

Incident Response Lifecycle

Reading

1h15m - 2h

✓ Status

Incomplete

Introduction

The Incident Response Life Cycle is a structured approach to handling cyber security incidents, which divides the process into four distinct phases: Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post Incident Activity. As you start a career in cyber security, understanding the Incident Response Life Cycle is essential, as it provides a framework for responding to security incidents in a systematic and efficient manner.

By breaking down the incident response process into four phases, the Incident Response Life Cycle helps security professionals to identify potential threats, contain and mitigate the impact of incidents, and ultimately learn from past incidents to improve their organization's overall security posture. In this reading, we will delve deeper into each of the four phases of the Incident Response Life Cycle and explore best practices for responding to cyber security incidents.

Instruction

As you read the below article, make note of the sample check lists presented to you.

These make excellent starting points that you can use. The Table 3-5 Incident Handling Checklist is an important resource for you, as it can give you the start of a basic workflow, telling you how our position in the SOC, or as an Analyst, may function.



Remember that this is a short, basic example, and in real life we might have a much longer and more granular list.

External Reading

The following information is condensed from the [NIST Special Publications 800-61v2](#).

The full publication is about 79 pages, and contains good, relevant usable information on Computer Security Incident Handling, as its name might imply. It is a good idea to have an overall familiarity with its content, but for today's reading we are going to focus on the Incident Response Life Cycle, to see how it applies to the creation of IR Policy and Playbooks. You might have come across this article in a previous course as further reading. If so, this should be a breeze!

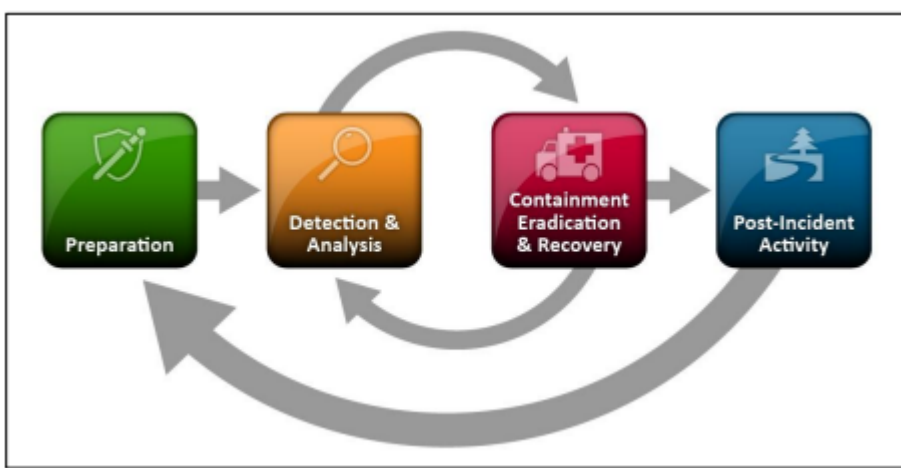


image source: NIST

The [Incident Response Life Cycle](#) divides the interactive process of Security Development into 4 phases:

1. Preparation
 - The home of Policy and Procedure preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
 - The home of our Playbooks
4. Post Incident Activity

As you can see from the diagram, this is an iterative process. That is, it is ongoing and, ideally, it is a process that learns from its mistakes and aims to correct them to ensure better preparation and performance in the future.

i Read carefully pages 12 through 45 of the PDF and consider how you did, or did not, follow this process in the Case Study in Unit 2.

Preparation Phase

Do you see how you “Prepared” by learning about the company, but that further information could be used to make a better plan? It is also worth noting that in the Preparation phase you also initiate the basic protections, firewalls, MDR, IPS for example, as well as set up the organization’s capacity to respond, the CSIRT team for example.

In this phase you are also informed by Policy and Procedure on how to respond, not specifically the tools or exact methods (those come later), but with an overarching guidance.

Detection and Analysis phase,

This is where as a blue team mainly spends their time. As a blue team, you plan to fail. You know that as good as you may set up your Preparations, the Bad Actors may, or more likely will, still get by you, or at the very least you must plan for this.

As an Analyst you depend on the setup done in the Preparation Phase, and on the technologies implemented there, to “see” when an event occurs, you depend on the sensors, logs and captures that monitor the day to day activities on the organization’s systems.

Containment, Eradication and Recovery.

At this point, determining that an incident has occurred, an incident specific Playbook or a SOP (Standard Operating Procedure) prepared in the Preparation phase may be enacted. This set of directions should give specific instructions and immediate actions, previously approved and permitted in Policy, to perform to contain the issue, clean it up and get business operations back to normal. It may take several iterations between the Containment, Eradication and Recovery phase and the Detection and Analysis phase as the later will confirm that the process was successful or that further actions are needed. You should also note that in complex attacks, several playbooks may be initiated.

Post Incident Activity

After the incident is closed, we conduct the Post Incident Activity. This is done AFTER the incident is closed because recommendations from this phase may include comments or suggested improvements that include the closing process. In fact Lessons Learned, though often omitted or down played, are at the heart of this iterative process as it provides feedback to the Preparation phase, that then may in turn make changes to the other phases.

Conclusion

As part of a larger process, creating a Playbook depends on an already established and mature IR infrastructure. The Playbook depends on the inputs from the Detection Phase and its goal is to close the incident in the Containment, Eradication and Recovery Phase.

Review Questions

Answer all of the questions below to review your understanding. Try to answer them in your own words.

?

During the Preparation phase, you are tasked with setting up the organization's capacity to respond to incidents. What key components and considerations should you focus on to ensure effective incident response?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

?

After a significant security incident, your team conducts a Post Incident Activity review. What are some key elements that should be included in this review to improve future incident responses?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

✓ Mark Completed

←

Previous

Review and Recommendations of Playbook

Next

The Incident Escalation Process

→

How well did this activity help you to understand the content?



W06D3

Wed Jul 31

> Lectures (1)

✓ Work (5)


8 hrs

 NIST 7 Step Process

 Incident Playbook Case Study

 Review and Recommendations of Playbook

 Incident Response Lifecycle

 The Incident Escalation Process

[W06D3 Schedule »](#)