Incident Playbook Case Study

Task

2h

Status | Incomplete

Introduction

In this case study, you will document the various pieces of information required to write an incident playbook for a specific type of incident happening in a specific company. Specifically, you will:

- Utilize the NIST seven step incident process.
- Collect the information required to create an incident playbook.

> This playbook will be submitted in a future project IR Plan, Playbook and Policy.

Scenario - It’s All About Knowing What’s Next

> For this case study, you will work with one other student from the class.

As members of the CSIRT in your organization, you and a colleague have been tasked with collecting and documenting the information required to create an incident playbook to respond to a particular type of incident. Once collected, you have been asked to organize and populate the incident playbook with all the customized particulars for your organization.

Step-by-Step Instructions

Part 1: Develop Your Playbook

For this scenario you will be creating an incident response plabook by following the steps below:

- Review the following links and choose a template you like: 1) Cybersecure Canada, Incident Response Plan template & example 2) CISA, Incident and Vulnerability Response Playbooks 3) Following the NIST RMF 7 Step process 4) NIST, Computer Security Incident Handling Guide 5) FRSecure, IR Plan Template 6) Cynet, Incident Response Plan Template sources
- From your chosen site, download/create the template for your playbook.
- The Jumphost already has LibraOffice installed. You can use LibraOffice to directly edit your playbook template.

- Alternatively, you may also download a template and transfer the content to a Google Doc for editing.

Use the Incident Response Playbook template found on your chosen site for the specific incident and technical aspects of the playbook you are creating. Combine it with the additional information you collect from the specific company you have chosen and the individuals and assets you identify that are specific to your chosen situation. Include as much information as you can.

1. To fill in company information for the playbook, select company information posted by a student NOT in your group from the Unit 1 Company Types and Stakeholders Case Study.
2. For the incident type you choose, fill in as much information as you can.
3. The information that is real world (that you can find), put an asterisk (*) beside it.
4. Information that you make up, put an exclamation mark (!) beside it
5. Items you are unsure of, put a question mark (?) beside them

> ⚠ Make sure you include detailed information in ALL seven steps.

1. From your detailed playbook, select five items where you feel escalations may be triggered, for example if “Systems Affected” includes servers, and explain your choice and reasoning.

   > ❓ Who might the escalation go to?

2. Next, select five items where stakeholders would need to be informed of the incident and detail the types of information that would need to be communicated and why.

   > ❓ Are there any specific types of information that should not be communicated?

   > 👉 Be sure to include a cross section of both internal and external stakeholders to communicate with.

3. Save the Playbook to your PKM.

Part 2: Case Study Reflection and Data

1. Write a brief document reflecting on your experience doing this, and any questions you may have.
2. Looking at the playbook you created, ask yourself the question “What policies need to be in force to run the playbook?”
3. Add them to your writeup with a rationale as to why you have included them. For example, if under Detect you conduct scans, do you have a policy that allows this?

Incident Playbook Case Study Data Template (Sample Only)

Use the following Data Template to assist you in ensuring that you are gathering all the data you need. Hint, for contacts for this scenario use titles not names.

Data Name	Content	Rationale
Company Information		

Company Name		
Contact Title *(Position)*		
Contact Availability		
Contact data permissions (TLP)		
(Add extra as needed for escalation or reporting)		
Incident Info:		
Incident Name		
Incident Type		
C Effect		
I Effect		
A Effect		
Team Members (CSIRT)		
(add as needed)		
Internal Stakeholders		
(add as needed)		
External Stakeholders		
(add as needed)		
Company data classifications & prioritizations		
Categories of assets/devices that may be compromised		
Measurable metrics that would indicate the playbook has been completed and closed		
Reports that would need to be written and to whom and when		
Frequency at which the Playbook needs to be tested and re-evaluated		

Conclusion

Utilizing the NIST seven step incident process helps you to outline the required steps and information needed in order to respond to an incident. In this case study, you have begun to explore the breadth and depth of information required to customize a playbook to a specific organization and incident, as well as the ties between IR, playbooks, and company policies. As you move into a career in cyber security, practicing this skill will help you to make secure recommendations, with supporting arguments, for escalations and stakeholder reportings for a given IR and playbook.

✓ Mark Completed

← Previous
NIST 7 Step Process

Next
Review and Recommendations of Playbook →

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

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 Lifecyle
- The Incident Escalation Process

W06D3 Schedule »