Activity Overview

In this activity, you will use the knowledge you've gained about networks throughout this course to analyze a network incident. You will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and create an incident report that you can include as part of your cybersecurity portfolio documentation. The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. For a refresher, please review this reading about NIST frameworks and the five functions of the NIST CSF framework. Creating a quality cybersecurity incident report and applying the CSF can help you build trust and improve security practices within your organization.

The CSF is scalable and can be applied in a wide variety of contexts. As you continue to learn more and refine your understanding of key cybersecurity skills, you can use the templates provided in this activity in other situations. Knowing how to identify which security measures to apply in response to business needs will help you determine which are the best available options when it comes to network security.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work. It will also provide an opportunity for you to answer rubric questions that allow you to reflect on key elements of your incident analysis.

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any

network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets
- Network monitoring software to detect abnormal traffic patterns
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy:

- **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.
- **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Instructions

Step 1: Access the incident report analysis template

To access template for this course item, click the following link and select *Use Template*.

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

Next, 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 to 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, 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.

Pro Tip: Save the incident report analysis template

Finally, be sure to save a copy of your incident report analysis worksheet somewhere accessible so that you can access it as you progress through the course and into the security field.

What to Include in Your Response

Later, you will have the opportunity to assess your performance using the criteria listed. Be sure to address the following in your completed activity.

Course 3 incident report analysis

- Identifies the type of attack and the systems impacted by the incident
- Offers a protection plan against future cybersecurity incidents
- Describes detection methods that can be used to identify potential cybersecurity incidents
- Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents
- Outlines recovery plans you and the organization can implement in future cybersecurity incidents.

Step 7: Assess your activity

The following is a self-assessment for your incident report portfolio activity. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your incident report.

There are a total of 6 points possible for this activity and each statement is worth 1 point. The items correspond to each step you completed for the activity.

To complete the self-assessment, first open your completed incident report document. Then respond yes or no to each statement.

When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity. The recommended passing grade for this project is at least 80% (or 4.8/ points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 5 points before continuing on to the next course item.