The Incident Escalation Process

Reading

40m

Status | Incomplete

Introduction

It's important to understand that not all incidents can be handled by first responders or level 1 SOC desk analysts. When the time comes, it is essential to make the call to escalate the incident quickly to another individual.

Beginning with the resources listed, read about and get comfortable with the defining characteristics of an escalation. See if you can come up with at least five different examples of incidents that would require, or include, different types or ways of escalating the incident handling procedures in a standard security playbook for an organization.

You can use the business you used for your stakeholder case study from Unit One if you wish, to aid you.

Required Reading

In this reading from MicroFocus - Incident Escalation, you get a glimpse of how escalations could look, and an understanding that escalation is not a "one size fits all" way of dealing with an issue, but must fit the specific circumstance or incident.

> Read the following article Incident Escalation (process SO 2.6) paying close attention to the Incident Escalation workflow.

Here are some important points to note for discussion:

- As is stated in the reading, escalation occurs when a first level responder cannot meet service level agreements (SLAs). What does this mean? An SLA often outlines items like response times and times to fix.
- The understanding is, given a relatively straight forward playbook, the analyst should be expected to complete the play in a known amount of time. If they can't, then escalation should occur.
- There are other causes of escalation to consider as well. The incident might be out of scope for the analyst; that is, too high a level or too damaging, though the playbook should include this and have escalation as part of its actions.
- Escalation may also occur if the analyst does not have sufficient resources to handle a specific incident. This might occur if, for example, the analyst has to pass the ticket on to a data or network analyst.

Further Reading

This reading details escalation as a business process, a slightly but not too dissimilar view of the escalation process.

> Read the following articles and make notes of the differences in escalation practices - [Introduction to Escalation]() and [Evaluating your business process and customizing events]()

> As you scroll through the document, use the left hand navigation to explore more topics under the ‘Best Practices for Escalation’ drop down.

Key Takeaways

- Escalation is a normal part of the processes that are included in a playbook and workflow for an organization.
- Escalations can take many forms and are therefore often not due to a particular urgency, but can be simply dependent on job specialization or team member function that is required.
- Escalations are not a sign of the inability to achieve a goal, but can be a normal and required step in the process of completing a particular procedure.

Conclusion

Escalation is a key part of the business processes incorporated in a playbook or SOP. As such, emphasis must be placed on the fact that they are normal, and not a sign of failure on the part of the SOC analysts in any way.

✓ Mark Completed

← Previous
Cover Letters

Next
Incident Escalation Research →

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D2

Tue Jul 30

› Lectures (1)

⌄ Work (8)

6 hrs

- Report on Company Types and Stakeholders
- Group Share and Feedback
- Recognizing an Incident
- Playbooks and Escalation
- Cover Letters
- The Incident Escalation Process
- Incident Escalation Research
- IR Quiz

W06D2 Schedule »

Powered by Lighthouse Labs.