Our security team
is your security team

Kaspersky ICS Security Assessment

kaspersky bring on the future

ICS Security challenges

- Outdated and proprietary industrial solutions with vulnerabilities, limited SOC visibility and lack of threat protection solutions
- Financial losses from attacks: disruption or loss of control over industrial processes, recovery after an incident, and regulatory fines
- Challenges in the integration of IT and OT systems, including configuration errors, conflicts, and security issues
- Shortage of OT cybersecurity specialists and maintaining up-to-date security knowledge and skills

Ensuring cyber resilience in OT environments

For a long time, the primary standard for securing ICS environments was their functional safety — preventing accidents, human casualties, and environmental pollution. In terms of information security, the focus was on network isolation and protection from physical impacts. The integration with OT of IT networks, support, engineering, telemetry, and other systems has expanded the attack surface, exposing highly vulnerable ICS solutions within the network, without the SOC having visibility. Industrial processes depend on this integration, and attacks on typical corporate environments can affect industrial operations.

~40% of ICS computers have been attacked with malware worldwide since the beginning of 2024[1]

Kaspersky ICS Security Assessment provides comprehensive analysis to identify and evaluate the exposure to risk and attack surface of operational technology (OT) environments, and the security levels of industrial network infrastructures, distributed control systems (DCS), and industrial devices, as well as the risk of compromise to mission-critical systems.

Kaspersky experts have been conducting ICS Security Assessments for almost 10 years and they hold numerous certifications from respected industry bodies, ensuring advanced expertise and up-to-date knowledge.

Kaspersky's approach to Industrial Security Assessment

Our approach is based on the Purdue Reference Model and involves techniques including:

1

ICS Security Assessment

Security-wise inventory, identifying vulnerabilities and providing recommendations for industrial network and automation solutions

2

Internal penetration testing[2]

How to reach an industrial (OT) network from the corporate level

3

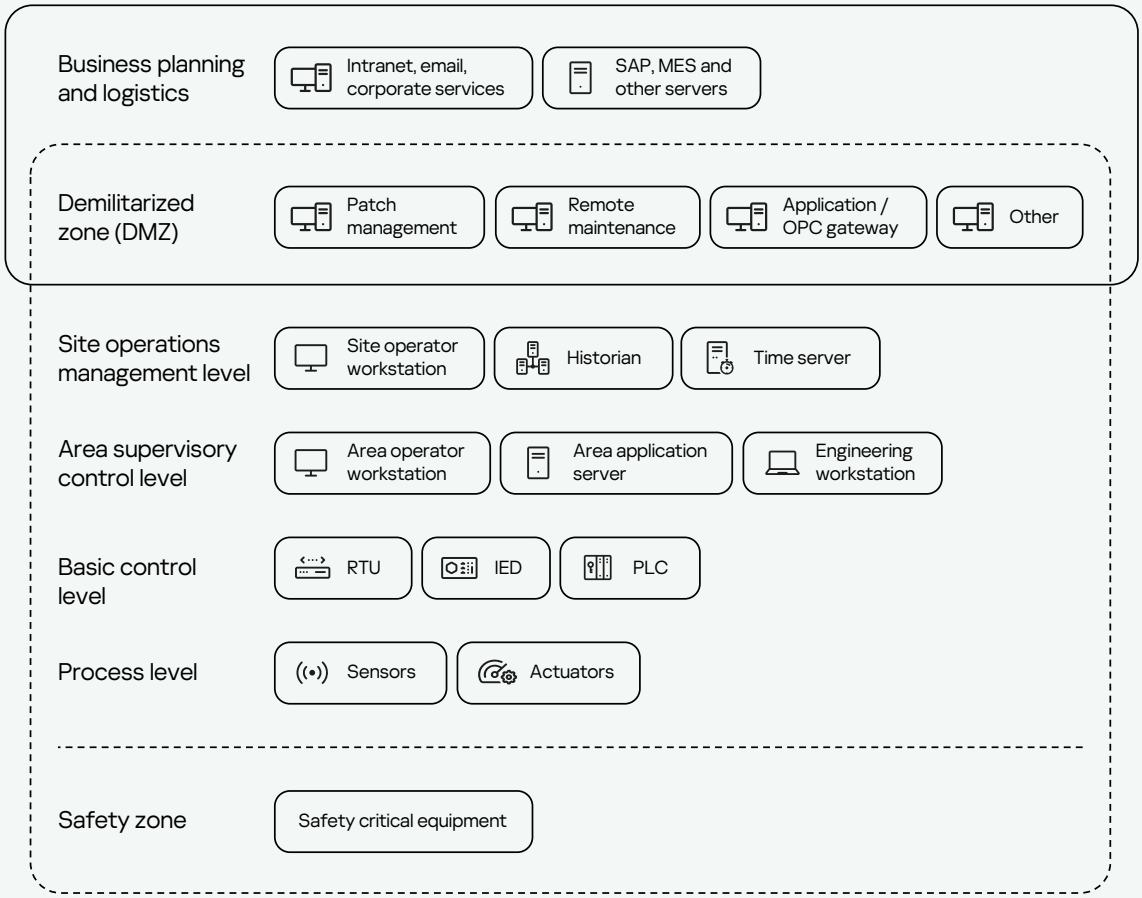
External penetration testing[2]

How the corporate network could be accessed from the internet

Our test methodologies are based on black-, grey-, and white-box techniques, enabling us to provide the most comprehensive security assessment possible.

[1] Kaspersky ICS CERT Statistics. To learn more follow the link
[2] The service can be purchased separately

The Purdue Model



Penetration Testing conducted in the enterprise (IT) zone

ICS Security Assessment conducted in the industrial (OT) zone

The process

1

Preparation

Define the scope of the project, its goals and limitations

2

Remote analysis

Analyze configuration files and conduct interviews with key stakeholders

3

Onsite analysis

Infrastructure assessment

4

Reporting

Prepare and present the results

5

Follow-up meeting

Live discussion of the assessment results

Deliverables:

- **Executive report**
- **Analytical report**
- **Detailed technical report**

- Threat modeling and vulnerability prioritization
- Attack scenarios for identified threats
- Secure default configuration to reduce attack surface
- Interaction with supplier / manufacturer
- System knowledge (expert and machine-readable) to improve monitoring and response
- Types of impact on the technological process
- Integration of security mechanisms into industrial solutions
- Development of configuration guides for industrial solutions
- Vulnerability mitigation with the manufacturer
- Verification of secure configuration with the manufacturer
- Attack surface and consequences of an attack

With Kaspersky ICS Security Assessment you can:

Enhance onsite security measures

Strengthen security controls to protect operators, engineers, and staff members

Prevent disruption

Understand what vulnerabilities hackers can use to cause breakdowns of assembly lines, manufacturing machines, or robotic arms

Safeguard your Intellectual Property

Protect your manufacturing schemes, projects, and programs from theft

Maintain product quality and safety

Avoid breaches in the production process that could lead to shortcomings in product quality or safety

When choosing an OT Security Assessment service, think about these critical advantages

Expertise across industries

Our certified experts have advanced knowledge and practical skills in working with industrial equipment and infrastructures in environments including rail, power generation plants, manufacturing, oil and gas, and many more.

Actionable insights

The assessment provides detailed and actionable insights into the identified vulnerabilities and risks. We explain how these findings relate to your production processes, enabling you to implement effective security measures.

Thorough testing methodology

We use a validated test methodology based on hundreds of actual projects. Tests can include a preparation phase in a laboratory, training or other simulated environment, in order to ensure the safety of testing in the actual production environment.

Compliance with global standards

We highlight those areas where our findings relate to leading best practices and standards including NIST, CIP, ISA, and others.

Kaspersky ICS Security Assessment

Contact us

Powered by Security Services

www.kaspersky.com

#kaspersky
#bringonthefuture