Step-By-Step Instructions

Follow the instructions and fill in the sections to complete the activity.

Step 1: Access the incident report analysis

Access the the template (Incident report analysis)

Supporting materials:

Applying the NIST CSF

Step 2: Identify the type of attack and the systems affected

Think about all of the concepts covered in the course so far and reflect on the scenario to determine what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled “Identify.”

Step 3: Protect the assets in your organization from being compromised

ext, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

- What systems or procedures need to be updated or changed to further secure the organization’s assets?

Write your response in the incident report analysis template in the “Protect” section.

Step 4: Determine how the detect similar incidents in the future

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization’s network firewall.

For this step, consider ways you and your team can monitor and analyze network traffic, and software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the “Detect” section.

Step 5: Create a response plan for future cybersecurity incidents

After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

- How can you and your team contain cybersecurity incidents and affected devices?
- What procedures are in place to help you and your team neutralize cybersecurity incidents?
- What data or information can be used to analyze this incident?
- How can your organization’s recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template under the “respond” section.

Step 6: Help your organization recover from the incident

Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.

Consider the following questions:

- What information do you need to be able to recover immediately?
- What processes are in place to help the organization recover from the incident?

Write your response in the “recover” portion of the worksheet.

Step 7: Assess your activity

An evaluation of your incident report portfolio activity is provided below. These are the statements you'll use to evaluate your own work. Since the self-assessment process enables you to evaluate your incident report objectively, it is a crucial component of the learning process.