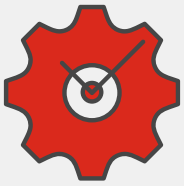
SOLUTION BRIEF

Learn Foundational Incident Response Skills

Executive Summary

Access to experienced first responders is critical to successfully resolving a cybersecurity incident. Offering incident response training to employees within an organization that deals with cybersecurity incidents is recommended by organizations such as the European Union Agency for Cybersecurity (ENISA).

The FortiGuard Incident Response Training Series teaches participants incident response topics through hands-on experience about what to do and what not to do during a security incident.



Median attack costs, as a percentage of revenues, are two-and-a-half times higher for firms ranked as "cyber novices."[1]

Filling the Cybersecurity Skills Gap

A cybersecurity incident response team (CSIRT) is a group of security and IT professionals that provide services related to assessing, managing, and preventing cybersecurity incidents. The goal of this team is to respond to security incidents efficiently and quickly to help minimize the damage. In smaller organizations, CSIRT services are usually assigned to internal employees who take on these additional duties on top of their daily roles. At larger organizations, they may have a dedicated team. ENISA indicates a lack of cybersecurity expertise as one of the challenges subject matter experts face and that providing appropriate training should be one of their principal priorities.[2]

The first minutes after a cybersecurity incident is detected are critical to a successful resolution of the incident. It is essential to quickly understand the incident's scope, properly secure volatile evidence that can help in assessing what happened and make the right decisions in mitigating the effects of the incident.

First responders and decision-makers must make critical decisions regarding the isolation of systems and the preservation of the IT environment based on the available information. Having trained first responders that know how to quickly collect evidence, identify indicators of compromise, and understand the incident's scope, improves an organization's ability to handle a security incident.

FortiGuard Incident Response Training Series

The FortiGuard Incident Response (IR) Training Series is modular, flexible training that is taught by experienced FortiGuard IR consultants to help fill the cybersecurity skills gap. These training courses aim to enhance overall IR knowledge within the organization and improve the technical skills of security operations center (SOC) analysts and organizational incident responders. Training participants learn the foundations of incident response and, through hands-on activity, become familiar with the techniques and tools they need to use for securely collecting forensic data and triaging the data to determine the criticality of an incident.

Participants in the FortiGuard Incident Response Training Series can choose from several different topics, depending on the nature of their IT environment and their level of expertise. The training can be delivered on-site or remotely by FortiGuard senior consultants with years of experience in IR and forensic analysis. In some courses, participants have access to virtual environments created specifically for this training to practice using the tools discussed during the training. Some courses also include hands-on activities, which allow participants to analyze malware samples and forensic artifacts similar to the ones they would encounter in an actual incident.

What Training Participants Learn

Training participants learn various IR tools and techniques, which can help organizations in their response efforts. Topics that will be covered through the various courses include:

- Common attack techniques and their countermeasures
- Key IR concepts and terms
- The IR life cycle
- Foundational IR and SOC concepts
- Proper evidence collection and preservation methods
- Critical Windows forensics concepts, including Windows artifacts and persistence
- Volatile data collection
- Acquiring and analyzing Linux file systems

Effective Response Is Crucial

When an incident is discovered, CSIRT members need to know what to do (and what not to do) to respond quickly and effectively to minimize damage. Training is vital for teams to quickly understand the nature, scope, and risks they're facing. The FortiGuard Incident Response Training Series teaches participants the methods, skills, and processes they need to effectively mitigate threats and minimize the impact of a breach.

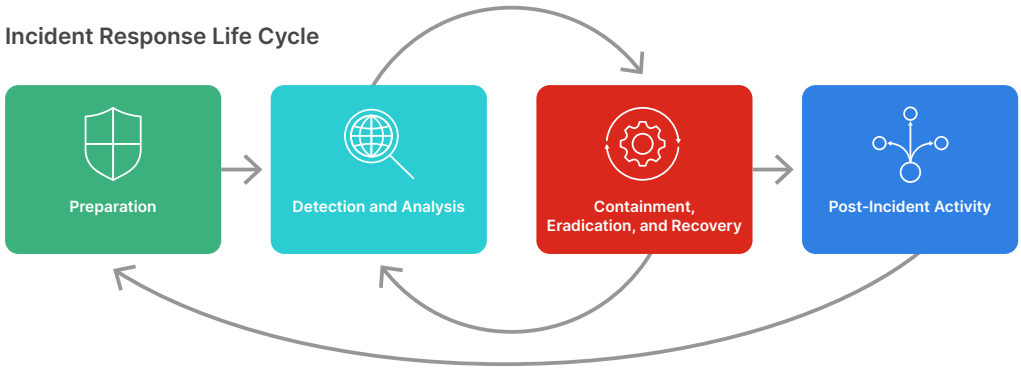


Figure 1: Preparation is the first and one of the most important parts of the NIST Incident Response Life Cycle.

[1] Hiscox Ltd, 2022 Hiscox Cyber Readiness Report.

[2] ENISA, Cybersecurity for SMEs - Challenges and Recommendations, June 28, 2021.

December 22, 2023 9:42 AM
2466071-0-0-EN