Free Questions for CS0-003 by vceexamstest

Shared by Gilbert on 12-07-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is the best reason why organizations need operational security controls?

Options:

A- To supplement areas that other controls cannot address

B- To limit physical access to areas that contain sensitive data

C- To assess compliance automatically against a secure baseline

D- To prevent disclosure by potential insider threats

Answer:

A

Explanation:

Operational security controls are security measures that are implemented and executed by people rather than by systems. Operational security controls are needed to supplement areas that other controls, such as technical or physical controls, cannot address. For example, operational security controls can include policies, procedures, training, awareness, audits, reviews, testing, etc. These controls

can help ensure that employees follow best practices, comply with regulations, detect and report incidents, and respond to emergencies. The other options are not specific to operational security controls or are too narrow in scope. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/operational-security-controls

Question 2

Question Type: MultipleChoice

A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited

resources to support testing. Which of the following exercises would be the best approach?

Options:

A- Tabletop scenarios

B- Capture the flag

C- Red team vs. blue team

D- Unknown-environment penetration test

Answer:

A

Explanation:

A tabletop scenario is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. A tabletop scenario is the best approach for a company that wants to test a new incident response plan without impacting the environment or using many resources. A tabletop scenario can help the company identify strengths and weaknesses in their plan, clarify roles and responsibilities, and improve communication and coordination among team members. The other options are more intensive and disruptive exercises that involve simulating a real incident or attack. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.linkedin.com/pulse/tabletop-exercises-explained-matt-lemon-phd

Question 3

Question Type: MultipleChoice

A technician working at company.com received the following email:

From: joe@gmail.com
To: technician@company.com
Subject: FW: Need help with my computer

Dear tech support,

Please contact me at +1-555-867-5309 as my computer was not fixed by the previous technician. My employee ID is 030234 and the computer serial # is A238482

---- Forward Message ----
From: joe@company.com
To: joe@gmail.com
Subject: FW: Need help with my computer

Dear joe, rebooting you computer should solve the issue.

After looking at the above communication, which of the following should the technician recommend to the security team to prevent exposure of sensitive information and reduce the risk of corporate data being stored on non-corporate assets?

Options:

A- Forwarding of corporate email should be disallowed by the company.

B- A VPN should be used to allow technicians to troubleshoot computer issues securely.

C- An email banner should be implemented to identify emails coming from external sources.

D- A rule should be placed on the DLP to flag employee IDs and serial numbers.

Answer:

C

Explanation:

An email banner is a message that is added to the top or bottom of an email to provide some information or warning to the recipient. An email banner should be implemented to identify emails coming from external sources to prevent exposure of sensitive information and reduce the risk of corporate data being stored on non-corporate assets. An email banner can help employees recognize phishing or spoofing attempts and avoid clicking on malicious links or attachments. It can also remind employees not to share confidential information with external parties or forward corporate emails to personal accounts. The other options are not relevant or effective for this purpose. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 13; https://www.csoonline.com/article/3235970/what-is-spoofing-definition-and-how-to-prevent-it.html

Question 4

Question Type: MultipleChoice

An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:

```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

Options:

A- Impair defenses.

B- Establish persistence.

C- Bypass file access controls.

D- Implement beaconing.

Answer:

B

Explanation:

The suspicious event was able to accomplish establishing persistence by creating a registry change that runs a command shell process every time a user logs on. The registry change modifies the Userinit value under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key, which specifies what programs should run

when a user logs on to Windows. By appending "cmd.exe," to the existing value, the event ensures that a command shell process will be launched every time a user logs on, which can allow the attacker to maintain access to the system or execute malicious commands. The other options are not related to the registry change. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/sysinfo/userinit-entry

Question 5

Question Type: MultipleChoice

A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?

Options:

A- A control that demonstrates that all systems authenticate using the approved authentication method

B- A control that demonstrates that access to a system is only allowed by using SSH

C- A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment

D- A control that demonstrates that the network security policy is reviewed and updated yearly

Answer:

C

Explanation:

A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/compensating-controls

Question 6

Question Type: **MultipleChoice**

An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:

```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

Options:

A- Impair defenses.

B- Establish persistence.

C- Bypass file access controls.

D- Implement beaconing.

Answer:

B

Explanation:

The suspicious event was able to accomplish establishing persistence by creating a registry change that runs a command shell process every time a user logs on. The registry change modifies the Userinit value under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key, which specifies what programs should run

when a user logs on to Windows. By appending "cmd.exe," to the existing value, the event ensures that a command shell process will be launched every time a user logs on, which can allow the attacker to maintain access to the system or execute malicious commands. The other options are not related to the registry change. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/sysinfo/userinit-entry

Question 7

Question Type: MultipleChoice

Which of the following is the best reason why organizations need operational security controls?

Options:

A- To supplement areas that other controls cannot address

B- To limit physical access to areas that contain sensitive data

C- To assess compliance automatically against a secure baseline

D- To prevent disclosure by potential insider threats

Answer:

A

Explanation:

Operational security controls are security measures that are implemented and executed by people rather than by systems. Operational security controls are needed to supplement areas that other controls, such as technical or physical controls, cannot address. For example, operational security controls can include policies, procedures, training, awareness, audits, reviews, testing, etc. These controls can help ensure that employees follow best practices, comply with regulations, detect and report incidents, and respond to emergencies. The other options are not specific to operational security controls or are too narrow in scope. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/operational-security-controls

Question 8

Question Type: MultipleChoice

A risk assessment concludes that the perimeter network has the highest potential for compromise by an attacker, and it is labeled as a critical risk environment. Which of the following is a valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques?

Options:

A- A control that demonstrates that all systems authenticate using the approved authentication method

B- A control that demonstrates that access to a system is only allowed by using SSH

C- A control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment

D- A control that demonstrates that the network security policy is reviewed and updated yearly

Answer:

C

Explanation:

A valid compensating control to reduce the volume of valuable information in the perimeter network that an attacker could gain using active reconnaissance techniques is a control that demonstrates that firewall rules are peer reviewed for accuracy and approved before deployment. This control can help ensure that the firewall rules are configured correctly and securely, and that they do not allow unnecessary or unauthorized access to the perimeter network. The other options are not compensating controls or do not address the risk of active reconnaissance. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/compensating-controls