kaspersky

Development of incident response handbook and training

The problem

The organization lacks established processes and procedures, as well as the communication and decision-making frameworks necessary to respond quickly and effectively to incidents. Employees also lack the necessary skills.

The solution

Development of an incident response handbook that provides detailed descriptions of measures and activities for anomalous situations, including containment, assessment and minimization of incident consequences, taking into account the organization's specific infrastructure and business processes. Incident response training for personnel.

Target audience

Organizations in any industry – energy, public services, transportation and logistics, etc. – including those with geographically distributed structures.

The issue

It's important to be prepared for incidents to cope with them quickly and with minimal losses. Therefore, it is necessary to develop a plan that describes all the required procedures and actions in case an anomalous situation occurs, and to train personnel. If contractors need to be involved, it is necessary to grant them access rights and agree on communication channels and communication procedures.

Many industrial entities have a geographically distributed structure. In this case, IR will require special coordination from personnel at various sites, as well as plans for the centralized collection of digital forensic evidence and for containing different kinds of incidents.

When an organization is hit with a cyberincident, the following actions are crucial:

- Promptly identifying the incident – the longer it takes to identify the incident, the higher the risk of confidential data being stolen, stoppages in industrial processes, production delays, threats to functional safety, etc.

- Rapidly and correctly containing the incident – an improper containment strategy can cause significant loss. Sometimes the affected organization's wrong actions cause more damage to the enterprise than the attackers' actions.
- Collecting and analyzing artifacts – it is much more difficult to determine the causes of the incident, assess losses and identify the safest choices for restoring systems to normal working states if the wrong methodology is used or if there are no effective tools in place for collecting and analyzing digital forensic evidence.
- Conducting lessons learned procedures – these are based on a complete analysis of the investigation results. Without this analysis, it is almost impossible to ascertain what technical and organizational measures are required to minimize the risk of similar incidents in the future.

For effective incident response, the following are needed:

- A team of properly trained experts who can identify incidents in a timely manner using existing enterprise technology, correctly classify them and choose response strategies.
- Incident response plans for different types of incident for all critical systems in the organization's IT and OT infrastructure.
- The necessary technology and resources for incident response, including hardware and software.
- The internal regulatory framework that enables the team of specialists to obtain the necessary access rights when needed, including when involving external experts.
- Understanding of the organizational structure, including the distribution of responsibilities for all investigation team members and external resources.
- Understanding of the industrial process and technical details of the OT and IT systems by all investigation personnel in order to follow the response scenarios that have been created.
- Proficiency in completing basic incident response operations such as gathering digital evidence for further expert analysis and isolating systems to contain an incident.

What we offer

When developing the incident response handbook, we review and analyze industrial and business processes, as well as OT systems. This allows us to propose effective incident detection and response methods and create instructions for using them, tailored to each organization. The resulting guide

includes step-by-step instructions for using utilities to collect and analyze the data required for incident investigations, as well as recommendations for containing various types of incidents and mitigating damage.

When drawing up instructions, we rely on our experience in detecting, preventing and investigating cyberattacks worldwide. We always take into account the security solutions that are already in use at the customer's enterprise.

After preparing the handbook, we conduct a number of training sessions for the organization's personnel to turn theory into real-life skills. During these sessions, we use specially configured demo stands with typical ICS elements to simulate the consequences of various attacks on the customer's infrastructure. Our simulations are based on real-world incidents investigated by the Kaspersky ICS CERT team.

What we do

Defining the scope

We conduct a seminar in which we discuss the main stages of incident response, common issues that need to be addressed, typical mistakes and best practices. The customer defines which IT and OT infrastructure objects and systems will be covered by the handbook, and identifies which departments' representatives will be involved in incident response processes. At this stage, we need:

- A description of the technical make-up and functions of the systems that need to be protected;
- A description of the information security solutions used on these systems;
- Interviews with personnel who will work on incident response.

Analysis of infrastructure, processes, existing practices and available hardware assets

We review and analyze all materials provided by the customer, as well as the interviews with personnel. We determine which computer equipment, system components, services and applications are most critical to the industrial and business processes. Then, based on the protected organization's specifics, the competence of the staff, the available technologies and realistic limitations, we determine how to structure the incident response process. After reaching agreement with the customer, we visit the facility.

Creating the incident response handbook

The handbook outlines the procedures for all six stages of incident response: preparation, identification, containment, eradication, recovery, and lessons learned. All instructions are tailored to the organization's infrastructure. For example, incident identification instructions are customized for the exact SIEM system used at a particular enterprise, and the event sources connected to it. Incident containment instructions take into account backup devices and communication channels, network topology, etc.

> We create a practical handbook that can be used immediately; no further modifications are required.

Moreover, when developing the handbook, we include the most likely attack scenarios against the customer's organizational infrastructure, according to our assessments. Based on our findings regarding weak points in security systems, we make recommendations for improving internal information security standards and technology. These recommendations will reduce the inherent risk of incidents within the organization and the severity of their impact.

Training and rollout

Each member of the incident response team must understand their role in the process. Training helps people apply their newly acquired knowledge and test themselves in real-life scenarios based on incidents drawn from Kaspersky's and the global community's experience. This stage is crucial for the success of the project.

What the customer gets

- Incident response handbook tailored to the enterprise's essential features.
- Trained personnel who are ready to independently respond to cybersecurity incidents.

BONUS: 40 hours of incident response service.

Request a consultation

Learn more

- Updated MATA attacks on industrial companies in Eastern Europe
- Common TTPs of attacks against industrial organizations. Implants for remote access
- Common TTPs of attacks against industrial organizations. Implants for gathering data

- Common TTPs of attacks against industrial organizations. Implants for uploading data
- Targeted attack on industrial enterprises and public institutions

Related services

- Incident response at industrial enterprises
- Advanced incident response training
- Analytical Reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence Portal
- ICS vulnerability database
- Ask the analyst

Request a consultation

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com