Incident Escalation Research

Task

45m

Status | Incomplete

Introduction

For this task, you are asked to research a specific industry incident type and develop or discuss what types of escalations might occur within the playbook or workflow for responding to that type of incident.

Select one of the incidents below to research:

- Distributed denial-of-service (DDoS) attack
- Malware
- Ransomware
- Phishing
- other incident of your choice

For the incident you selected, find a single reported example of this type of incident

Research Resources

- To learn more about the incident type you chose, try searching for current examples of that kind of incident on the Internet and read stories about what happened.
- Resources such as the ones listed below provide up-to-date information about current events. These are a good starting point for staying informed on the latest computer incidents.
- Practice your research skills by seeking out these resources online, reviewing them, and extracting the information needed to determine the escalation required.

It's important to keep in mind that the information provided on these sites may not be exhaustive and may not cover all the incidents that happen in the cyber world.

- US-CERT: the United States Computer Emergency Readiness Team (US-CERT) provides information on recent cyber incidents, vulnerabilities, and threats. It also provides guidance on how to protect against these incidents.

- CERT-EU: the European Union Agency for Cybersecurity (ENISA) operates the Computer Emergency Response Team for the EU (CERT-EU) which provides information on recent cyber incidents, vulnerabilities, and threats affecting the EU.
- National Cyber-Forensics & Training Alliance (NCFTA): NCFTA is a non-profit organization that provides information on recent cyber incidents, vulnerabilities, and threats, as well as threat intelligence and analysis.
- Cybersecurity Ventures: Cybersecurity Ventures is a research firm that provides information on the latest Cyber Security incidents, trends, and predictions.
- KrebsOnSecurity: KrebsOnSecurity is a well-known website that provides in-depth coverage of the latest cyber incidents, threats, and vulnerabilities.
- DarkReading: DarkReading is a website that provides news and analysis on cyber threats, vulnerabilities, and incidents, as well as best practices for protecting against them.
- The Hacker News: The Hacker News is a website that provides news and analysis on the latest cyber incidents, vulnerabilities, and threats, as well as information on hacking techniques and tools.

Research Tips and Questions

After reviewing the required resources, create a document to address the following issues in your research:

- Should this be immediately escalated?
- Which group was impacted by this?
- How many individuals were impacted?. How extensive was the damage or disruption, if any, that was disclosed?
- Who would we escalate this to (assuming we had input into this decision)?
- What secondary escalations might occur, and what might trigger them?

> ☞ Respond in paragraph form to the questions above. Post your response in Discord. Reply, giving constructive criticism or suggestions, to improve two other postings by your peers. Add anything else you think is relevant and interesting. Review your own feedback and update your report before adding to your PKM portfolio.

Conclusion

By the end of this exercise you should have an understanding of what escalations are and what kind of roles they play in the creation of playbooks and the completion of organization procedures and workflows.

✓ Mark Completed

← Previous
The Incident Escalation Process

Next
IR Quiz →

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 »