In April 2021, Forrester conducted a study on how our industrial security solution, KICS for Networks, impacted the economic indicators of a major energy supplier and compared our customer's potential losses to the cost of a KICS license.

What was the result?

US$2.5 million
decrease in the risk of security breaches

US$338,000
reduction in possible equipment damage

US$1.6 million NPV[2]

135% ROI

The researchers concluded that the solution paid for itself in just eight months, and ROI was recorded as 135 percent net present value for an average customer over three years. In addition, introducing KICS helped the company correlate the real and documented network and created more transparency in terms of network assets and access points.

[1] All types of threats.
[2] Net Present Value is a financial indicator of the amount of cash an investor expects to receive from a project after cash inflows make up for its initial investment costs and the periodic cash outflows associated with the project.

Solutions

Protect all levels of an industrial enterprise's systems and networks

Kaspersky OT CyberSecurity

We are committed to providing each and every customer with the value they need from the introduction of our cybersecurity systems, regardless of their industry, level of maturity or complexity of their request.

Our industrial cyber-physical security ecosystem, Kaspersky OT CyberSecurity (KOTCS), reduces the threat of cyberattacks and eliminates the risk of unacceptable events. It contains:

- **Technology:** a robust selection of tested, compliant, and approved industrial security solutions;
- **Knowledge:** reliable threat analytics and comprehensive industrial cybersecurity training;
- **Expertise:** a full range of professional services for comprehensive industrial cybersecurity.

The KOTCS ecosystem consists of 18 products and services for industrial enterprises that were developed by Kaspersky specialists with world-class expertise, including 15 years of experience in protecting industrial facilities and 10 years of work to develop the KICS. The most mature ecosystem on the cybersecurity market, it protects industrial enterprises at every level from a central location. It has advanced functionalities to protect against all cyber-physical threats (such as its own unique Antidrone system) and ensures safety at industrial facilities, including nuclear power plants, reliability of which is subject to the most stringent requirements by the regulatory authorities.

KOTCS – protection at every level

Level 3. Enterprise systems

- Convergence of IT and OT and correlation of data from all available sources
- Unified security processes and approaches using Hybrid XDR (Extended Detection and Response)
- Training programs, consulting and advanced threat analytics

Level 2. Monitoring and control

- IIoT[1], connectivity and perimeter supervisory control and data acquisition (SCADA)
- Access and usage control, audit and visibility of OT systems
- Expert on-site support

Level 1. Controllers and protection

- Detection of intrusions, hacking and compromise attempts, as well as vulnerabilities in microprocessor technological equipment at the lower level of automation, such as controllers, security terminals and measuring centers
- Deep protocol inspection (DPI) and protection of embedded operating systems in industrial equipment against network threats and attempts to maliciously influence process settings (parameters)
- Detection of anomalies in technological processes with machine learning based on samples from databases or real-time data

Level 0. Technological process

Monitoring of airspace to protect essential equipment against cyber-physical threats and ensure the safety of connected vehicles

[1] The Industrial Internet of Things consists of a multi-tiered system that includes sensors and controllers installed on an industrial facility's components and assemblies, equipment to transmit and display data, powerful analytical tools to interpret information and numerous other components.