Kaspersky® Industrial CyberSecurity

Kaspersky ICS Security Assessment

For a long time, providing security of industrial control systems (ICS) was mainly about ensuring safety and functional security to avoid production accidents, human losses and environmental pollution. For IT security, during design and maintenance of industrial control systems, vendors, integrators and owners were mainly focused on physical security and physical network isolation. An increase in malware and attacks on Industrial Control Systems (ICS), the growing number of new vulnerabilities in ICS equipment and an increased necessity for these systems to be integrated with other environments (like ERP, for example) have necessitated a more thorough approach to ICS security. In addition, ICS security is closely tied with functional security and a successful hacker attack could lead to production accidents.

ICS Security Assessment Results

As a result of the ICS security assessment service, various vulnerabilities leading to obtaining unauthorized access to critical network components may be identified, including:

- Insufficient physical protection of ICS equipment
- Vulnerable network architecture, insufficient network protection (including flaws in separation of the ICS network from other networks)
- Vulnerabilities leading to network traffic interception and redirection (including ones in industrial communication protocols)
- Vulnerabilities in ICS components, such as SCADA, PLCs, smart meters, etc.
- Insufficient authentication and authorization in various services
- Weak user credentials
- Configuration flaws, including excessive user privileges, as well as non-compliance with security standards and vendors' recommendations
- Vulnerabilities in communications between the analyzed ICS and other systems (for instance, through a MES)
- Vulnerabilities caused by errors in applications' code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by using outdated hardware and software versions without the latest security updates
- Information disclosure

ICS Security Assessment is a service aimed at identifying various security flaws in your ICS on all layers: starting from physical and network security, to vendor-specific vulnerabilities in ICS components, such as supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs) and others. This service provides you with information on vulnerabilities in your ICS and the consequences of their exploitation, evaluates the effectiveness of implemented security measures, and enables you to plan further actions to fix detected flaws and improve security.

Why you should do this

ICS Security Assessment by Kaspersky Lab helps organizations to:

- Understand the weakest spots of ICS and focus on improving the corresponding security processes
- Avoid human, environmental, financial, operational and reputational loss that potentially could be caused by malefactors, by proactively detecting and fixing the vulnerabilities which could be used for attacks
- Analyze systems' compliance to ICS security standards specific to your region and industry, for instance NERC CIP standards
- Comply with government, industry and internal corporate standards that require security assessments to be carried out

What we are testing

Industrial control systems of any vendor and industry can be analyzed by Kaspersky Lab experts: **power generation and transmission, transportation systems, oil and gas production, mining operations, and many others.**

Depending on your infrastructure and needs, different security assessment approaches and combinations may be used:

- **Penetration Testing** – A security assessment that simulates various types of intruders upon your choice, the goal of which is to elevate the current privileges and access the ICS environment.

- **ICS Infrastructure Security Assessment** – White-box security assessment, during which our experts will analyze technical ICS documentation, have interviews with ICS personnel, analyze industrial systems and protocols in use, and provide comprehensive technological audit of ICS components in the production environment.

- **ICS Solution Security Assessment** – A deep security research of software and hardware ICS solutions in the test environment to look for new vulnerabilities, followed by pre-approved tests demonstrated on the real system.

The project team members are experienced professionals in practical security with deep knowledge in this field, constantly improving their skills, and renowned for their ICS security research.

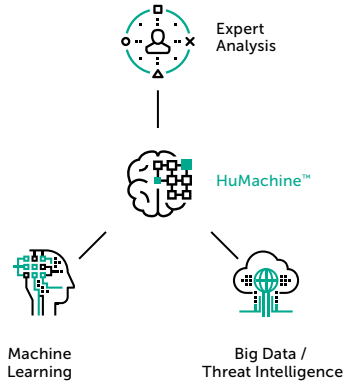
Once the service has been completed, our customers receive a report containing detailed technical information on the testing process, results, security flaws and recommendations, and a comprehensible executive summary describing the conclusions of the test results and illustrating industry-specific attack scenarios. Screen videos with attack demonstrations and final presentations for your technical team or top management can be provided if required.

How we do this

The service is performed by experienced Kaspersky Lab security experts who respect your systems' confidentiality, integrity and availability in strict adherence to international laws and best practices.

Kaspersky Lab provides ICS security assessments in accordance with the following international standards and best practices:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Center for Internet Security (CIS) standards
- Common Vulnerability Scoring System (CVSS) and other standards (depending on your organization's business and location).



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/fraudprevention
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

#truecybersecurity
#HuMachine

www.kaspersky.com