# Post-Incident Activity Stage

In this stage, our objective is to document the incident and improve our capabilities based on lessons learned from it. This stage gives us an opportunity to reflect on the threat by understanding what occurred, what we did, and how our actions and activities worked out. This information is best gathered and analyzed in a meeting with all stakeholders that were involved during the incident. It generally takes place within a few days after the incident, when the incident report has been finalized.

## Reporting

The final report is a crucial part of the entire process. A complete report will contain answers to questions such as:

- What happened and when?
- Performance of the team dealing with the incident in regard to plans, playbooks, policies, and procedures
- Did the business provide the necessary information and respond promptly to aid in handling the incident in an efficient manner? What can be improved?
- What actions have been implemented to contain and eradicate the incident?
- What preventive measures should be put in place to prevent similar incidents in the future?
- What tools and resources are needed to detect and analyze similar incidents in the future?

Such reports can eventually provide us with measurable results. For example, they can provide us with knowledge around how many incidents have been handled, how much time the team spends per incident, and the different actions that were performed during the handling process. Additionally, incident reports also provide a reference for handling future events of similar nature. In situations where legal action is to be taken, an incident report will also be used in court and as a source for identifying the costs and impact of incidents.

This stage is also a great place to train new team members by showing them how the incident was handled by more experienced colleagues. The team should also evaluate whether updating plans, playbooks, policies, and procedures is necessary. During the post-incident activity state, it is important that we reevaluate the tools, training, and readiness of the team, as well as the overall team structure, and not focus only on the documentation and process front.

We will explore the reporting part of the Incident Handling Process in more detail in the `Security Incident Reporting` module of the `SOC Analyst` job role path.

Enable step-by-step solutions for all questions

### Questions

Answer the question(s) below to complete this Section and earn cubes!

+1 True or False: We should train junior team members as part of these post-incident activities.

True

Submit

Previous Finish

Go to Questions

Table of Contents

Introduction

Incident Handling

Cyber Kill Chain

The Incident Handling Process

Incident Handling Process Overview

Preparation Stage (Part 1)

Preparation Stage (Part 2)

Detection & Analysis Stage (Part 1)

Detection & Analysis Stage (Part 2)

Containment, Eradication, & Recovery Stage

Post-Incident Activity Stage

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left