Southern New Hampshire University

CYB 200 Project Three Guidelines and Rubric

Overview

One of the three focus projects for this course is the creation of a **technical brief** based on research you've conducted. The audience for this brief is the security/IT director for a fictional organization at which you are employed for the purposes of this assignment. This technical brief will serve as the basis for a proactive adversarial detection plan that your director will be creating. The final product represents an authentic demonstration of competency because, as a security analyst, you will need to be able to develop skills that employ a variety of methods and tools necessary to detect, characterize, and counter cyber threat actors. Your work will contribute to larger team projects across your organization. This project will also help position you to cultivate an important mind-set: thinking responsibly, proactively, and in terms of what threat actors would do to attack organizational assets.

The project incorporates **one milestone**, which will be submitted in **Module Five**. The project will be submitted in **Module Seven**.

In this assignment, you will demonstrate your mastery of the following course competency:

- CYB-200-02: Develop reliable, ethical methods to detect, characterize, and counter cyber threat actors

Scenario

In a course announcement, your instructor will provide you with some scenarios for you to choose from. You will situate yourself as the security analyst in one of the provided scenarios, creating a technical brief that explains to the security/IT director how the situation informs the larger proactive adversarial detection plan that he or she is writing for the organization. You do not require specific technical information from the system at hand, as the results or determinations are supplied for you within the scenario. Rather, you should address each critical element in the Project Three prompt, speaking broadly to what your best-practice tactics or methods would be, based on your research from the decision aid you completed as the milestone for this project. The Conclusion section of this activity requires you to extrapolate on all the research you have done for the decision aid.

Prompt

In your technical brief, you must address the **critical elements** listed below. The codes shown in brackets indicate the course competency to which each critical element is aligned.

I. **Introduction**
   A. Identify your threat actors and **characterize** their motivations or desired outcomes. Use research from the Project Three resource guide or decision aid to support your response. For example, is the threat actor gathering information for financial gain? [CYB-200-02]

II. **Analysis**

A. Describe best practices or methods for **detecting the threat actors** from the scenario. Use research from the Project Three resource guide or decision aid to support your response. [CYB-200-02]

B. Describe **ethical and legal factors** that should be considered and their significance in terms of the company for which you are employed in the scenario. Use research from the Project Three resource guide or decision aid to support your response. [CYB-200-02]

C. Describe at least one tactic or method that is important in **responding to and countering this threat actor**. Use research from the Project Three resource guide or decision aid to support your response. [CYB-200-02]

D. Describe at least one tactic or method that would be employed to **reduce the likelihood** of the same situation happening again. Use research from the Project Three resource guide or decision aid to support your response. [CYB-200-02]

III. **Conclusion**

A. Explain the potential **ramifications** of the tactics or methods you have suggested. Use research from the resource guide or decision aid to support your response. [CYB-200-02]

Key Deliverables

Deliverable	Module Due	Grading
Project Three Milestone: Decision Aid	Five	Project Three Milestone Rubric
Project Three: Technical Brief	Seven	Project Three Rubric

Project Three Rubric

Guidelines for Submission: Your submission should be approximately 2 pages in length (plus a cover page and references) and should be written in APA format. Use double spacing, 12-point Times New Roman font, and one-inch margins. Include at least three references, which should be cited according to APA style. Use a file name that includes the course code, the assignment title, and your name—for example, CYB_200_Project_Three_Neo_Anderson.docx.

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Introduction: Characterize [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Identifies threat actors and characterizes their motivations or desired outcomes, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16

Southern New Hampshire University

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Analysis: Detecting Threat Actors [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes best practices or methods for detecting the threat actors, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16
Analysis: Ethical and Legal Factors [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes ethical and legal factors that need to be considered and their significance, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16
Analysis: Responding to and Countering Threat Actor [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes at least one tactic or method that is important in responding to and countering the threat actor, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16
Analysis: Reduce Likelihood [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes at least one tactic or method that would be employed to reduce the likelihood of the same situation happening again, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16
Conclusions: Ramifications [CYB-200-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Explains the potential ramifications of the tactics or methods suggested, using research from the resource guide or decision aid to support the response	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	16
Articulation of Response	Submission is free of errors related to citations, grammar, spelling, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations, grammar, spelling, or organization	Submission has some errors related to citations, grammar, spelling, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, or organization that prevent understanding of ideas	4
				Total	**100%**