Activity: Document a timeline of events

Activity Overview

In this activity, you will construct an engaging visual timeline of events leading up to a security incident.

Cloud security analysts rely on documentation to communicate with their team, make decisions, and improve workflows. As you've learned, documentation conveys critical information because it provides historical insight into what happened previously, support for the present, and recommendations for the future. There are many forms of documentation that can be used. In incident response, some common forms of documentation include incident summaries, timelines, technical findings, and more.

Be sure to complete this activity before moving on. The next course item will quiz your comprehension, and then you'll be provided with a completed exemplar to compare to your own work.

Scenario

Review the following scenario. Then, access the supporting materials before moving on to the next course item to take the quiz.

As a cloud security analyst at Cymbal Bank, part of your role involves developing and implementing incident response processes and procedures. This includes creating processes like playbooks to protect Cymbal Bank's data and reputation.

Recently, a team member received a high-severity alert involving a phishing attempt. Over a week-long investigation into the alert, the team discovered that the employee who received the phishing email had mistakenly provided their cloud credentials through the phishing link. The team quickly worked on containing and remediating the attack.

This is the first time Cymbal Bank has experienced a severe phishing attempt after adopting cloud services. Cymbal Bank's executive leadership has been made aware of this alert and wants to use it as a learning opportunity to grow and develop their security awareness training program.

Your team lead, Chloe, is preparing a presentation for Cymbal Bank's executive stakeholders. The purpose of this presentation is to provide an executive summary about the incident findings. Chloe requested your help in developing a visual timeline of this security incident. The timeline will be included in the presentation so that nontechnical stakeholders can better understand the core details of this incident.

Chloe provided all of the technical findings about the alert. First, you'll analyze the technical findings to understand what happened, who was affected, and when the incident happened. Then, you'll organize the series of events into chronological order. Finally, you'll create an engaging visual timeline that captures the details of this security incident in a chronological order.

Step-By-Step Instructions

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your work to the exemplar provided.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.

🔔 **RIGHT CLICK LINKS TO OPEN IN NEW TAB** 🔔
Link to template: Phishing presentation template
Link to supporting materials: Alert ticket and technical findings

Step 2: Review the alert ticket

The **Alert ticket and technical findings** document contains the technical details about the phishing incident. Consider the following key details as you review it:

- The date and time of each event
- The name(s) of the user(s) affected
- The number of events leading up to the incident (user clicking on email, attacker using credentials, etc).
- The different types of malicious activity that happened after the incident

After you've scoped out the important details of the incident, you will need to present them in a way that's easy for Cymbal Bank's executive stakeholders to understand.

Note: *The event timestamps are provided in Coordinated Universal Time (UTC). The format is **YYYY-MM-DDThh:mmTZD**. TZD is a time zone designator and if it's set to Z then it's set to UTC time zone.*

Step 3: Create a timeline

Use the **Phishing presentation** template to create a timeline of the incident. Review slides 1-3 to help you understand the purpose of the presentation. Go to slide 4, remember that Chloe has asked for your help developing this part of the presentation only. Chloe will complete the remaining slides in the presentation.

On the slide with the heading **A timeline of events** (slide 4), enter the details of the phishing alert into the timeline in chronological order:

- In the **Date** section, enter the date of the incident.
- In the **Time** sections, enter the time of each respective event. Ensure that you enter the time in the format "hh:mm."
- In the **Event** sections, enter a brief description **(1 sentence)** summarizing each respective event.

***Pro tip**: Optionally, you can use visual graphics and icons to improve the presentation of the timeline. For example, you could place a fishing hook graphic beside the phishing event in the timeline.*

Step 4: Access the quiz and answer questions about the incident timeline

Go to the next course item and answer the quiz questions. Then compare your work to the exemplar provided.

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following elements in your completed activity:

- The date and time of each event
- A description of each event
- A chronological ordering of the chain of events