STUDENT WORKSHEET, Capstone 2 Scenario 1

Student Name: Leonard Sterling

Scenario 1: Analyzing SIEM Alerts

You have recently joined your organization's cybersecurity team serving as an analyst. You have been reviewing the SIEM for alerts and found the following alerts that you need to respond to. For each of the following alerts, please provide answers to the following question:

- Does the alert represent an issue that should be escalated?
    - If yes, please provide a short briefing serving as justification for the incident response. Please be sure to include the following information:
        - Brief description of the potential impact of the issue
        - Immediate action to mitigate the risk
        - Recommendation of security control to resolve the issue
    - If no, explain why not and give justification for dismissing the alert.
- 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.

Exemplars

Here are two examples that demonstrate how you'll respond to the alerts in this worksheet. The first shows what a "yes" answer might look like, and the second shows what a "no" answer might include.

Exemplar 1 **Alert:** Data Modification – Large number of files deleted
Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   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 It could be harmless, such as purging outdated documents to meet retention requirements.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.**
   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.**
   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 No:

1. Reason for dismissing alert.

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

Should this issue be escalated?

If 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 No:

1. **Reason for dismissing alert.**
   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 SIEM alerts for Scenario 1 of Capstone 2

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

1 Alert: Certificate error- There is a problem with a website's security certificate

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   The site not being certified and the integrity of the website could be lost also the risk of the website. and putting the company of data at risk and giving ransomware attacks.

2. **Describe any recommended immediate action to address the event.**
   Make sure you have the latest versions of security of the website making sure everything is up to date.

3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Making sure the window security is up to date and the browser is also aware of the vulnerability.

If No:

1. **Reason for dismissing alert.**

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

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   The common impact that this would have is data theft, sensitive data could be copied or transferred to the C&C. Also an attacker could shut down any number of compromised machines.

2. **Describe any recommended immediate action to address the event.**
   Shutdown the device and the network station that it is connected to.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Limit user permissions as much as possible, the principle of least privileges should be implemented in your organization. Assign each user with the least amount of permission required to do their work.

If No:

1. **Reason for dismissing alert.**

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

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   Then will attract the systems administrator which will get them access to sensitive data and the system and will compromise credentials for any privileged account. escalated due to confidentiality risk of information being leaked to the public
2. **Describe any recommended immediate action to address the event.**
   Fully manage the identity lifecycle including provisioning and de-provisioning of identities and accounts to ensure there are no accounts to hijack. revoke preflishes to the account and add another layer of security.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Password management solution to consistently apply strong credentia management practices, this also entails eliminating default and hardcoded credentials. Another thing that can be done is remove admin rights from users and reduce application and machine privileges to the minimum required. and another layer of security MFA authentication to have access to that.

If No:

1. **Reason for dismissing alert.**

4 Alert: 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

Should this issue be escalated? No

If 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 No:

1. **Reason for dismissing alert.**

   The user may have gained access by being promoted and was granted access for different credentials. The previous account status wasn't able to keep the user in a group with least authorization.

5 Alert: Device login- A user account logged into a desktop computer

Should this issue be escalated? no

If 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 No:

1. **Reason for dismissing alert.**

   User was able to access from the desktop by answering security questions for him to gain authorization.

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

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   Puts the computer at risk of contracting viruses that would go quietly in the background and without additional antivirus windows defender is the only thing left.
2. **Describe any recommended immediate action to address the event.**
   revoke access to the networking using that computer and remove the credentials that are being used.
   Change the windows defender's scheduling options, and disable real time protection and reschedule scans, and add antimalware service to the list then disable windows defender.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Check for if the antimalware is scanning its own folders regularly to make sure it doesn't stop again.

If No:

1. **Reason for dismissing alert.**

7 Alert: Logon/Logoff pattern- User login outside of normal pattern

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   Someone could be trying to access the network and apply the network DNS.
2. **Describe any recommended immediate action to address the event.**
   Revoke access to the network using that computer credentials that are being used because someone else credentials could be in use.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Limit the login times between regular work hours and if someone is trying to access the server after it limits the time frame.

If No:

1. **Reason for dismissing alert.**

8 Alert: File integrity- Evidence log files were deleted or tampered with

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**

   The security which consists of verifying the integrity of operating systems and application software files to determine if tamerping or fraud has occurred by comparing to trusted baseline.
2. **Describe any recommended immediate action to address the even**
   Find the user that tampered and deleted the files.
   Data recovery and forensics software can recover deleted files by looking for entries in the file table that have not been overwritten.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   By keeping software available to keep the files secure. you could add another layer of security so people who have access can have access.

If No:

1. **Reason for dismissing alert.**

9 Alert: 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.

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   Someone trying to intercept your login and access the system from a remote location
2. **Describe any recommended immediate action to address the event.**
   Shut down a person's credentials revoking access because they may have clicked on a link within an email.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   You would go over importance of not clicking suspicious links

If No:

1. **Reason for dismissing alert.**

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

Should this issue be escalated? Yes

If Yes:

1. **Briefly describe the potential impact of the issue including its potential impact to C.I.A.**
   A hacker could be trying to guess the user's password in order to gain access to information. The hacker could also gain access to a corporate network and they are using brute force passwords or steal hashes so that they can login to other systems in the network.
2. **Describe any recommended immediate action to address the event.**
   revoke the user's credentials from being used.
   Get information from the security event log to see why there were failed login attempts and perform an audit.
3. **Provide your recommendation for a security control to mitigate risk moving forward.**
   Conduct a routine check on the logs and implement a two factor authorization to minimize the risk of compromising

If No:

1. **Reason for dismissing alert.**