KASPERSKY INDUSTRIAL CYBERSECURITY EXPERT SERVICES: CYBERSECURITY ASSESSMENT

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI panels, engineering workstations, PLCs, network connections and people – without impacting on operational continuity or consistency of the technological process.

For organizations concerned about the potential operational impact of IT/OT security, Kaspersky Lab's Industrial CyberSecurity Assessment provides a minimally invasive pre-installation cybersecurity assessment. A crucial first step in establishing security requirements within the context of operational needs, it can also provide significant insight into cybersecurity levels without any further deployment of protection technologies.

Why industrial environments are uniquely vulnerable

Modern industrial control systems (ICS) are vulnerable to cyberattack for some unique reasons. They often combine networked technologies with legacy systems and it's not unusual for organizations to leave critical vulnerabilities unpatched rather than interrupt a process – something cybercriminals are keenly aware of.

Weak access controls, default settings, usage rules and policies - all in the name of operational continuity – can have dire consequences. Vulnerabilities unique to industrial-specific software, such as hard-coded passwords and insecure protocols are hangovers from a past where ICS wasn't connected to the network and the concept of 'software vulnerabilities' barely existed.

Kaspersky Lab uses a consistent, structural approach to identify relevant vulnerabilities and threats – finding the most cost-effective way to improve cybersecurity.

CyberSecurity Assessment service scope:

Stage 1: Identification of objects requiring protection ('objects of protection' or OoP) and impact assessment, based on[1]:

- Potential damage from cyber-incident for specific industrial object – including direct financial losses from physical damage, downtime aftermath, reputational costs, etc.
- Role and influence of information system supporting the OoP.

[1] For the purposes of this document, we've listed the most important criteria. Organization-specific, individual criteria are also considered during every assessment.

Based on these criteria, KICS experts will identify the infrastructure's most critical OoPs and provide customers with:

- Full list of information systems behind the OoP that should be examined.
- Prioritized list of information systems critical for cybersecurity.

Stage 2: Examination and Risk Analysis, including:

- Interviews with managers, engineers, operators and system administrators.
- Estimation of current state of protection through analysis of current configurations, network traffic, memory dumps, logs, etc.
- Penetration testing of IS via all possible vectors – internet connections, connections to interfacing networks and objects.
- Emulation of specific attack vectors – testing of specific IS' components – controllers and software.
- Research into zero-day vulnerabilities in selected ICS' components (SCADA, HMI, Engineering WS, PLC, IED, terminals etc.) is performed on isolated ICS infrastructure in order to better understand of real state of protection.
- KICS experts can, additionally, scan for malicious activity inside the customer's infrastructure.

At stage 2 customers receive:

- Full list of discovered vulnerabilities and existing security gaps with detailed analysis of how they can be exploited.
- Description of detected and confirmed attack vectors that can damage continuity or integrity of technological process.

Stage 3: Threat Model and CyberSecurity recommendations.

Based on data from Stages 1 and 2, KICS experts develop a threat model that will be used as a basis for developing specific recommendations. Stage 3 customers receive:

- A list of security recommendations for specific components like SCADA, controllers, etc. including mitigation techniques for vulnerabilities that cannot be directly addressed.

Stage 4: Plan of action for enhanced OoP security.

Very often security recommendations are shelved due to the specifics of technological processes, narrow maintenance windows or a need for additional analyst work. To ensure success, at this additional stage Kaspersky Lab experts will work with the customer to develop a genuinely actionable security plan mapping Stage 3 requirements to the specifics of the customer's infrastructure, limitations and all.

Stage 4 customers receive an achievable "To-do" plan of action for each OoP, developed by Kaspersky Lab experts in conjunction with customer reps.

Why Kaspersky Lab

Kaspersky Lab is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures. We're one of the few vendors with genuine experience and expertise in the sector:

- Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure.
- Unique scan methodology to detect industrial attack vectors that can cause downtime.
- Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.
- Kaspersky Industrial CyberSecurity is a holistic portfolio of services and technologies, including malware analysis, training and awareness programs, industrial network monitoring, incident response and many more. One vendor supplies all the bricks you need for your security wall.

KASPERSKY lab