Unit 10 Discussion 1: Incident Response Strategies

Learning Objectives and Outcomes

You will learn the phases of incident response and the team members involved who respond to incidents.

Discussion Requirements

You are provided a handout that describes a scenario in which an incident occurred along with corrective actions taken. The handout also includes a description of the phases of information security incident response.

Discuss the phases of a typical information security incident response. Using the information presented in the handout, discuss the following questions:

- What are the effective responses to a security breach?
- Which actions would you recommend for each phase?
- What is the significance of the incident response team members?

Summarize your thoughts in a Microsoft Word document and submit it to your instructor.
Respond to at least two other students' views to engage in a meaningful debate regarding their choices or to defend your choice.

Submission Requirements

Font: Arial 10 point size
Line Spacing: Double
Due: By Unit 10

Worksheet

Text sheet: Incident Response Strategies

Discussion Process Checklist

I have engaged in discussion of the assigned topic(s) with at least two of my peers. ☐

I have raised questions and solicited peer and instructor input on the topic(s) discussed. ☐

I have articulated my position clearly and logically. ☐

I have supported my argument with data and factual information. ☐

I have provided relevant citations and references to support my position on the issue discussed. ☐

I have compared and contrasted my position with the perspectives offered by my peers and highlighted critical similarities and differences. ☐

I have solicited peer and instructor feedback on my arguments and propositions. ☐

I have offered a substantive, critical evaluation of the peer's perspective on the discussed issue(s) that is opposite of mine, and supported my critical review with data and factual information. ☐

Discussion Summary Checklist

I have covered topical requirements assigned for this document. ☐

I have captured critical points of the discussion. ☐

I have summarized different perspectives offered by the discussants. ☐

I have summarized 2-3 major learning moments I experienced during the discussion. ☐

I have briefly discussed how my perspective changed or got validated through this discussion. ☐

I have provided feedback on how the discussion could be improved. ☐

I have followed the submission requirements: ☐

File Format:	Microsoft Word (.doc / .docx)
Length:	1-2 pages
Font:	Arial 10 point size
Line Spacing:	Double

Unit 10 Assignment 1: Postincident Executive Summary Report

Learning Objectives and Outcomes

You will learn how to write a postincident executive summary report detailing an incident event and corrective actions taken.

Assignment Requirements

You have been working as a technology associate in the information systems department at Corporation Techs for almost three months now. Yesterday, you got an e-mail, which specified that a security breach has occurred in your company. The other members of your team also received such e-mails. You checked the firewall logs and it confirmed the security breach.

Later, your team took corrective actions in the environment. They isolated the incident and assessed the damage. Today, your manager calls you and asks you to create an executive summary report detailing the events to be presented to executive management. You need to include a summary of corrective options, which may be in the form of architectural adjustments or other configuration changes that will prevent the reoccurrence of this incident in the future.

You need to create a postincident executive summary report that addresses a security breach. Include an overview of actions taken at each phase of the incident response. Also include suggestions for corrective modifications that would prevent the incident from reoccurring.

Submission Requirements

Font: Arial 10 point size
Line Spacing: Double
Due: By Unit 11