Introduction

The capstone for this course has three parts, each one focusing on a different scenario:

- Part I: Identify **indicators of compromise**
- Part II: Write an incident report
- Part III: Provide a leadership briefing

This part of your capstone involves answering a series of multiple-choice questions based on a scenario. In this scenario, you are a cybersecurity analyst who is responsible for reviewing the alerts from the organization's **security incident and event management** (SIEM) tool. You will answer a variety of questions to demonstrate your knowledge and skills in identifying **indicators of compromise** (IOCs).

Need help? We're here for you! Just click the bottom-right chat button.

Autograded

Final capstone: Identify indicators of compromise

For this assessment, you will read each scenario and select the best option based on the information provided about the IOC.

Please click **Start** when you are ready to begin the activity.

You receive an alert indicating that user credentials have been compromised through a brute force attack. Which of the following is most likely the indicator of compromise for this attack?

A	A large number of user logon failures
B	Network traffic between an internal host and an external IP address known to be malicious
C	Unexpected compressed files found on a system
D	Unexpected service running on a web server

For each of the questions below, you are a cybersecurity analyst responsible for reviewing alerts that come from the organization's SIEM.

You see several alerts related to a user workstation. Which of the following would be an indicator of compromise?

A	A user logged into a workstation at 9:12am
B	Windows updates are ready
C	A new version of Microsoft Office has been installed
D	Numerous failed login attempts followed by a successful login

Which of the following could be an IOC?

A	A user logged into a workstation during normal business hours
B	Windows update service detected running on a workstation
C	Anti-malware software updated its software package
D	A user had multiple failed login attempts within a short period of time

Which of the following is an IOC of a whaling attack?

A	A malware infected email suddenly starts sending to a large amount of users based on their address books
B	The email server goes offline due to an influx of data
C	The CEO receives a fraudulent email claiming to be from a customer needing a wiring transfer
D	None of the above describe an IOC for a whaling attack

Lesson 2

Final capstone: Write an incident report

2 hours Estimated completion time

Overview

In this lesson, you'll complete the second part of your final capstone project. In completing this lesson, you'll demonstrate your knowledge of how to analyze event alerts and follow proper incident response procedures by writing an incident report.

Introduction

In this second part of your capstone, you will **write an incident report** about the **2017 Equifax data breach.** Some of this will be done with the resources provided below and some using your own independent research.

Introduction

In this second part of your capstone, you will **write an incident report** about the **2017 Equifax data breach.** Some of this will be done with the resources provided below and some using your own independent research.

Instructions: Write an incident report

Downloading and saving the template

To complete this assignment, you will need to download the template. Both Word and PDF versions are provided below.

- Course 3 Capstone Part II – Write an incident report template (Word)
- Course 3 Capstone Part II – Write an incident report template (PDF)

Once you've downloaded the document, we recommend that you upload it to Google Drive. Use **Open with Google Docs** to keep the formatting from changing.

You can refer to the ***Supplementary resources*** at the bottom of this page for videos that'll walk you through how to save and access these documents in Google Drive.

Completing your assignment

The following are some sources related to the 2017 Equifax Data Breach incident.

- CSO article
- Krebs on Security article
- NIST Vulnerability Database
- US GAO Equifax report

In addition to these sources, you may need to conduct additional research to complete this project.

- Download the final capstone incident template as a starting point for your report.
- You can refer to this exemplar of an incident report about a different data breach for an example of what your report might look like.
  - **IMPORTANT**: This example is about a *different* data breach that occurred at Target. **Your report will be about the Equifax data breach**.

Using the sources provided and your additional research, write an incident report summarizing the 2017 Equifax Data Breach incident. Include the following incident report sections:

1. **Executive summary.** Provide a high-level explanation that summarizes the breach. It should be no more than 2-4 sentences.
2. **A detailed summary of the incident.** This should include a description of what was compromised, a timeline of major events related to the breach, a summary of the internal and external parties involved, the ramifications of the breach, and the solutions put in place.
3. **Major findings from the incident.** This should include a discussion about vulnerabilities that contributed to the breach, as well as the indicators of compromise (IOCs) that led to the detection of the breach.
4. **Recommendations for remediation.** Recommend 2-3 actions or policies the facility can do or implement to prevent future breaches.
5. **Conclusion.** Summarize why the event is important to study as a cybersecurity professional.

Grading requirements

Remember, this is a graded lesson. That means that someone from the Thinkful team will review your work using the rubric provided below. Here are the specifics:

- **Grading rubric:** The graders will use the criteria in the following rubric when grading your work. All questions use a yes-no framework, unless otherwise indicated.
- **Additional feedback:** Graders will also use the rubric to provide you with feedback. This feedback does not affect whether you pass or fail; it is there to help you revise your work or improve upon it.
- **Passing score:** This assessment requires a passing score of 80%. Therefore, **at least 10 of the 12 items** on the grading rubric must be marked *Yes* for you to pass. It isn't expected that all students will pass the assessment on their first attempt. Use the feedback provided by the graders to improve your assessment and resubmit if needed.

Keep this information on hand as you work, and good luck!

Submission details

Once you've confirmed that all **12** requirements in the rubric below have been addressed, save a copy of your completed document somewhere it can be shared online. Make sure that the link access is set to **Anyone with the link**. Submit a link to your document in the box below. You'll receive feedback from a member of the Thinkful grading team.

If you need a refresher on how to share links from Google Drive, please refer to these instructions. You can also refer to the ***Supplementary resources*** below for a video that'll walk you through how to set your sharing preferences.

Need help? We're here for you! Just click the bottom-right chat button.

Graded Assignment

Final capstone: Write an incident report

To pass this part of your capstone, you'll need to meet the criteria outlined in the instructions and rubric above. When you're done, set the sharing preferences to your file as **Anyone with the link**, and then submit that link below. You'll receive feedback from a member of the Thinkful grading team.

Your work

bold _italic_ `code` > quote - bullet list

Submit

Lesson 3

Final capstone: Provide a leadership briefing

2 hours Estimated completion time

Overview

In this lesson, you'll create and submit a presentation to demonstrate your knowledge and skills in vulnerability management and threat assessment.

Key Terms

Common vulnerabilities and exposures	Known as CVE, a list of publicly known cybersecurity and technology vulnerabilities; a CVE assignment describes the vulnerability identification number and the vulnerability

Introduction

Well done! You have reached the last part of your capstone. In this lesson, you will create a presentation to share your incident report and make recommendations for actions that should be considered by your team.

Instructions: Provide a leadership briefing

Downloading and saving the template

To complete this assignment, you will need to download the template. Both PowerPoint and PDF versions are provided below.

- Course 3 Capstone Part III – Provide a leadership briefing template (PPT)
- Course 3 Capstone Part III – Provide a leadership briefing template (PDF)

Once you've downloaded the document, we recommend that you upload it to Google Drive. Use **Open with Google Docs** to keep the formatting from changing.

You can refer to the ***Supplementary resources*** at the bottom of this page for videos that walk you through how to save and access these documents in Google Drive.

Completing your assignment

Imagine you are the security lead for an IT team in 2017 when the Equifax breach occurred. Your manager has asked you to share your incident report with the team and make recommendations for action that should be considered by the team.

To do this, you'll need to create a presentation with 3-5 slides to summarize key information and your recommendations. You can refer to this example of a leadership briefing as a guide for what your report might look like and what type of content it might contain.

Be sure to include the following in your presentation:

1. **Provide a briefing of the incident.** Write your response as if you really are a security professional who's providing the information to a leader on your team.
2. **Describe the significance of the incident.** Your response should include information about who or what systems are affected, the scope of the issue, etc.
3. **Describe the known information about the threat actors involved.**
4. **Imagine yourself in the role of a cybersecurity analyst.** Summarize your recommendation for the next steps.
5. **List your information sources.** In your sources, be sure to include specific information on **common vulnerabilities and exposures** (CVE).

Grading requirements

Remember, this is a graded lesson. That means that someone from the Thinkful team will review your work using the rubric provided below. Here are the specifics:

- **Grading rubric:** The graders will use the criteria in the following rubric when grading your work. All questions use a yes-no framework, unless otherwise indicated.
- **Additional feedback:** Graders will also use the rubric to provide you with feedback. This feedback does not affect whether you pass or fail; it is there to help you revise your work or improve upon it.
- **Passing score:** This assessment requires a passing score of 80%. Therefore, **at least 5 of the 6 items** on the grading rubric must be marked *Yes* for you to pass. It isn't expected that all students will pass the assessment on their first attempt. Use the feedback provided by the graders to improve your assessment and resubmit if needed.

Keep this information on hand as you work, and good luck!

Submission details

Once you've confirmed that all six requirements in the rubric below have been addressed, save a copy of your completed document somewhere it can be shared online. Make sure that the link access is set to **Anyone with the link**. Submit a link to your document in the box below. You'll receive feedback from a member of the Thinkful grading team.

If you need a refresher on how to share links from Google Drive, please refer to these instructions. You can also refer to the ***Supplementary resources*** below for a video that'll walk you through how to set your sharing preferences.

Graded Assignment

Final capstone: Provide a leadership briefing

To pass this part of your capstone, you'll need to meet the criteria outlined in the instructions and rubric above. When you're done, set the sharing preferences to your file as **Anyone with the link**, and then submit that link below. You'll receive feedback from a member of the Thinkful grading team.

Your work

bold _italic_ `code` > quote - bullet list

Submit