Severstal

Expert industrial cybersecurity training for Severstal employees

kaspersky BRING ON THE FUTURE

Kaspersky ICS CERT

Severstal

severstal.com

Mining and metallurgy industry

- Severstal has over 70 plants with 50,000 employees.
- Severstal has 5,000 customers in 60 countries.
- The company has one of the highest profit margins, as well as stable share growth.

PAO Severstal is a vertically integrated steel and steel-related mining company. Severstal is a global leader in efficiency, with the highest EBITDA margin in the steel industry globally.

CherMK (Cherepovets Steel Mill of PAO Severstal) is one of the largest integrated steel plants in the world. The company's customer base, taking into account the distribution network, includes about 10,000 Russian and foreign companies working in the construction, mechanical engineering, automotive and oil and gas industries. Its high level of product quality is certified by both international (ABS, Bureau Veritas, Det Norske Veritas, Germanischer Lloyd, Lloyd's Register) and Russian (Russian Maritime Register of Shipping, Russian River Register, GOST R, etc.) certificates. Severstal seeks to gain a competitive advantage when it comes to reducing manufacturing costs for its core products. To achieve this, the company uses advanced technologies and modern business models.

The company provides services that include metal services centers, repair and design of hardware, design and construction of buildings and structures, as well as laboratory services. The company's customers operate in core industrial sectors, such as construction, automobile production, fuel energy, mechanical engineering, shipbuilding, etc.

The Cherepovets Steel Mill, owned by Severstal, has been operating since 1955 and has eight types of production facilities: sintering, coke-oven, blast furnace, steelmaking, hot-rolled flat-rolled, cold-rolled, long products and tubes. In 2019, the company produced 11.8 million tonnes of steel, 4.7 million tonnes of coal, 11 million tonnes of pellets and 6.2 million tonnes of iron ore concentrate.

Cybersecurity of production systems

It is important for Severstal to ensure the safety of its production management systems without disrupting operations. To do this, the company implements a comprehensive approach to building a protection system for its production systems. Since 2015, one of the key elements of the industrial cybersecurity system has been a range of Kaspersky products and services. The company uses KICS for Nodes, KICS for Networks and KES products to protect workstations, servers and industrial networks. In addition to basic functionality, these solutions can increase situational awareness, which is further enriched by Kaspersky's ICS threat intelligence services.

Activities to ensure cybersecurity and cyber-resilience for production processes are impossible without the active participation of the personnel involved in analyzing attacks on the enterprise, identifying current threats, speeding up incident response and enhancing cybersecurity systems.

"During training we received a lot of useful information and practical skills applicable to our work. It should also be noted that the training is conducted by experts with real practical experience who are ready to answer any questions that arise. The forensics methodology we received has been tested for our production systems and will integrate seamlessly with our processes"

Sergey Povyshev, Senior Manager of the Production Systems Protection Group of Severstal's Information Security Department.

Required knowledge
With the active digitalization of control systems and their integration with corporate systems increasing the number of cyber-incidents in industrial automation systems, there is a growing need to increase employee awareness of ICS cybersecurity.

Effective learning
Kaspersky training for industrial cybersecurity specialists, based on the real-life experience of Kaspersky experts, enables participants to develop skills in digital forensics and the security analysis of production systems in a short period of time.

Setting the foundations
Completing the portfolio of Kaspersky Industrial CyberSecurity training lays the foundation for a systematic approach to industrial cybersecurity at an enterprise.

Challenge

One important step to achieving the stated goals is solving the issue of increasing competencies and the acquisition of practical skills by company employees in the field of information security. Solving this is difficult without first mastering penetration testing tools, demonstrating practical real-life attack scenarios that take into account production site specifics, and conducting master classes by leading experts for the detection of vulnerabilities and genuine threats to industrial control systems.

Solution

Kaspersky experts conducted the specialized ICS Pentesting and Digital Forensics and Incident Response training sessions. Under the guidance of experienced specialists, the participants developed the skills needed to analyze the security of SCADA, PLCs and other elements of ICS. They also learned how to detect and investigate cybersecurity incidents, from the collection of evidence to the formation of expert recommendations on incident prevention and how to eliminate the effects of attacks.

Training included the simulation of attacks based on real-life situations at industrial enterprises, as well as interactive training of skills to conduct penetration testing, security analysis and digital forensics.

The training programs are designed both for IT/OT security professionals who have already worked with industrial environments and for other employees aiming to develop their skills in penetration testing and incident response.

"I should emphasize the practical relevance of the knowledge gained in relation to my work. We were given the right focus for further development in the field of digital forensics. I'd rate the course a 10 out of 10!"

Alexander Igoshin, Manager in the Information Security Department at Severstal.

Results

The ICS Pentesting and Digital Forensics and Incident Response expert training conducted by Kaspersky enhanced the professional skills of the Severstal specialists responsible for information security of industrial systems. They acquired skills enabling them to:

- investigate cybersecurity incidents independently, using the latest tools for collecting evidence;
- detect indicators of compromise in production systems, including hidden ones.

With the knowledge that they gained, the participants were able to demonstrate to ICS engineers threats and vulnerabilities in production systems based on real-world examples.

As a result of the training, the level of employee awareness in the field of information security has increased significantly.

Thanks to the knowledge gained and the forensic toolkit that was created:

- information security specialists have reduced the time required to investigate incidents;
- disclosure of incidents has increased in the company, partly due to the enhanced methods of searching for undocumented features in software;
- the number of incidents where the perpetrator cannot be identified has decreased;
- the number of incidents with identified root causes has increased in the company.

© 2020 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization – including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers – without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics