# CAS-005$^{Q\&As}$

CompTIA SecurityX Exam

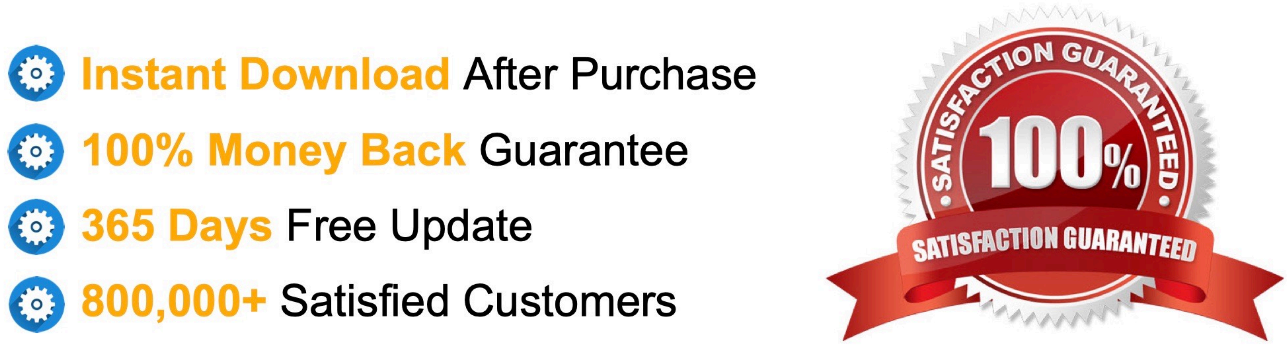
## Pass CompTIA CAS-005 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

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


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

**QUESTION 1**

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

1.

Exfiltration of intellectual property

2.

Unencrypted files

3.

Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

A. Implementing data loss prevention

B. Deploying file integrity monitoring

C. Restricting access to critical file services only

D. Deploying directory-based group policies

E. Enabling modem authentication that supports MFA

F. Implementing a version control system

G. Implementing a CMDB platform

Correct Answer: AE

To mitigate the identified vulnerabilities, the following solutions are most appropriate:

A. Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive

data transfers.

E. Enabling modern authentication that supports Multi-Factor Authentication (MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by

making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

B. Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords. C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate

all identified vulnerabilities. D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication. F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities. G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues

mentioned.

References:

CompTIA Security+ Study Guide

NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

**QUESTION 2**

An organization is implementing Zero Trust architecture A systems administrator must increase the effectiveness of the organization\\'s context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

A. Secure zone architecture

B. Always-on VPN

C. Accurate asset inventory

D. Microsegmentation

Correct Answer: D

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of

attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring

within Zero Trust environments.

Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

**QUESTION 3**

An organization is required to

1.

Respond to internal and external inquiries in a timely manner

2.

Provide transparency.

3.

Comply with regulatory requirements

The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future.

Which of the following is the best way for the organization to prepare?

A. Outsourcing the handling of necessary regulatory filing to an external consultant

B. Integrating automated response mechanisms into the data subject access request process

C. Developing communication templates that have been vetted by internal and external counsel

D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Correct Answer: C

Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and

provide transparency in the event of a breach.

Why Communication Templates?

Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.

Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements. Consistent Messaging: Ensures that all responses are consistent, clear, and accurate, maintaining the

organization\\'s credibility. Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately. Other options, while useful, do not provide the

same level of preparedness and compliance:

A. Outsourcing to an external consultant: This may delay response times and lose internal control over the communication.

B. Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.

D. Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.

References:

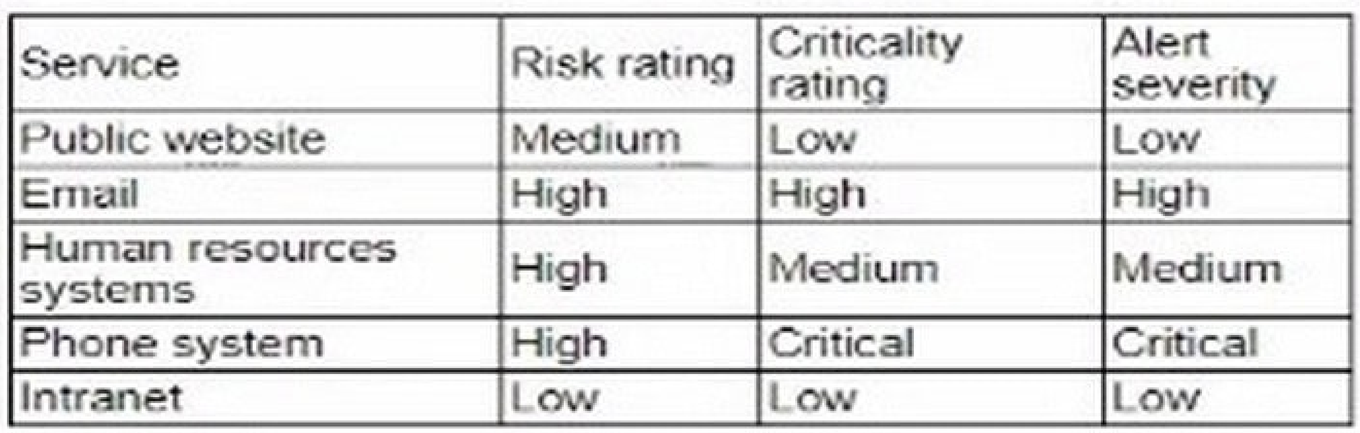
CompTIA SecurityX Study Guide

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

ISO/IEC 27002:2013, "Information technology -- Security techniques -- Code of practice for information security controls"

**QUESTION 4**

After an incident response exercise, a security administrator reviews the following table:



| Service | Risk rating | Criticality rating | Alert severity |
|---|---|---|---|
| Public website | Medium | Low | Low |
| Email | High | High | High |
| Human resources systems | High | Medium | Medium |
| Phone system | High | Critical | Critical |
| Intranet | Low | Low | Low |

Which of the following should the administrator do to beat support rapid incident response in the future?

A. Automate alerting to IT support for phone system outages.

B. Enable dashboards for service status monitoring

C. Send emails for failed log-In attempts on the public website

D. Configure automated Isolation of human resources systems

Correct Answer: B

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response,

real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues. Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline

incident response efforts.

Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise. Improved Decision Making: Real-time data helps incident response teams make

informed decisions quickly, reducing downtime and mitigating impact. Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

A. Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services. D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

"Best Practices for Implementing Dashboards," Gartner Research

**QUESTION 5**

While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter.

Which of the following best describes this type of correlation?

A. Spear-phishing campaign

B. Threat modeling

C. Red team assessment

D. Attack pattern analysis

Correct Answer: A

The situation where several employees were contacted by the same individual impersonating a recruiter best describes a spear-phishing campaign. Here\\'s why:

Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.

Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack. Correlated Contacts: The fact that several

employees were contacted by the same individual suggests a coordinated effort to breach the organization\\'s security by targeting multiple points of entry through social engineering.