**Cybersecurity Course 2 Capstone: Part I**

**Student Template**

**Scenario 1: Analyzing SIEM alerts**

You recently joined your organization’s cybersecurity team as an analyst. You have been reviewing the SIEM tool for alerts. You come across the 10 alerts listed below. For each of the alerts, answer the following question by filling out the appropriate fields in the template:

* **Question: Does the alert represent an issue that should be escalated?**
  + **If yes**, please provide a short, three-part justification for the incident response. Please be sure to include the following information in your answer:
    - Brief description of the potential impact of the issue
    - Immediate action to mitigate the immediate risk
    - Recommended security control to resolve the issue going forward
  + **If no**, explain why the issue does not need to be escalated and justify your decision to dismiss the alert.

**Grading criteria**

* All parts of the justification must be correct to earn credit for each question.
* 8 of 10 alerts must be correct to pass Scenario 1.

**Sample alerts and answers**

Here are two example alerts that demonstrate how you’ll respond to the alerts in this template. The first shows what a “yes” answer might look like, and the second shows what a “no” answer might include.

These example alerts demonstrate the type and level of information that will be expected in your responses to the 10 alert questions below.

Remember, the examples are just a guide. The specific answers that are shown for the example alerts will *not* be the same answers that you’ll need for the 10 graded alerts below. Be sure to read the alerts carefully and provide your own answers.

**Example Alert 1: Data Modification – Large number of files deleted**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. First, it is important to identify who deleted the files. It could be harmless, such as purging outdated documents to meet retention requirements. However, it could also be a malicious action by either a disgruntled employee or a hacker trying to create a disruption in business operations. Having important business files deleted before they are intended to be destroyed disrupts the availability of the data.
2. **Describe any recommended immediate action to address the event.** 
   1. An immediate action to take is to disable the user account conducting the activity, followed by identifying if it is being accomplished by an insider threat (such as a disgruntled employee) or a hacker.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. It is important to ensure that proper access control rules are assigned to applications and data. Additionally, data loss prevention technologies can allow for data tagging so that the organization can control who has access to data as well as identify which data is classified at what data levels for real-time protection.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Example Alert 2: Data Modification - New user added to primary AD group by HR admin**

**Question**: Should this issue be escalated?

**Answer**: No

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.**
2. **Describe any recommended immediate action to address the event.**
3. **Provide your recommendation for a security control to mitigate risk moving forward.**

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**
   1. HR administrators are often the personnel who either add or request to have new employees added to AD groups. Many companies have a primary AD group which gives them access to basic tools that all employees need to access.

**Analyze the following 10 SIEM alerts**

For each of the 10 alerts below, please provide answers describing how you should respond as an analyst. Refer to the example alerts above for guidance on how to answer the questions.

**Note**: These are the 10 alerts you will be graded on. Be sure to enter your answers directly onto this template in the relevant fields below.

**Alert #1: Certificate error – There is a problem with a website’s security certificate**

**Question**: Should this issue be escalated?

**Answer**: No

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.**
2. **Describe any recommended immediate action to address the event.**
3. **Provide your recommendation for a security control to mitigate risk moving forward.**

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**
   1. This alert doesn’t necessarily need escalation as certificate errors can occur due to various reasons, including temporary server issues or misconfigurations. They don’t always indicate a breach.

**Alert #2: C&C communication – An internal device connected to an IP address that has been used as a command-and-control server**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Connecting to a command and control server indicates potential malicious communication, jeopardizing confidentiality, integrity, and availability of data and systems
2. **Describe any recommended immediate action to address the event.** 
   1. Isolate the affected device, conduct a thorough investigation, and contain any potential malware/ Identify affected systems and assess the extent of the compromise.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement advanced threat detection mechanisms and endpoint protection to identify and block malicious communication patterns.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #3: Privilege escalation – A system was accessed by an unexpected account with administrative privileges**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Unauthorized access with administrative privileges can lead to data manipulation, theft, or system damage, compromising confidentiality, integrity, and availability.
2. **Describe any recommended immediate action to address the event.** 
   1. Isolate the affected system, revoke the unauthorized privileges, change passwords, and conduct a thorough investigation to identify the source and intent of the unauthorized access.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement the principle of least privilege and multi-factor authentication to reduce the likelihood of unauthorized access and privilege escalation.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #4: Account status change – User was added to a different group, removed from a group, or added to the security group by user IT\_User\_Admin**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Unauthorized changes to user account status or group memberships can lead to potential security breaches, compromise of sensitive information, or misuse of privileges, affecting confidentiality, integrity, and availability.
2. **Describe any recommended immediate action to address the event.** 
   1. Investigate the changes made to the user account status or group memberships to ascertain if they were legitimate or unauthorized. If unauthorized, revoke the changes and restore the original account status and group memberships. Assess the impacted account for any signs of compromise and potential abuse of privileges.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement robust access controls and auditing mechanisms to detect and prevent unauthorized changes to user accounts and group memberships. Implement a principle of least privilege to ensure that users have the minimum level of access required to perform their duties, mitigating the risk of unauthorized changes.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #5: Device login – A user account logged into a desktop computer**

**Question**: Should this issue be escalated?

**Answer**: No

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.**
2. **Describe any recommended immediate action to address the event.**
3. **Provide your recommendation for a security control to mitigate risk moving forward.**

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**
   1. This alert does not need escalation because it is a routine activity for a user to log into a desktop computer. Logins are expected behavior and do not necessarily indicate a security threat.

**Alert #6: Service change – Anti-malware service stopped on a host**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. The stopping of the anti-malware service on a host poses a significant threat as it leaves the system vulnerable to malware and other malicious activities. This impacts the confidentiality, integrity, and availability of the system and potentially the entire network.
2. **Describe any recommended immediate action to address the event.** 
   1. Investigate the reason for the anti-malware service being stopped. It could be due to a malfunction, misconfiguration, or malicious activity. If the stoppage is due to a legitimate reason (maintenance), ensure it is reinstated promptly after ensuring the activity is authorized and secure. If the stoppage is suspicious or malicious, isolate the affected system and perform a thorough security analysis to identify and mitigate any potential threats.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement intrusion detection and prevention systems to monitor and detect unusual activities, including unauthorized attempts to stop critical services. Utilize security monitoring tools that provide real-time alerts and automated responses to service disruptions, enabling swift action to mitigate potential threats.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #7: Logon/Logoff pattern – User login outside of normal pattern**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. An abnormal login/logoff pattern can indicate potential unauthorized access or a compromised user account. This could impact the confidentiality, integrity, and availability of data and systems.
2. **Describe any recommended immediate action to address the event.** 
   1. Investigate the abnormal login/logoff pattern to determine if it's a legitimate activity or a security threat. If it's unauthorized access, immediately revoke access and change passwords for the affected account. Analyze affected systems for any signs of compromise or malicious activity.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement anomaly detection mechanisms to monitor user login patterns and trigger alerts for suspicious activities. Utilize behavior analysis tools to establish a baseline of normal user behavior and detect deviations from this baseline, enabling rapid identification of potential threats.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #8: File integrity – Evidence log files were deleted or tampered with**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Tampering or deletion of evidence log files could indicate an attempt to hide unauthorized access or activities. This threatens the integrity and potentially the confidentiality of the data, impacting the organization's ability to accurately assess security incidents.
2. **Describe any recommended immediate action to address the event.** 
   1. Isolate the affected system to prevent further tampering or potential data loss. Preserve any remaining evidence for forensic analysis to determine the extent of the tampering and identify the source. Assess the system and logs to identify any signs of compromise or malicious activity.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement robust access controls and monitoring systems to ensure that only authorized individuals have access to critical log files. Utilize file integrity monitoring systems to detect and alert on any unauthorized changes to critical log files.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #9: Geographic login disparity – A user attempted to log in from places that are geographically separated by a long distance in a short amount of time.**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Attempted logins from geographically distant locations within a short timeframe can indicate potential unauthorized access or a compromised account. This threatens the confidentiality and potentially the integrity of the data and systems.
2. **Describe any recommended immediate action to address the event.** 
   1. Investigate the login attempts to confirm their legitimacy or identify potential unauthorized access. If unauthorized access is confirmed, immediately revoke access, change passwords, and secure the affected account. Perform a thorough security analysis to determine the extent of the breach and assess the potential risks.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement geolocation-based login restrictions to allow logins only from authorized regions or countries. Utilize multi-factor authentication (MFA) to provide an additional layer of security and verify the identity of users attempting to log in from new or unusual locations.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**

**Alert #10: Log-on/log-off pattern – Excessive login attempts for a user**

**Question**: Should this issue be escalated?

**Answer**: Yes

* **If you answered *Yes*:**

1. **Briefly describe the potential impact of the issue, including its potential impact to C.I.A.** 
   1. Excessive login attempts may indicate a brute force attack, risking unauthorized access to the user account or system. This threatens the confidentiality, integrity, and availability of data and systems.
2. **Describe any recommended immediate action to address the event.** 
   1. Investigate the login attempts to confirm if they are legitimate or potentially malicious. If it appears to be a brute force attack, lock the affected user account temporarily to prevent further unauthorized login attempts. Assess the logs for patterns or indicators of compromise.
3. **Provide your recommendation for a security control to mitigate risk moving forward.** 
   1. Implement account lockout policies to lock user accounts after a defined number of unsuccessful login attempts, preventing brute force attacks. Utilize CAPTCHA or reCAPTCHA mechanisms to differentiate between automated bots and genuine users, adding an additional layer of security during login attempts.

* **If you answered *No*:**

1. **Provide your reason for dismissing the alert.**