Free Questions for CS0-002 by ebraindumps

Shared by Nielsen on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

An application has been updated to fix a vulnerability. Which of the following would ensure that previously patched vulnerabilities have not been reintroduced?

Options:

A- Stress testing

B- Regression testing

C- Code review

D- Peer review

Answer:

B

Explanation:

Regression testing is a type of software testing that ensures that a recent program or code change has not adversely affected existing features123Regression testing is useful for checking if previously patched vulnerabilities have not been reintroduced by the new update.

Stress testing is a type of software testing that evaluates the performance and reliability of a system under extreme conditions, such as high load, limited resources, or concurrent users. Stress testing is not directly related to checking for vulnerabilities.

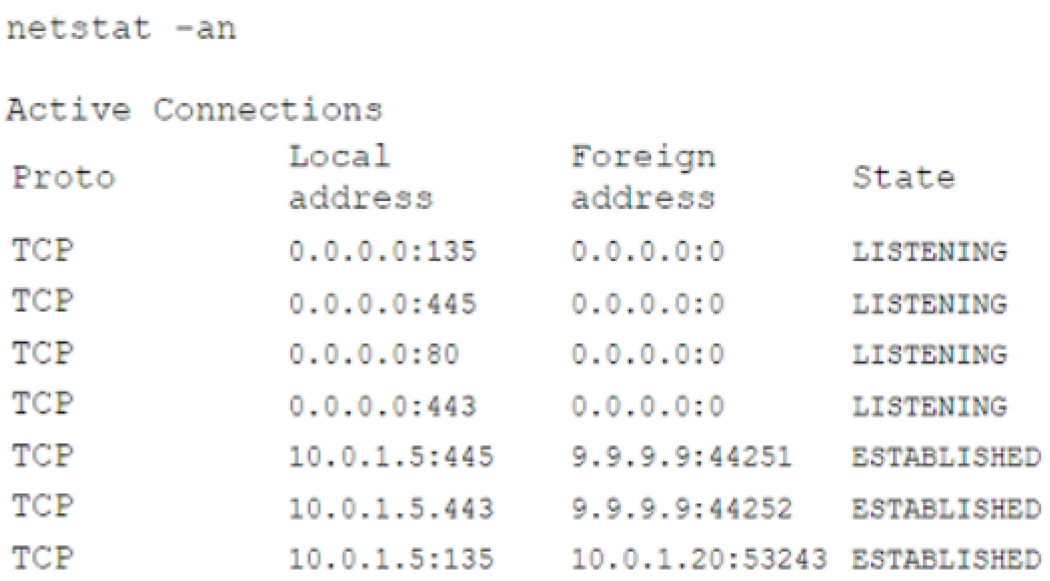
Code review is a process of examining the source code of a software program to find and fix errors, improve quality, and ensure compliance with standards and best practices. Code review can help prevent vulnerabilities from being introduced in the first place, but it does not verify that existing features are working as expected after a code change.

Peer review is a process of evaluating the work of another person or group of people, such as a research paper, a report, or a design. Peer review can provide feedback and suggestions for improvement, but it does not test the functionality or security of a software product.

Question 2

Question Type: **MultipleChoice**

During a routine security review, anomalous traffic from 9.9.9.9 was observed accessing a web server in the corporate perimeter network. The server is mission critical and must remain accessible around the world to serve web content. The Chief Information Security Officer has directed that improper traffic must be restricted. The following output is from the web server:



```
netstat -an

Active Connections
Proto        Local          Foreign         State
             address        address
TCP          0.0.0.0:135    0.0.0.0:0       LISTENING
TCP          0.0.0.0:445    0.0.0.0:0       LISTENING
TCP          0.0.0.0:80     0.0.0.0:0       LISTENING
TCP          0.0.0.0:443    0.0.0.0:0       LISTENING
TCP          10.0.1.5:445   9.9.9.9:44251   ESTABLISHED
TCP          10.0.1.5.443   9.9.9.9:44252   ESTABLISHED
TCP          10.0.1.5:135   10.0.1.20:53243 ESTABLISHED
```

Which of the following is the best method to accomplish this task?

Options:

A- Adjusting the IDS to block anomalous activity

B- Implementing port security

C- Adding 9.9.9.9 to the blocklist

D- Adjusting the firewall

Answer:

D

Explanation:

Based on the output of the "netstat -an" command, it seems that the web server is listening on port 80 for HTTP traffic and port 443 for HTTPS traffic. The anomalous traffic from 9.9.9.9 is accessing the web server on port 443, which means it is using a secure connection.

The best method to accomplish the task of restricting improper traffic from 9.9.9.9 isD. Adjusting the firewall. A firewall is a device or software that controls the flow of network traffic based on predefined rules. By adjusting the firewall rules, you can block or allow specific IP addresses, ports, protocols, or domains from accessing your web server.

Question 3

Question Type: MultipleChoice

Which of the following are the most likely reasons to include reporting processes when updating an incident response plan after a breach? (Select two).

Options:

A- To use the SLA to determine when to deliver the report

B- To meet regulatory requirements for timely reporting

C- To limit reputation damage caused by the breach

D- To remediate vulnerabilities that led to the breach

E- To isolate potential insider threats

F- To provide secure network design changes

B) To meet regulatory requirements for timely reporting: Many industries and jurisdictions have laws and regulations that mandate reporting of security breaches within a certain time frame. Failing to comply with these requirements can result in fines, penalties, lawsuits, and loss of trust. Therefore, it is important to have a clear and consistent reporting process that ensures timely and accurate disclosure of the breach to the relevant authorities.

C) To limit reputation damage caused by the breach: A security breach can have a negative impact on the reputation and credibility of the organization. Customers, partners, investors, and the public may lose confidence in the organization's ability to protect their data and interests. Therefore, it is important to have a transparent and honest reporting process that informs the affected parties about the nature, scope, and consequences of the breach, as well as the actions taken to mitigate and prevent future incidents. This can help restore trust and goodwill among the stakeholders.

Answer:

B, C

Explanation:

According to the CompTIA CySA+ Study Guide Exam CS0-002, 2nd Edition1, reporting is an essential part of the incident response process. It helps communicate the details and impact of the incident to various stakeholders, such as management, customers, regulators, law enforcement, and the public. Reporting also provides valuable feedback and lessons learned that can improve the security posture and readiness of the organization.

Based on this information, the most likely reasons to include reporting processes when updating an incident response plan after a breach are:

Question 4

Question Type: **MultipleChoice**

Which of the following is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs?

Options:

A- Unifying and migrating all services in a single CSP

B- Executing an API hardening process on the CSPs' endpoints

C- Integrating the security benchmarks of the CSPs with a CASB

D- Deploying cloud instances using Nikto and OpenVAS

Answer:

C

Explanation:

This is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs. CSP stands for cloud service provider, which is a company that offers cloud-based services such as infrastructure, platform, or software. CASB stands for cloud access security broker, which is a software or service that acts as a gateway between the company and the CSPs, and provides visibility, control, compliance, and threat protection for the cloud services.

Integrating the security benchmarks of the CSPs with a CASB means that the company can use a common set of standards and metrics to measure and compare the security posture and performance of different cloud service models, such as IaaS, PaaS, or SaaS. Security benchmarks are predefined criteria or best practices that define the minimum level of security required for a cloud service model. For example, some security benchmarks may include encryption, authentication, logging, auditing, patching, backup, etc. By integrating these benchmarks with a CASB, the company can monitor and enforce them across multiple CSPs, and identify any gaps or risks in their cloud security.

Question 5

Question Type: MultipleChoice

A current, validated DLP solution Is now in place because of a previous data breach However, a new data breach has taken place The following symptoms were observed shorty after a recent sales meeting:

* Sensitive corporate documents appeared on the dark web.

* Unusually large packets of data were being sent out.

Which of the following is most likely occurring?

Options:

A- Documents are not tagged properly to restrict sharing.

B- An insider threat is exfiltration data.

C- The DLP solution is not configured for unsecured web traffic

D- File audits are not enabled on CASB.

Answer:

B

Explanation:

This is most likely occurring based on the symptoms observed after a recent sales meeting. An insider threat is a person who has legitimate access to an organization's network or data and uses it for malicious purposes, such as stealing, leaking, or sabotaging information. The symptoms suggest that someone from the sales team or someone who attended the meeting has copied sensitive corporate documents and uploaded them to the dark web using large data packets.

Question 6

Question Type: MultipleChoice

A company has Detected a large number of tailed login attempts on its network A security analyst is investigating the network's activity logs to establish a pattern of behavior. Which of the following techniques should the analyst use to analyze the increase in failed login attempts?

Options:

A- Evidence visualization

B- Pattern matching

C- Event correlation

D- Network sniffing

Answer:

C

Explanation:

This is the technique that the analyst should use to analyze the increase in failed login attempts on the network. Event correlation is a process that analyzes multiple events or logs from different sources and identifies patterns, relationships, or causal links between them. Event correlation can help reveal the root cause, scope, impact, and sequence of a security incident.

Question 7

Question Type: **MultipleChoice**

A manufacturing company has joined the information sharing and analysis center for its sector. As a benefit, the company will receive structured IoC data contributed by other members. Which of the following best describes the utility of this data?

Options:

A- Other members will have visibility into Instances o' positive IoC identification within me manufacturing company's corporate network.

B- The manufacturing company will have access to relevant malware samples from all other manufacturing sector members.

C- Other members will automatically adjust their security postures lo defend the manufacturing company's processes.

D- The manufacturing company can automatically generate security configurations for all of Its Infrastructure.

Answer:

B

Explanation:

This best describes the utility of the structured loC data contributed by other members of the information sharing and analysis center (ISAC) for its sector. loC stands for indicator of compromise, which is a piece of information that suggests a potential intrusion or attack, such as an IP address, a file hash, a domain name, or a malware signature. By sharing loC data, the ISAC members can benefit from each other's threat intelligence and improve their security defenses.

Question 8

Question Type: **MultipleChoice**

Which of the following is an advantage of continuous monitoring as a way to help protect an enterprise?

Options:

A- Continuous monitoring leverages open-source tools, thereby reducing cost to the organization.

B- Continuous monitoring responds to active Intrusions without requiring human assistance.

C- Continuous monitoring blocks malicious activity by connecting to real-lime threat feeds.

D- Continuous monitoring uses automation to identify threats and alerts in real time

Answer:

D

Explanation:

Continuous monitoring uses automation to identify threats and alerts in real time. This is an advantage of continuous monitoring as a way to help protect an enterprise because it enables faster detection and response to security incidents, reduces the risk of human error, and improves the overall security posture and compliance of the organization.