Southern New Hampshire University

CJ 467 Milestone Two Guidelines and Rubric

For this assignment, continue creating a consolidated summary of the Suspicious Activity Reports (SARs) provided, and cover what is known about the nature and imminence of the potential threat and how to protect critical information from falling into the hands of the adversary. Use Suspicious Activity Reports #1 through #15. Your essay should be in two parts, labeled "Threat Assessment" and "Information Security."

The SARs can be found in the Assignment Guidelines and Rubrics section of the course.

Specifically, the following **critical elements** must be included:

III. **Threat Assessment**

In this section of the report, you should lay out what is known about the nature and imminence of the potential threat. You may wish to use the Threat Assessment Worksheet, found in the Assignment Guidelines and Rubrics section of the course, to record and analyze relevant information from Suspicious Activities Reports (SARs) in preparing your response. However, you should present the information from the worksheet in narrative form in your finished intelligence report.

A. Distinguish the **nature** of the threat, including specific potential target(s), the location of likely attack (if the target is an individual), and potential means of attack based on the summary information and analysis above. Draw out the elements that would be most important to the agency receiving the report in determining the threat and focusing their efforts.
B. Assess whether the adversary has the **intent**, opportunity, and capability to carry out a threatening behavior. Is the threat being actively pursued? Support your answer with information from the SARs.
C. Assess the **vulnerabilities** of the potential target(s) and law enforcement's ability to protect the target(s). Support your answer using information from the SARs and reasonable assumptions about potential vulnerabilities. For example, how tight is security for entry into a particular building? Could a target be threatened from a street location? Could law enforcement be impeded from quickly responding to a threat? Note that these questions are illustrative only, and the vulnerabilities that you identify should correspond to your analysis of the specific threat identified.
D. Using the analyses in Parts A–C above, assess the **current level of risk** using a scale from 0–10, with 0 being "no threat" and 10 being "great threat." How imminent is the threat? Is it going to happen now, next week, in the next year, never? What level of damage could the adversary inflict if they are successful in carrying out the threat? Justify your answer based on your analysis.
E. Recommend what **countermeasures**, if any, might be appropriate for addressing vulnerabilities and mitigating the potential threat that you identified above. Depending on your analysis, you may suggest multiple countermeasures, a single countermeasure, or no countermeasures. Be sure to support your answer using your threat assessment analysis and information from the SARs.

IV. **Information Security**

In this section of the report, you should address how to prevent critical information from falling into the hands of the adversary (i.e., operations security). You may wish to use the Operations Security Worksheet, found in the Assignment Guidelines and Rubrics section of the course, to record and analyze relevant information from the Suspicious Activity Reports (SARs) in preparing your response. However, you should present the information from the worksheet in narrative form in your finished intelligence report.

A. Assess what **critical information** surrounding the potential target and law enforcement activities to mitigate the threat needs to be protected. In other words, what information do we not want the adversary to have and why? Justify your answer.
B. Assess the **adversary's methods** for collecting intelligence about their target and law enforcement activities. Are they making multiple visits to the target? Are they using informants within the community? Are they doing research on the internet? Monitoring police bands? Taking pictures? What other methods might they be using? Support your answer using information from the SARs and reasonable assumptions.
C. Assess **potential weaknesses** in information security that might give away critical details about the target or law enforcement activities. Support your answer using information from the SARs and reasonable assumptions.
D. **Risk assessment**. Using the analyses in Parts A–C above, assess the current level of risk from information security weaknesses as high, medium, or low. In other words, how high is the risk that the adversary will obtain the critical information, and what level of damage could the adversary inflict if the information is acquired? Support your answer using information from the SARs and reasonable assumptions.
E. **Recommendations**. Suggest what countermeasures, if any, might be appropriate for addressing the information security vulnerabilities that you identified above. Justify these suggestions in terms of monetary cost versus effectiveness. How can we prevent or subvert the adversary's methods for collecting intelligence? How do we keep the adversary from knowing that we are aware of the threat and acting to avert it? Depending on your analysis, you may recommend multiple countermeasures, a single countermeasure, or no countermeasures. Be sure to support your answer using your operations security analysis and information from the SARs.

Guidelines for Submission: Milestone Two must be three to six pages in length with 12-point Times New Roman font, double spacing, and one-inch margins. Separate different sections with headings so that the reader can easily understand your information.

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Threat Assessment: Nature	Meets "Proficient" criteria and analysis is exceptionally articulate, modeling language that would be used in a real-world intelligence report and expertly balancing detail with brevity and clarity	Distinguishes the nature of the threat, including specific target(s), location (if target is an individual), and potential means of attack based on analysis of SARs, emphasizing elements that would be most important to the agency receiving the report in determining the threat and focusing their efforts	Distinguishes the nature of the threat based on analysis of SARs, but does not emphasize elements that would be most important to the agency receiving the report	Does not distinguish the nature of the threat based on analysis of SARs	10

Threat Assessment: Intent	Meets "Proficient" criteria and assessment is exceptionally articulate, modeling language that would be used in a real-world intelligence report and expertly balancing detail with brevity and clarity	Assesses whether adversary has the intent, opportunity, and capability to carry out a threatening behavior and whether threat is being actively pursued, supported by relevant information from the SARs	Assesses whether adversary has intent, opportunity, and capability to carry out a threatening behavior and whether threat is being actively pursued, but assessment is not supported by relevant information from the SARs	Does not assess whether adversary has intent, opportunity, and capability to carry out a threatening behavior or whether threat is being actively pursued	10
Threat Assessment: Vulnerabilities	Meets "Proficient" criteria and analysis addresses a broad spectrum of vulnerabilities surrounding the potential target and law enforcement activities in this threat scenario	Assesses vulnerabilities of the potential target(s) and law enforcement's ability to protect the target(s), supported by information from the SARs and reasonable assumptions	Assesses vulnerabilities of potential target(s) and law enforcement's ability to protect target(s), but analysis is not supported by information from SARs and reasonable assumptions	Does not assess vulnerabilities of the potential target(s) or law enforcement's ability to protect the target(s)	10
Threat Assessment: Current Level of Risk	Meets "Proficient" criteria and analysis of imminence and potential damage is particularly well supported	Assesses the current level of risk, including imminence and potential damage, using a scale from 0–10, and justifies rating based on analysis of SARs	Assesses current level of risk, including imminence and potential damage, using a scale from 0–10, but does not justify rating based on analysis of SARs	Does not assess current level of risk, including imminence and potential damage, using a scale from 0–10	10
Threat Assessment: Countermeasures	Meets "Proficient" criteria and recommendations are particularly well aligned with specific needs of the scenario and real world constraints	Recommends what countermeasures, if any, might be appropriate for addressing vulnerabilities and mitigating the threat identified, supported by threat assessment analysis and information from the SARs	Recommends what countermeasures, if any, might be appropriate, but recommendations are not supported by threat assessment analysis and information from the SARs	Does not recommend what countermeasures, if any, might be appropriate for addressing vulnerabilities and mitigating the threat	10
Information Security: Critical Information	Meets "Proficient" criteria and justification is particularly well supported	Assesses what critical information surrounding the potential target and law enforcement activities to mitigate the threat needs to be protected, and justifies response	Assesses what critical information needs to be protected, but does not justify response	Does not assess what critical information needs to be protected	10
Information Security: Adversary's Methods	Meets "Proficient" criteria and assessment addresses a broad and realistic spectrum of methods given the parameters of this threat scenario	Assesses the adversary's methods for collecting intelligence about target and law enforcement activities and supports answer using information from SARs and reasonable assumptions	Assesses adversary's methods for collecting intelligence, but does not support answer using information from SARs and reasonable assumptions	Does not assess adversary's methods for collecting intelligence	10

Information Security: Potential Weaknesses	Meets "Proficient" criteria and assessment addresses a broad and realistic spectrum of potential information security weaknesses given the parameters of this threat scenario	Assesses potential weaknesses in information security, and supports answer using information from the SARs and reasonable assumptions	Assesses potential weaknesses in information security, but does not support answer using information from the SARs and reasonable assumptions	Does not assess potential weaknesses in information security	10
Information Security: Risk Assessment	Meets "Proficient" criteria and assessment of likelihood of breach and potential damage are particularly well supported	Assesses the current level of risk from information security weaknesses, including likelihood of adversary obtaining information and the damage that could be inflicted, using a high-medium-low scale, and supports assessment with information from SARs and reasonable assumptions	Assesses the current level of risk from information security weaknesses, using a high-medium-low scale, but does not support with information from SARs and reasonable assumptions	Does not assess the current level of risk from information security weaknesses	10
Information Security: Recommendations	Meets "Proficient" criteria and suggestions are particularly well aligned with the specific needs of the scenario and real-world constraints	Suggests what countermeasures, if any, might be appropriate for addressing information security vulnerabilities, supported by operations security analysis and information from SARs	Suggests what countermeasures, if any, might be appropriate, but recommendations are not supported by operations security analysis and information from SARs	Does not suggest what countermeasures, if any, might be appropriate for addressing information security vulnerabilities	10
				Earned Total	**100%**