Kaspersky ICS Threat Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting provides in-depth intelligence and greater awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in the most popular industrial control systems and underlying technologies. Reports are delivered via a web-based portal, which means you can start using the service immediately.

Reports included in your subscription

1. **APT reports.** Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats.
2. **The threat landscape.** Reports on significant changes to the threat landscape for industrial control systems, newly discovered critical factors affecting ICS security levels and ICS exposure to threats, including regional, country- and industry-specific information.
3. **Vulnerabilities found.** Reports on vulnerabilities identified by Kaspersky in the most popular products used in industrial control systems, the industrial internet of things, and infrastructures in various industries.
4. **Vulnerability analysis and mitigation.** Our advisories provide actionable recommendations from Kaspersky experts to help identify and mitigate vulnerabilities in your infrastructure.

Threat intelligence data empowers you to

Detect and prevent

reported threats to safeguard critical assets, including software and hardware components and ensure the safety and continuity of technological process

Correlate

any malicious and suspicious activity you detect in industrial environments with Kaspersky's research results to attribute your detection to the malicious campaign in question, identify threats and promptly respond to incidents

Perform

a vulnerability assessment of your industrial environments and assets based on accurate assessments of the vulnerability scope and severity, to make informed decisions on patch management and implement other preventative measures recommended by Kaspersky

Leverage

information on attack technologies, tactics and procedures, recently discovered vulnerabilities and other important threat landscape changes to:

- Identify and assess the risks posed by the reported threats and other similar threats
- Plan and design changes to industrial infrastructure to ensure the safety of production and the continuity of technological process
- Perform security awareness activities based on analysis of real-world cases to create personnel training scenarios and plan red team vs. blue team exercises
- Make informed strategic decisions to invest in cybersecurity and ensure resilience of operations

www.kaspersky.com