



- Expert Verified, Online, **Free**.



Custom View Settings

Topic 1 - Exam A

Question #1

Topic 1

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

- A. Hacktivist
- B. Whistleblower
- C. Organized crime Most Voted
- D. Unskilled attacker

Correct Answer: C

Community vote distribution

C (100%)

Question #2

Topic 1

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

- A. Key stretching
- B. Data masking
- C. Steganography
- D. Salting Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Topic 1

Question #3

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message. Which of the following types of social engineering attacks occurred?

- A. Brand impersonation
- B. Pretexting
- C. Typosquatting
- D. Phishing Most Voted

Correct Answer: D*Community vote distribution*

D (91%) 9%

Question #4

Topic 1

An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

- A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
- B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
- C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
- D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 Most Voted

Correct Answer: D*Community vote distribution*

D (89%) 11%

Question #5

Topic 1

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

- A. SSO Most Voted
- B. LEAP
- C. MFA
- D. PEAP

Correct Answer: A*Community vote distribution*

A (100%)

Question #6

Which of the following scenarios describes a possible business email compromise attack?

- A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- B. Employees who open an email attachment receive messages demanding payment in order to access files.
- C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account. Most Voted
- D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Correct Answer: C

Community vote distribution

C (62%) A (27%) 11%

Question #7

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers.

Which of the following should a database administrator use to access the database servers?

- A. Jump server Most Voted
- B. RADIUS
- C. HSM
- D. Load balancer

Correct Answer: A

Community vote distribution

A (100%)

Question #8

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

- A. NGFW
- B. WAF Most Voted
- C. TLS
- D. SD-WAN

Correct Answer: B

Community vote distribution

B (94%) 6%

Question #9

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

- A. Multifactor authentication Most Voted
- B. Permissions assignment
- C. Access management
- D. Password complexity

Correct Answer: A

Community vote distribution

A (100%)

Question #10

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation Most Voted
- D. Vishing
- E. Smishing Most Voted
- F. Misinformation

Correct Answer: CE

Community vote distribution

CE (89%)

11%

[Next Questions ➔](#)

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.



Custom View Settings

Question #11

Topic 1

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training. Most Voted
- C. Issue a general email warning to the company. Most Voted
- D. Have the CEO change phone numbers.
- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

Correct Answer: BC

Community vote distribution

BC (100%)

Question #12

Topic 1

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. A thorough analysis of the supply chain Most Voted
- B. A legally enforceable corporate acquisition policy
- C. A right to audit clause in vendor contracts and SOWs
- D. An in-depth penetration test of all suppliers and vendors

Correct Answer: A

Community vote distribution

A (71%)

C (29%)

Question #13

Which of the following provides the details about the terms of a test with a third-party penetration tester?

- A. Rules of engagement Most Voted
- B. Supply chain analysis
- C. Right to audit clause
- D. Due diligence

Correct Answer: A

Community vote distribution

A (94%) 6%

Question #14

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

- A. Active Most Voted
- B. Passive
- C. Defensive
- D. Offensive

Correct Answer: A

Community vote distribution

A (100%)

Question #15

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. IRP
- B. DRP Most Voted
- C. RPO
- D. SDLC

Correct Answer: B

Community vote distribution

B (100%)

Question #16

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking
- B. Memory injection
- C. Resource reuse
- D. Side loading Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #17

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

- A. Password spraying Most Voted
- B. Account forgery
- C. Pass-the-hash
- D. Brute-force

Correct Answer: A

Community vote distribution

A (100%)

Question #18

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones Most Voted
- B. Subject role Most Voted
- C. Adaptive identity
- D. Threat scope reduction

Correct Answer: B

Community vote distribution

B (44%) A (33%) D (15%) 8%

Question #19

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

- A. RDP server
- B. Jump server Most Voted
- C. Proxy server
- D. Hypervisor

Correct Answer: B*Community vote distribution*

B (100%)

Question #20

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off
- B. http:// Most Voted
- C. www.*.com
- D. :443

Correct Answer: B*Community vote distribution*

B (100%)

[← Previous Questions](#)[Next Questions →](#)

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.



Custom View Settings

Question #21

Topic 1

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

- A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0 Most Voted
- C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: B

Community vote distribution

B (100%)

Question #22

Topic 1

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Implementing a bastion host Most Voted
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Correct Answer: A

Community vote distribution

A (91%)

9%

Question #23

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

- A. Application
- B. IPS/IDS
- C. Network
- D. Endpoint Most Voted

Correct Answer: D*Community vote distribution*

D (91%) 9%

Question #24

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

- A. Digital forensics
- B. E-discovery
- C. Incident response
- D. Threat hunting Most Voted

Correct Answer: D*Community vote distribution*

D (100%)

Question #25

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A. Accept
- B. Transfer Most Voted
- C. Mitigate
- D. Avoid

Correct Answer: B*Community vote distribution*

B (100%)

Question #26

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- A. Partition
- B. Asymmetric
- C. Full disk Most Voted
- D. Database

Correct Answer: C

Community vote distribution

C (100%)

Question #27

Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive Most Voted

Correct Answer: D

Community vote distribution

D (90%) 10%

Question #28

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

- A. Hardening
- B. Employee monitoring
- C. Configuration enforcement
- D. Least privilege Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #29

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A. Risk tolerance
- B. Risk transfer
- C. Risk register Most Voted
- D. Risk analysis

Correct Answer: C

Community vote distribution

C (100%)

Question #30

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure Most Voted

Correct Answer: D

Community vote distribution

D (100%)

[◀ Previous Questions](#)

[Next Questions ➔](#)

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.



Custom View Settings

Question #31

Topic 1

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

- A. Open-source intelligence
- B. Bug bounty Most Voted
- C. Red team
- D. Penetration testing

Correct Answer: B

Community vote distribution

B (100%)

Question #32

Topic 1

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

- A. Insider
- B. Unskilled attacker
- C. Nation-state Most Voted
- D. Hacktivist

Correct Answer: C

Community vote distribution

C (100%)

Question #33

Which of the following enables the use of an input field to run commands that can view or manipulate data?

- A. Cross-site scripting
- B. Side loading
- C. Buffer overflow
- D. SQL injection Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #34

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

- A. Encrypted
- B. Intellectual property Most Voted
- C. Critical
- D. Data in transit

Correct Answer: B

Community vote distribution

B (100%)

Question #35

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

- A. If a security incident occurs on the device, the correct employee can be notified. Most Voted
- B. The security team will be able to send user awareness training to the appropriate device.
- C. Users can be mapped to their devices when configuring software MFA tokens.
- D. User-based firewall policies can be correctly targeted to the appropriate laptops.
- E. When conducting penetration testing, the security team will be able to target the desired laptops.
- F. Company data can be accounted for when the employee leaves the organization. Most Voted

Correct Answer: AF

Community vote distribution

AF (70%)

AC (20%)

10%

Question #36

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training. Most Voted
- D. Implement a phishing campaign.

Correct Answer: C*Community vote distribution*

C (100%)

Question #37

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard Most Voted

Correct Answer: D*Community vote distribution*

D (100%)

Question #38

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

- A. The end user changed the file permissions.
- B. A cryptographic collision was detected.
- C. A snapshot of the file system was taken.
- D. A rootkit was deployed. Most Voted

Correct Answer: D*Community vote distribution*

D (100%)

Question #39

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

- A. Client Most Voted
- B. Third-party vendor
- C. Cloud provider
- D. DBA

Correct Answer: A

Community vote distribution

A (93%)	7%
---------	----

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

- A. MSA
- B. SLA
- C. BPA
- D. SOW Most Voted

Correct Answer: D

Community vote distribution

D (94%)	6%
---------	----

◀ Previous Questions

Next Questions ➔

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.



Custom View Settings

Question #41

Topic 1

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A. Secure cookies
- B. Version control
- C. Input validation** Most Voted
- D. Code signing

Correct Answer: C

Community vote distribution

C (100%)

Question #42

Topic 1

Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Ease of recovery** Most Voted
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness** Most Voted
- E. Attack surface
- F. Extensible authentication

Correct Answer: AD

Community vote distribution

AD (75%) AC (15%) 10%

Question #43

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request. Most Voted
- D. Apply the patch to the system.

Correct Answer: C

Community vote distribution

C (100%)

Question #44

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A. To gather IoCs for the investigation
- B. To discover which systems have been affected
- C. To eradicate any trace of malware on the network
- D. To prevent future incidents of the same nature Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #45

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

- A. Fines
- B. Audit findings Most Voted
- C. Sanctions
- D. Reputation damage

Correct Answer: B

Community vote distribution

B (83%)

Other

Question #46

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

- A. Capacity planning Most Voted
- B. Redundancy
- C. Geographic dispersion
- D. Tabletop exercise

Correct Answer: A

Community vote distribution

A (100%)

Question #47

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

- A. Data masking
- B. Encryption
- C. Geolocation policy Most Voted
- D. Data sovereignty regulation

Correct Answer: C

Community vote distribution

C (100%)

Question #48

Which of the following is a hardware-specific vulnerability?

- A. Firmware version Most Voted
- B. Buffer overflow
- C. SQL injection
- D. Cross-site scripting

Correct Answer: A

Community vote distribution

A (100%)

Question #49

While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

- A. Documenting the new policy in a change request and submitting the request to change management
- B. Testing the policy in a non-production environment before enabling the policy in the production network Most Voted
- C. Disabling any intrusion prevention signatures on the “deny any” policy prior to enabling the new policy
- D. Including an “allow any” policy above the “deny any” policy

Correct Answer: B*Community vote distribution*

B (60%)

A (40%)

Question #50

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

- A. Real-time recovery
- B. Hot
- C. Cold
- D. Warm Most Voted

Correct Answer: D*Community vote distribution*

D (84%)

C (16%)

[← Previous Questions](#)[Next Questions →](#)

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.



Custom View Settings

Question #51

Topic 1

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

- A. Enumeration
- B. Sanitization Most Voted
- C. Destruction
- D. Inventory

Correct Answer: B

Community vote distribution

B (100%)

Question #52

Topic 1

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive Most Voted
- D. Public

Correct Answer: C

Community vote distribution

C (100%)

Question #53

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

- A. Local data protection regulations Most Voted
- B. Risks from hackers residing in other countries
- C. Impacts to existing contractual obligations
- D. Time zone differences in log correlation

Correct Answer: A

Community vote distribution

A (73%) C (27%)

Question #54

Which of the following would be the best way to block unknown programs from executing?

- A. Access control list
- B. Application allow list Most Voted
- C. Host-based firewall
- D. DLP solution

Correct Answer: B

Community vote distribution

B (100%)

Question #55

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

- A. White
- B. Purple
- C. Blue
- D. Red Most Voted

Correct Answer: D

Community vote distribution

D (85%) B (15%)

Question #56

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

- A. Testing input validation on the user input fields
- B. Performing code signing on company-developed software Most Voted
- C. Performing static code analysis on the software
- D. Ensuring secure cookies are used

Correct Answer: B*Community vote distribution*

B (100%)

Question #57

Which of the following can be used to identify potential attacker activities without affecting production servers?

- A. Honeypot Most Voted
- B. Video surveillance
- C. Zero Trust
- D. Geofencing

Correct Answer: A*Community vote distribution*

A (100%)

Question #58

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

- A. Analysis Most Voted
- B. Lessons learned
- C. Detection
- D. Containment

Correct Answer: A*Community vote distribution*

A (100%)

Question #59

Topic 1

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

- A. Conduct an audit.
 - B. Initiate a penetration test.
 - C. Rescan the network. Most Voted
 - D. Submit a report.

Correct Answer: C

Community vote distribution

C (100%)

Question #60

Topic 1

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

- A. Penetration testing
 - B. Phishing campaign
 - C. External audit
 - D. Insider threat [Most]

Correct Answer: *D*

Community vote distribution

D (100%)

[← Previous Questions](#)

Next Questions →

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, **Free**.



Custom View Settings

Question #61

Topic 1

Which of the following allows for the attribution of messages to individuals?

- A. Adaptive identity
- B. Non-repudiation Most Voted
- C. Authentication
- D. Access logs

Correct Answer: B

Community vote distribution

B (100%)

Question #62

Topic 1

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Automation Most Voted
- B. Compliance checklist
- C. Attestation
- D. Manual audit

Correct Answer: A

Community vote distribution

A (100%)

Question #63

Topic 1

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. SCAP
- B. NetFlow
- C. Antivirus
- D. DLP Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #64

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ., &, ` , and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation Most Voted
- D. Static code analysis

Correct Answer: C

Community vote distribution

C (100%)

Question #65

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- A. Place posters around the office to raise awareness of common phishing activities.
- B. Implement email security filters to prevent phishing emails from being delivered.
- C. Update the EDR policies to block automatic execution of downloaded programs. Most Voted
- D. Create additional training for users to recognize the signs of phishing attempts.

Correct Answer: C

Community vote distribution

C (80%)

13% 7%

Question #66

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Compensating control Most Voted
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Correct Answer: A

Community vote distribution

A (90%)

10%

Question #67

The management team notices that new accounts that are set up manually do not always have correct access or permissions. Which of the following automation techniques should a systems administrator use to streamline account creation?

- A. Guard rail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script Most Voted

Correct Answer: D

Community vote distribution

D (100%)

Question #68

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

- A. Corrective
- B. Preventive
- C. Detective Most Voted
- D. Deterrent

Correct Answer: C

Community vote distribution

C (100%)

Question #69

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

- A. Serverless framework Most Voted
- B. Type 1 hypervisor
- C. SD-WAN
- D. SDN

Correct Answer: A

Community vote distribution

A (100%)

Question #70

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

A. Tuning Most Voted

B. Aggregating

▲
11 votes.

C. Quarantining

D. Archiving

Correct Answer: A

Community vote distribution

A (100%)

[◀ Previous Questions](#)

[Next Questions ➔](#)

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 71 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 71

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst reviews domain activity logs and notices the following:

User ID jsmith, password authentication: succeeded, MFA: failed (invalid code)
User ID jsmith, password authentication: succeeded, MFA: failed (invalid code)
User ID jsmith, password authentication: succeeded, MFA: failed (invalid code)
User ID jsmith, password authentication: succeeded, MFA: failed (invalid code)

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on jsmith's workstation.
- C. An attacker is attempting to brute force jsmith's account. Most Voted
- D. Ransomware has been deployed in the domain.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (65%)

B (35%)

by Xavierallen9711 at May 11, 2024, 5:16 p.m.

Comments

✉ **nyyankee718** Highly Voted 2 months, 3 weeks ago

Selected Answer: B

Can be B or C, but leaning B
Since they already have the password, its not a brute force attack
upvoted 5 times

✉ **a4e15bd** 2 months, 2 weeks ago

I thought the same, but trying multiple MFA codes is also considered brute force.
upvoted 5 times

 **barracouto** Most Recent 3 days, 10 hours ago

Selected Answer: C

The log entries show multiple successful password authentications followed by multiple failed MFA (Multi-Factor Authentication) attempts due to invalid codes. This pattern suggests that the user's password has been correctly entered multiple times, but the MFA codes are consistently failing.

The best explanation for what the security analyst has discovered is:

C. An attacker is attempting to brute force jsmith's account.

The repeated successful password authentications followed by failed MFA attempts indicate that an attacker may have obtained the user's password and is now trying to bypass the second layer of security, the MFA, by attempting multiple invalid codes.

upvoted 3 times

 **dbrowndiver** 2 months ago

Selected Answer: C

The scenario perfectly matches a common security issue where attackers gain partial access through stolen credentials but are thwarted by MFA, which they try to bypass unsuccessfully. The repeated success in password authentication suggests that the attacker has access to jsmith's password, but the failure of MFA points to an attempt to guess or brute-force the MFA code.

upvoted 3 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: C

The log entries indicate that the user "jsmith" has successfully authenticated with a password but has repeatedly failed the Multi-Factor Authentication (MFA) step due to an invalid code. This pattern suggests that the correct password is known or has been compromised, but the attacker is unable to provide the correct MFA code.

Given this information, the most likely explanation is:

C. An attacker is attempting to brute force jsmith's account.

The repeated MFA failures suggest that someone other than the legitimate user is trying to gain access, potentially indicating a brute force attempt or another form of unauthorized access where the password is known, but the second factor of authentication is not.

upvoted 1 times

 **leedsbarber** 3 months, 4 weeks ago

Selected Answer: C

Brute force involves trying different combinations of passwords/other credentials. This attacker knows the username and password and is clearly not guessing. A keylogger would know the username and password, but not have access to the MFA.

upvoted 2 times

 **c80f5c5** 4 months ago

Selected Answer: C

If the question mentioned a login from a specific workstation, or said its local login only, then yes it would be keylogger. However, this could be a login from home computer, mobile device, anything. Answer B could be correct but more info would be needed. Based on available info C is best.

upvoted 2 times

 **e56400d** 4 months ago

If someone enter their credentials correctly but not their MFA you can indicate that the person can be a keylogger. I think "B" is a better answer because its more specific.

upvoted 2 times

 **123456789User** 4 months ago

Selected Answer: C

Brute force. They have the password but are guessing the MFA code repeatedly.

upvoted 2 times

 **Oluwasheeun** 4 months, 2 weeks ago

Selected Answer: B

Clearly shows MFA Failed. So the most likely answer is the person knows the keys, but not the MFA. Which can be achieved by keylogger.

upvoted 3 times

 **MAKOhunter33333333** 4 months, 2 weeks ago

Selected Answer: C

This is a log of failed attempts to login (brute force), but are blocked by mfa. There is no indication of a keylogger based on this log.

upvoted 1 times

 **SHADTECH123** 4 months, 3 weeks ago

Selected Answer: C

The logs show that the password authentication for the user jsmith has succeeded multiple times, but the Multi-Factor Authentication (MFA) has failed repeatedly with an "invalid code" error. This pattern is consistent with an attacker who has obtained or guessed the user's password but is unable to bypass the MFA step, indicating a brute force attempt.

upvoted 1 times

 **e5c1bb5** 4 months, 3 weeks ago

not C. password was correct MFA was wrong. they have the password
upvoted 1 times

 **7662357** 4 months, 3 weeks ago

It looks like the the password has been successfully entered, but a multi-factor authenticator is not being used correctly. If there's a keylogger installed on their computer without their knowledge they may be continuously attempting to log in to their profile to no avail. Therefore, I'd would lean more towards "B" being the correct answer.

upvoted 3 times

 **Xavierallen9711** 4 months, 3 weeks ago

I'm not sure about C being correct
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 72 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 72

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A. Clustering servers
- B. Geographic dispersion Most Voted
- C. Load balancers
- D. Off-site backups

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by 123456789User at June 1, 2024, 7:43 p.m.

Comments

✉ **barracouto** 2 days, 6 hours ago

Selected Answer: B

Given the concern about weather events causing damage to the server room and resulting downtime, the company should consider measures that protect against physical damage and ensure business continuity. The most relevant option for this scenario is:

- B. Geographic dispersion

Geographic dispersion involves placing critical infrastructure in multiple, geographically distant locations. This strategy ensures that even if one site is affected by a weather event, operations can continue at another site, minimizing downtime and maintaining availability.

upvoted 2 times

✉ **RIDA_007** 2 weeks ago

Correct it's B.

geographical dispersal refers to placing physical distances between duplicate systems so the organization can avoid damages to both the primary and alternate resources from the same disaster.

upvoted 2 times

 **dbrowndiver** 2 months ago

Selected Answer: B

In this scenario, option B. Geographic dispersion is the correct answer because it provides a comprehensive solution to the risk of weather-related damage to the server room. By spreading resources across multiple locations, the company can maintain service continuity and minimize downtime, even when one location is affected by severe weather conditions.

upvoted 2 times

 **123456789User** 4 months ago

Selected Answer: B

distributing your infrastructure across multiple physical locations makes it so if you lose one site to weather or a disaster of sorts, you can continue operating via another location

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 73 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 73

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a primary security concern for a company setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape
- D. Jailbreaking Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [jennyka76](#) at June 27, 2024, 6:27 p.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: D

In this scenario, D. Jailbreaking is the correct answer because it directly affects the security of personal devices used in a BYOD program. Jailbreaking removes built-in security controls, making devices vulnerable to various threats, and is a primary concern for companies allowing personal devices to access corporate networks and data.

upvoted 1 times

✉ **barracouto** 4 months, 2 weeks ago

Selected Answer: D

When setting up a Bring Your Own Device (BYOD) program, the primary security concern is ensuring that personal devices, which may not be under the company's direct control, do not introduce security risks into the organization. Among the options provided, the most relevant concern is:

D. Jailbreaking

Jailbreaking refers to removing the manufacturer's restrictions on a device, which can compromise the security of the device. This makes it more susceptible to malware and unauthorized access, posing a significant risk to the company's network and data when such a device is connected.

upvoted 4 times

 **jennyka76** 4 months, 3 weeks ago

D

Jailbreaking is the process of removing software restrictions that a device manufacturer has intentionally put in place. This allows users to gain more control over their device, such as:

Installing custom firmware

Installing third-party applications

Choosing their operating system

Getting apps from unofficial stores

Turning their phone into a hotspot

Changing the look and operation of their phone

Changing phone settings at the administrator level

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 74 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 74

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.

Which of the following analysis elements did the company most likely use in making this decision?

- A. MTTR
- B. RTO
- C. ARO (Most Voted)
- D. MTBF

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [e5c1bb5](#) at May 9, 2024, 6:30 p.m.

Comments

[e5c1bb5](#) Highly Voted 4 months, 4 weeks ago

Selected Answer: C

MTTR= mean time to repair

RTO=recovery time objective

ARO= annualized rate of occurrence

MTBF= mean time between failures.

ARO is it

upvoted 19 times

[barracouto](#) Highly Voted 2 days, 6 hours ago

Selected Answer: C

MTTR (Mean Time to Repair): This measures the average time it takes to repair a system or component after a failure. It is used to assess how quickly an organization can respond to and fix issues.

RTO (Recovery Time Objective): This is the maximum acceptable amount of time that a system or application can be down after a failure or disaster. It defines the target time for recovery.

ARO (Annualized Rate of Occurrence): This estimates the frequency with which a specific risk or event is expected to occur in a year. It helps in assessing the likelihood of risks.

MTBF (Mean Time Between Failures): This measures the average time between failures of a system or component. It is used to predict the reliability and performance of systems over time.

In the context of the company deciding to remove ransomware coverage to reduce costs, they likely assessed the ARO (Annualized Rate of Occurrence) to determine how often ransomware attacks are expected to occur and decided the risk was low enough to justify the cost savings.

upvoted 7 times

 **dbrowndiver** Most Recent 2 months ago

Selected Answer: C

In this scenario, option C. ARO (Annualized Rate of Occurrence) is the correct answer because it assesses the frequency of ransomware attacks. The company likely used ARO to evaluate the likelihood of such incidents occurring and decided that the probability did not justify the cost of insurance coverage for ransomware, leading to the decision to reduce the policy cost.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 75 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 75

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities Most Voted
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [c80f5c5](#) at June 5, 2024, 3:56 a.m.

Comments

  [c80f5c5](#) Highly Voted 4 months ago

Selected Answer: A

Easiest way to think of this question is this security awareness program is likely to be made company wide for the avg employee with no computer skills. B C D are all for the cybersecurity team specifically

upvoted 9 times

  [d4a5620](#) Most Recent 1 month ago

Selected Answer: A

The keyword here is "communication" and reporting is the only answer option given that effectively communicates phishing attempts
upvoted 2 times

  [chasingsummer](#) 1 month, 3 weeks ago

Selected Answer: A

The most likely answer is A.
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

◀ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 76 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 76

Topic #: 1

[\[All SY0-701 Questions\]](#)

HOTSPOT -

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -

Not all attacks and remediation actions will be used.

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

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Logic Bomb	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Backdoor	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Virus	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

[Hide Answer](#)

Suggested Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Virus	Patch vulnerable systems
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

by  Th3irdEye at May 16, 2024, 7:17 p.m.

Comments

 **Th3irdEye**  4 months, 3 weeks ago

I think the 3rd line is wrong.
It should be:
Database server / Worm / Change the default application password

The prompt talks about compromising an SQL database with well known credentials. So you need to change the app default password to fix this. It also talks about the attack being self propagating which would make it a worm.

I believe the rest of the answers are correct.
upvoted 26 times

 **c80f5c5**  4 months ago

These are the answers I got when I took a Sec+ bootcamp for work, they went over this lab during the course.

1. Botnet - Enable DDoS
2. RAT - Implement Host based IPS
3. Worm - Change default application password
4. Keylogger - Disable remote access services
5. Backdoor - Conduct code review

I've seen various answers around the web. I'm going with these.
upvoted 16 times

 **PAWarriors**  1 month ago

Correct order:

- A. Botnet - Enable DDoS
- B. RAT - Implement Host based IPS
- C. Worm - Change default application password
- D. Keylogger - Disable remote access services
- E. Backdoor - Conduct code review

upvoted 1 times

 **a4e15bd** 1 month, 2 weeks ago

- 1- Botnet - Enable DDoS
2. RAT - Disable remote services
3. Worm - Change default application password
4. Keylogger - Enable MFA
5. Backdoor - Conduct a code review.

upvoted 2 times

 **chasingsummer** 1 month, 3 weeks ago

These make sense to me:

1. Botnet > Enable DDoS protection
2. RAT > Implement a host-based IPS
3. Worm > Change the default application password
4. Keylogger > Implement 2FA using push notification
5. Backdoor > Conduct a code review

upvoted 1 times

 **Zayrdis** 2 months, 3 weeks ago

Upon vast research these make the best sense.
1. Botnet - Enable DDoS
2. RAT - Disable remote access services
3. Worm - Change default application password
4. Keylogger - Implement a host-based IPS
5. Backdoor - Conduct code review

upvoted 7 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

- 1 An attacker sends multiple SYN packets from multiple sources.
- Botnet
- Enable DDoS protection
- 2 The attack establishes a connection, which allows remote commands to be executed.
- Attack Identified. RAT Remote Access Trojan
- BEST Preventive or Remediation Action. Disable remote access services
- 3 The attack is self-propagating and compromises a SQL database using well-known credentials as it moves through the network.
- Attack Identified. Worm
- BEST Preventive or Remediation Action. Patch vulnerable systems
- 4 The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.

- Attack Identified. Keylogger
- BEST Preventive or Remediation Action. Conduct a code review

5 The attacker embeds hidden access in an internally developed application that bypasses account login.

- Attack Identified. Backdoor
- BEST Preventive or Remediation Action. Implement a host-based IPS

upvoted 5 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

EXAM SY0-701 TOPIC 1 QUESTION 77 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 77

Topic #: 1

[\[All SY0-701 Questions\]](#)

HOTSPOT -

You are a security administrator investigating a potential infection on a network.

INSTRUCTIONS -

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

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

192.168.10.22 X

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31 Warn Scheduled scan disabled by process svchost.exe
4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe
```

192.168.10.37 X

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

192.168.10.41

```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svchost.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svchost.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```

Firewall

Timestamp		Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019	16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019	16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019	16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019	16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019	16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019	16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019	16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019	23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019	23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019	23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019	2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019	2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019	2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019	2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019	2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019	2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019	2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019	13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019	13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019	13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019	13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019	13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019	13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019	14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019	14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

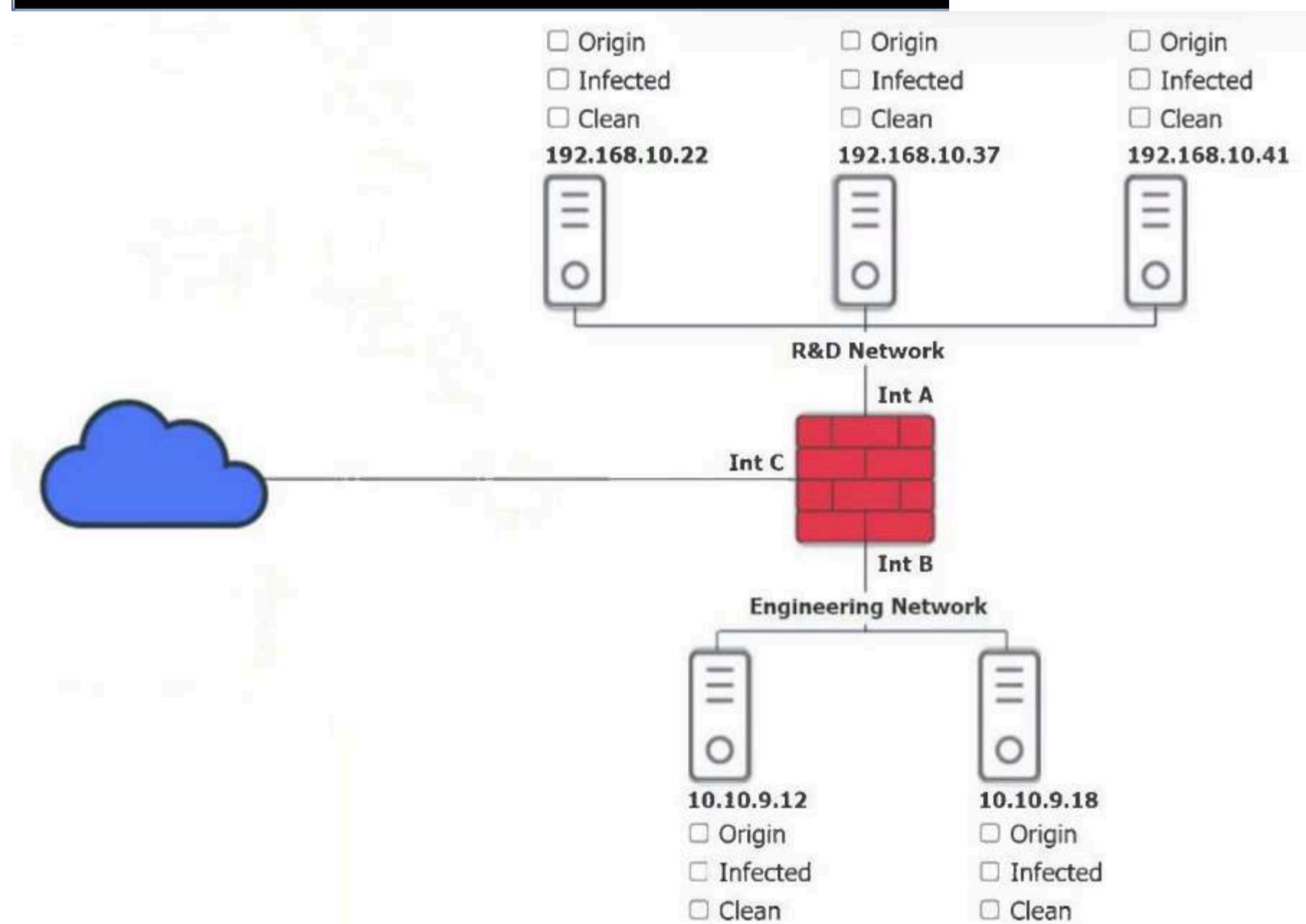
10.10.9.12

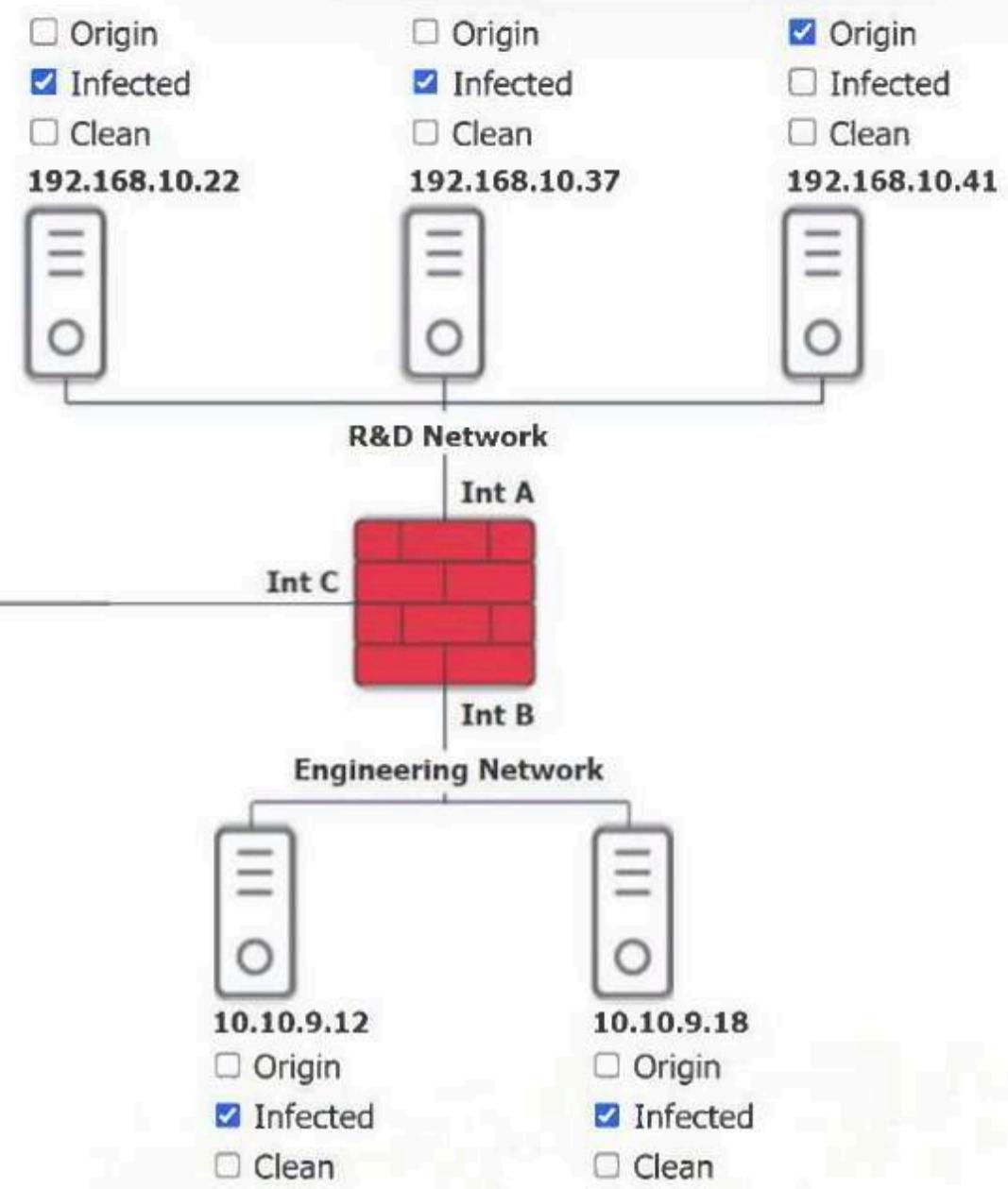
X

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

10.10.9.18

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svchost.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svchost.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```

**Hide Answer**

Suggested Answer:

by 3056f7e at May 10, 2024, 2:03 a.m.

Comments

Fazliddin4515 4 months, 3 weeks ago

Why Are you choosing random answers.
Here is real answers => {
22 is Origin. It has started infection first.
37 is Clean, because it is able to get new updates and quarantine malicious file.
41 is Infected, because it was not able to quarantine infected file.
12 is Clean, because it is able to get new updates and quarantine malicious file.
18 is Infected, because it was not able to get new update and quarantine file.

These are real answers.

upvoted 52 times

edmondme 3 months, 4 weeks ago

41 is the origin, since that's the one has smbv1. 22 even though the time was earlier, its not the origin.
upvoted 4 times

Boats 4 months, 1 week ago

This is correct.
upvoted 5 times

succulentchinesemeal 4 months, 3 weeks ago

thank you. makes so much more sense now
upvoted 5 times

c80f5c5 4 months ago

Commenting to reiterate Fazliddin's comment:
.22 infected at 2:31AM, it was infected 12 hrs before all other IPs
.37 clean, quarantined at 2:43PM
.41 infected at 2:43PM
.12 clean, quarantined at 2:43PM
.18 infected at 2:43PM

I took a Sec+ Bootcamp and they went over this lab, these are the answers they gave us.

upvoted 15 times

Monopeeya Most Recent 15 hours, 54 minutes ago

.37 reached out over the internet after the initial virus scan on the 17th, which we know can detect the virus regardless of infected status. It was on 443 (secure port) but was using SSL (outdated insecure) instead of TLS. This was their "gotcha".

Viruses do not come out of nowhere. It had to be one of the two that reached out to the internet after the first scan. You would not see the lateral communication of IPs on either side of the firewall because they are not talking across it. The 192 side of the firewall were the only ones to start trying to make connections to check software version of the 10 side of the firewall.

.22 - smbV1 - least secure. Had AV scan completely disabled.
.41 .18 - smbV2 - little more secure. Was able to prevent definition updates. Preventing QT.
.12 .37 - smbV3 - secure. Was not able to modify AV scan. Definitions updated. Malware QT.
upvoted 1 times

Monopeeya 16 hours, 3 minutes ago

TLDL THE ORIGIN IS NOT .22

.37 Origin (QT'd)
.22 (Still Infected)
.41 (Still Infected)
.12 (QT'd)
.18 (Still Infected)

I do not know if Comptia considers a host with quarantined malware as infected, but all PCs had the malware. Here is the break down if you are interested..

upvoted 1 times

jsmthy 1 week, 2 days ago

22 Infected
37 Origin
41 Infected
12 Clean
18 Infected

192.168.10.37 is the origin point because it is 1 of 2 IP addresses that accessed the public internet prior to 02:30, has a visible file transfer chain, and is tied to active reconnaissance activity. Furthermore, we must note the firewall's location means only cross firewall access is recorded to the log. Lateral movement is not recorded.

Let's get rid of the incumbent answer: 22 can't be the origin because we must take the host log on the 17th as fact that 22 was clean at that time, otherwise the scan should have triggered the heuristic match on the 17th. It would not have started its own infection when it was perfectly fine and there is no proof of other file transfers other than the firewall itself.

No, I believe 22 was selected as a host with persistence and the process looks like this:

37 is infected at 16:01 via a malicious file.
12 is infected at 16:35 via SMBv2.

12 sends out a ping sweep at 23:58, identifying active machines on the network.
22 executes post-exploit payload at 02:30.

18 performs what looks like exfiltration (9GB) at 02:39.

This is the limit of what I see with these logs. Maybe I'm overthinking it since it is this a Comptia exam.

upvoted 1 times

FrozenCarrot 4 weeks, 1 day ago

10.22 Origin
10.37 Clean
10.41 Infected
9.12 Clean
9.18 Infected
upvoted 1 times

PAWarriors 1 month ago

Correct answers:

10.22 --> started the infection and scvh0st.exe disabled scheduled scan and update. (Origin)
10.37 --> the malicious file was in quarantine and it got a new update. (Clean)
10.41 --> No update unable to quarantine file. (Infected)
9.12 --> the malicious file was in quarantine and it got a new update. (Clean)
9.18 --> No update and unable to quarantine. (Infected)

upvoted 2 times

3330278_111 1 month, 1 week ago

If .22 is the Origin, then it's also infected, right? The scan got disabled right away, and it continued spreading to the other computers afterwards. So I'm checking both Origin and Infected for .22 if they allow me to
upvoted 2 times

barracouto 2 months, 2 weeks ago

If I get this question i'm going to think "OH boy do I miss cici's pizza"
22- Origin - OH

CICI
37 - Clean
41 - Infected
12 - Clean
18 - Infected
upvoted 6 times

✉️ **WOW_ThatsCrazy** 2 months, 3 weeks ago

192.168.10.22

Status: Clean

Reasoning: The scan completed without finding any issues.

192.168.10.37

Status: Infected

Reasoning: The scan found and quarantined the file svch0st.exe.

192.168.10.41

Status: Infected

Reasoning: The scan found the file svch0st.exe but was unable to quarantine it.

10.10.9.12

Status: Origin

Reasoning: The firewall log shows traffic from 10.10.9.12 to multiple IP addresses in the network, indicating it may have spread the infection.

Additionally, the scan found and quarantined svch0st.exe.

10.10.9.18

Status: Infected

Reasoning: The scan found the file svch0st.exe but was unable to quarantine it, similar to 192.168.10.41.

upvoted 2 times

✉️ **jennyka76** 3 months, 1 week ago

I AGREE

22 is Origin. It has started infection first.

37 is Clean, because it is able to get new updates and quarantine malicious file.

41 is Infected, because it was not able to quarantine infected file.

12 is Clean, because it is able to get new updates and quarantine malicious file.

18 is Infected, because it was not able to get new update and quarantine file.

upvoted 3 times

✉️ **Etc_Shadow28000** 3 months, 3 weeks ago

Conclusion

Based on the logs, 192.168.10.37 appears to be the first to identify and quarantine the svch0st.exe file on 4/18/2019 at 14:34, suggesting it might have been the origin of the infection.

Status of Each Host

- 192.168.10.22:Infected Scheduled update disabled by svch0st.exe, no quarantine action

- 192.168.10.37:Infected svch0st.exe quarantined

- 192.168.10.41:Infected svch0st.exe detected and quarantined after initial failure

- 10.10.9.12: Infected svch0st.exe quarantined

- 10.10.9.18:Infected svch0st.exe detected and quarantined after initial failure

Summary

- 192.168.10.22:Infected

- 192.168.10.37:Origin

- 192.168.10.41:Infected

- 10.10.9.12:Infected

- 10.10.9.18:Infected

upvoted 2 times

✉️ **420JhonnySins69** 1 month ago

wrong

37

4/18/2019 14:34 Update

4/18/2019 14:37 WARN

47

4/18/2019 14:37 heuristic pattern

upvoted 1 times

✉️ **Mehsotopes** 4 months, 2 weeks ago

Every computer was clean until the 18th, & the first computer to do insecure communication protocols was 192.168.10.41 on the 17th using SMBv1 which is not a recommended, or safe protocol to use anymore.

A host is still considered infected even with quarantined virus files.

upvoted 3 times

✉️ **e5c1bb5** 4 months, 2 weeks ago

origin is 41. it uses SMBV1 (an unsecure application) first. then you can see the RPC being used which was used in multiple documented malware attacks (wannacry, etc.). so starts with 41 sending malware with SMBV1 then RPC to others

upvoted 2 times

✉️ **Yoez** 4 months, 3 weeks ago

and also if you check the traffic on the Firewall at 2:31:45 AM, this trade was used for HTTP, that is an unsecured port

upvoted 2 times

✉️ **Yoez** 4 months, 3 weeks ago

for me is ORIGIN, and the rest infected because they installed the update that was the .EXE. And the first one is the ORIGIN because I sow the .exe at 2:00 AM and the rest was 2:00pm

upvoted 3 times

✉️ **3056f7e** 4 months, 4 weeks ago

It must be origin, clean, infected, clean, infected

upvoted 6 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 78 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 78

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A. Preparation Most Voted
- B. Recovery
- C. Lessons learned
- D. Analysis

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (81%)

C (19%)

by [mr_reyes](#) at May 21, 2024, 12:51 p.m.

Comments

✉ [Etc_Shadow28000](#) Highly Voted 3 months, 3 weeks ago

Selected Answer: A

A. Preparation

The preparation phase in the incident response process is when a security analyst reviews roles and responsibilities. This phase involves planning and setting up the necessary tools, processes, and team structures to effectively respond to potential security incidents.

Therefore, the correct answer is:

- A. Preparation
upvoted 8 times

✉ [Cee007](#) Most Recent 1 month ago

Selected Answer: A

A. Preparation
upvoted 1 times

 **dbrowndiver** 2 months, 1 week ago

Selected Answer: A

The Preparation phase is the initial step in the incident response process where an organization establishes the foundation for handling potential incidents. It involves planning, setting up necessary tools, and defining roles and responsibilities.

upvoted 2 times

 **a4e15bd** 2 months, 1 week ago

The correct phase for reviewing and defining roles and responsibilities in the incident response process is the preparation phase. Lessons Learned is more about reviewing the entire incident after it has been resolved, identifying what went well and what didn't and making improvements for future responses.

upvoted 1 times

 **AutoroTink** 3 months, 4 weeks ago

Selected Answer: A

This is a tough one! "The Preparation phase includes not only the initial establishment of roles and responsibilities but also their ongoing review and maintenance". I feel like these two steps kind of can blend into each other...review/lessons learned of one incident, can be preparation for the next incident.

upvoted 3 times

 **leedsbarber** 4 months ago

Selected Answer: A

Roles and responsibilities should be regularly reviewed, not just after an event. This enables good preparation.

Events are reviewed retrospectively, that's when lessons are learned.

upvoted 3 times

 **MahiMahiMahi** 4 months ago

Selected Answer: C

C. Review seems to be the key word here.

upvoted 2 times

 **mr_reyes** 4 months, 2 weeks ago

Selected Answer: C

Given the options, the phase in the incident response process when a security analyst reviews roles and responsibilities is the Lessons learned phase. During this phase, the team reflects on their performance, identifies gaps, and ensures that roles and responsibilities are well-defined and understood for future incidents. The keyword in this question is "reviews". In the Lessons Learned step we review the roles to see if anything needs to be changed, in the preparation step we are just creating the roles, nothing to review yet.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 79 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 79

Topic #: 1

[\[All SY0-701 Questions\]](#)

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols
- C. VLANs
- D. Web-based administration Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [499c5c4](#) at June 12, 2024, 12:13 p.m.

Comments

✉ **499c5c4** Highly Voted 3 months, 4 weeks ago

The most appropriate option to disable to harden the routers would be:

- D. Web-based administration

Web-based administration, also known as remote management or HTTP/HTTPS access, is a common feature in routers that allows administrators to manage the device remotely using a web browser. However, this feature also introduces a potential vulnerability, as it opens up the router to potential web-based attacks.

Disabling web-based administration would reduce the attack surface and prevent potential exploits, making the router more secure.

Console access (A) is necessary for local management, routing protocols (B) are essential for network operation, and VLANs (C) are used for network segmentation and security. Disabling web-based administration (D) is the most appropriate option to harden the router.

upvoted 9 times

✉ **chasingsummer** Most Recent 1 month, 3 weeks ago

Selected Answer: D

D. Web-based administration
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 80 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 80

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

- A. SPF
- B. GPO
- C. NAC
- D. FIM Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by Abcd123321 at May 12, 2024, 10:02 p.m.

Comments

✉ Etc_Shadow28000 Highly Voted 5 months, 1 week ago

Selected Answer: D

D. FIM (File Integrity Monitoring)

File Integrity Monitoring (FIM) is a security technology that monitors and detects changes in files. FIM solutions can track modifications, access, or deletions of files and notify administrators of any changes, thus ensuring data integrity and security.

Therefore, the correct answer is:

D. FIM
upvoted 7 times

✉ Examplary Highly Voted 1 month, 2 weeks ago

Note to the admins: There is a typo in this one.
"checks SO track any changes" should be
"checks TO track any changes"

upvoted 6 times

✉ **Syl0** Most Recent 2 months, 2 weeks ago

SPF - Sender policy framework - identify mail servers that are allowed to send emails to domain
GPO - Group Policy Object - let admin control and implement a group of settings
NAC - Network Access Control - Restricts unauthorised users and devices from gaining access to the network
FIM - File Integrity Monitoring - security process that monitors and analyses integrity of asset
upvoted 3 times

✉ **whatsupdeepak** 6 months ago

FIM - stands for File Integrity Monitoring, which is a method to secure data by detecting any changes
upvoted 4 times

✉ **Abcd123321** 6 months, 1 week ago

Selected Answer: D

File Integrity Monitoring (FIM)

- Validates the integrity of operating system and application software files by comparing their current state with a known, good baseline
- Identifies changes to
 - Binary files
 - System and Application Files
 - Configuration and Parameter Files
- Monitors critical system files for changes using agents and hash digests, triggering alerts when unauthorized changes occur

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

◀ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 81 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 81

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	09/16/2022 11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

- A. Brute-force attack Most Voted
- B. Privilege escalation
- C. Failed password audit
- D. Forgotten password by the user

[Hide Answer](#)**Suggested Answer: A***Community vote distribution*

A (100%)

by Etc_Shadow28000 at June 12, 2024, 6:44 p.m.

Comments **Etc_Shadow28000** Highly Voted 3 months, 3 weeks ago**Selected Answer: A**

A. Brute-force attack

The log shows multiple failed login attempts within a very short time frame, which is characteristic of a brute-force attack. In a brute-force attack, an attacker attempts many different passwords or passphrases with the hope of eventually guessing correctly. The pattern of frequent and continuous login failures seen in the log entries aligns with this type of attack.

Therefore, the correct answer is:

A. Brute-force attack
upvoted 7 times **PAWarriors** Most Recent 1 month ago**Selected Answer: A**

A. Brute-force attack

--> Event ID 4625 is logged for any logon failure. It generates on the computer where logon attempt was made.
--> In this scenario we can see multiple login attempts every few seconds indicating that this is a potential brute-force attack.
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 82 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 82

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Choose two.)

A. Key escrow Most Voted

B. TPM presence Most Voted

C. Digital signatures

D. Data tokenization

E. Public key management

F. Certificate authority linking

[Hide Answer](#)

Suggested Answer: AB

Community vote distribution

AB (100%)

by [e5c1bb5](#) at May 9, 2024, 10:56 p.m.

Comments

✉ **dbrowndiver** 2 months ago

Selected Answer: AB

In this scenario, A. Key escrow and B. TPM presence are the most important considerations for implementing Full Disk Encryption (FDE) on laptops. These elements ensure that encryption keys are securely managed and stored, providing both data security and recoverability in case of lost keys, and that hardware-based security is used to protect against unauthorized access.

upvoted 1 times

✉ **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: AB

A. Key escrow
B. TPM presence

- **Key escrow:** This is important to ensure that encryption keys can be recovered in case they are lost or forgotten. It is a crucial consideration for Full Disk Encryption (FDE) to maintain access to data even if issues arise with the primary encryption keys.
- **TPM presence:** Trusted Platform Module (TPM) is a hardware-based security feature that can store encryption keys securely. Ensuring the presence of TPM on laptops enhances the security of FDE by protecting the encryption keys from being accessed or tampered with.

Therefore, the most important considerations for the security engineer are:

- A. Key escrow
 - B. TPM presence
- upvoted 3 times

 **Shaman73** 4 months ago

Selected Answer: AB

- A. Key escrow
 - B. TPM presence
- upvoted 1 times

 **shady23** 4 months, 3 weeks ago

Selected Answer: AB

- A. Key escrow
 - B. TPM presence
- upvoted 1 times

 **shady23** 4 months, 3 weeks ago

Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.

TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and

upvoted 1 times

 **Fazliddin4515** 4 months, 3 weeks ago

I think E is also correct one
upvoted 1 times

 **Yoez** 4 months, 4 weeks ago

I don't think so that are the correct answers.
upvoted 1 times

 **e5c1bb5** 4 months, 4 weeks ago

Selected Answer: AB

this one is tough because public key management is fundamental to full disc encryption.
that being said, key escrow is arguably more important for the following reasons.

public key's are used to encrypt the data and the PRIVATE key is used to decrypt the data.
once the data is encrypted, i would argue who holds the keys (another department or another 3rd party) is more important than establishing the encryption (because that's kind of the easy part). TPM presence is even more fundamental to FDE than the public key is because without it, you can't even consider FDE. those are my thoughts going with AB for now. please share your thoughts. if i didn't pick AB i'd go BE
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 83 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 83

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

- A. Changing the remote desktop port to a non-standard number
- B. Setting up a VPN and placing the jump server inside the firewall Most Voted
- C. Using a proxy for web connections from the remote desktop server
- D. Connecting the remote server to the domain and increasing the password length

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [MahiMahiMahi](#) at June 4, 2024, 10:34 p.m.

Comments

✉ **dbrowndiver** 2 months ago

Selected Answer: B

Setting up a VPN and placing the jump server inside the firewall is the most secure approach because it reduces the attack surface and ensures that only authorized users can access the remote desktop service. This solution addresses the primary security concern of protecting sensitive production systems by ensuring that only verified users can gain access, thus minimizing the attack surface and potential vulnerabilities.
upvoted 3 times

✉ **Shaman73** 4 months ago

Selected Answer: B

B. Setting up a VPN and placing the jump server inside the firewall
upvoted 1 times

✉ **MahiMahiMahi** 4 months ago

Selected Answer: B

B. Setting up a VPN and placing the jump server inside the firewall

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 84 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 84

Topic #: 1

[\[All SY0-701 Questions\]](#)

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. ACL
- B. DLP
- C. IDS
- D. IPS Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (96%) 4%

by AutoroTink at May 8, 2024, 5:28 a.m.

Comments

AutoroTink Highly Voted 5 months ago

Selected Answer: D

An IPS is designed to continuously monitor network traffic and take immediate action to block potential threats based on known signatures. It's an active security measure that not only detects but also prevents the exploitation of known vulnerabilities.

- A. ACL (Access Control List): ACLs are used to control the flow of traffic based on rules, but they are not dynamic enough to monitor or block signature-based attacks effectively.
- B. DLP (Data Loss Prevention): DLP systems are focused on preventing data breaches by detecting and blocking potential data leaks/exfiltration, not on monitoring or blocking attacks per se.
- C. IDS (Intrusion Detection System): While an IDS can detect known signature-based attacks, it does not block them; it only alerts the system administrators of the potential threat.
- D. IPS (Intrusion Prevention System): As mentioned, an IPS actively monitors and blocks attacks, making it the most suitable option for the scenario described.

upvoted 8 times

barracouto Most Recent 3 days, 9 hours ago

Selected Answer: D

ACL (Access Control List): Used to control network traffic and define which users or system processes have permissions to access resources or perform operations on a network.

DLP (Data Loss Prevention): Designed to prevent sensitive data from being lost, misused, or accessed by unauthorized users, and to monitor data transfers to ensure compliance with data protection policies.

IDS (Intrusion Detection System): Monitors network or system activities for malicious activities or policy violations. An IDS alerts administrators of potential threats but does not take action to block them.

IPS (Intrusion Prevention System): Monitors and controls network and system activities to protect against malicious activities by detecting and preventing attacks in real-time. An IPS can block traffic that matches known attack signatures.

Correct Answer: D. IPS

The IPS is the appropriate solution as it can monitor and block known signature-based attacks.

upvoted 3 times

 **Collapsar** 3 days, 9 hours ago

Selected Answer: D

An IPS is designed to continuously monitor network traffic and take immediate action to block potential threats based on known signatures. It's an active security measure that not only detects but also prevents the exploitation of known vulnerabilities.

- A. ACL (Access Control List): ACLs are used to control the flow of traffic based on rules, but they are not dynamic enough to monitor or block signature-based attacks effectively.
- B. DLP (Data Loss Prevention): DLP systems are focused on preventing data breaches by detecting and blocking potential data leaks/exfiltration, not on monitoring or blocking attacks per se.
- C. IDS (Intrusion Detection System): While an IDS can detect known signature-based attacks, it does not block them; it only alerts the system administrators of the potential threat.
- D. IPS (Intrusion Prevention System): As mentioned, an IPS actively monitors and blocks attacks, making it the most suitable option for the scenario described.

upvoted 1 times

 **bufffalobilll** 2 weeks, 5 days ago

Selected Answer: D

And block

upvoted 1 times

 **a0bfa81** 2 weeks, 5 days ago

Selected Answer: D

D. IPS - Intrusion Prevention System
is the correct answer

upvoted 1 times

 **93a09c9** 2 months ago

D is the correct answer here. The answer is most definitely not C.

upvoted 1 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: D

D. IPS (Intrusion Prevention System)

An Intrusion Prevention System (IPS) is designed to monitor network and/or system activities for malicious activities or policy violations and can take actions to block or prevent those activities. Since the enterprise is dealing with known signature-based attacks, an IPS is the best solution because it can actively block these attacks by using signatures to identify and mitigate them in real-time.

Therefore, the correct answer is:

D. IPS

upvoted 1 times

 **Shaman73** 4 months ago

Selected Answer: D

D:

IPS

upvoted 1 times

 **SHADTECH123** 4 months, 3 weeks ago

Selected Answer: D

An Intrusion Prevention System (IPS) is designed to monitor network traffic for suspicious activity, and it can take proactive steps to block or prevent those activities in real-time. IPS uses signature-based detection to identify known vulnerabilities and exploits, making it particularly effective against attacks that exploit well-documented and widely known browser vulnerabilities.

upvoted 3 times

 **shady23** 4 months, 4 weeks ago

Selected Answer: D

D. IPS

upvoted 1 times

 **Mehsotopes** 4 months, 4 weeks ago

Selected Answer: C

An IPS system being configured can have a chance of blocking code that certain systems with newer web browsers may need, or not be vulnerable to at all. An IDS would allow you to be notified of these recognized signatures, & determine if it's appropriate to allow, or not.

Another safe option would be to know what systems are using older browser versions, & update them, if not, then segment them specifically, & use an IPS appliance if anti-virus automation is what is necessary.

upvoted 1 times

 **e5c1bb5** 4 months, 4 weeks ago

Selected Answer: D

was confused by "correct answer" IPS forsure

upvoted 1 times

 **Kevans242** 5 months ago

Selected Answer: D

Definitely D

upvoted 1 times

 **e56400d** 5 months ago

Can someone explain to me why the answer is IDS?

IDS only alerts, it does not block anything. IPS alerts and blocks suspicious activity. Therefore, the answer should be IPS.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 85 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 85

Topic #: 1

[\[All SY0-701 Questions\]](#)

Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

- A. Remote access points should fail closed.
- B. Logging controls should fail open.
- C. Safety controls should fail open. Most Voted
- D. Logical security controls should fail closed.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Mehsotopes](#) at May 10, 2024, 1:28 a.m.

Comments

✉ **dbrowndiver** 2 months ago

Selected Answer: C

Safety controls failing open is a critical design principle that ensures human life is prioritized in the event of a failure. This principle applies to situations where failing open provides an immediate safety benefit, such as allowing exit doors to unlock automatically during a fire.

upvoted 3 times

✉ **Shaman73** 4 months ago

Selected Answer: C

C. Safety controls should fail open.
upvoted 1 times

✉ **Yoez** 4 months, 4 weeks ago

Selected Answer: C

C. Safety controls should fail open: Safety controls, such as fire suppression systems or emergency exits, should indeed fail open. This means that in the event of a failure or malfunction, they should default to a state that ensures safety, such as allowing people to exit a building or mitigating

hazards.

upvoted 2 times

 **Mehsotopes** 4 months, 4 weeks ago

Selected Answer: C

Fail Open:

* Activates specified controls; in this case, safety measures such as sprinklers, or alarm systems to ensure the safety of staff members, & system devices.

Fail Close:

* Locks controls such as access to the perimeter, & devices to protect from exfiltration.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 86 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 86

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be best suited for constantly changing environments?

- A. RTOS
- B. Containers Most Voted
- C. Embedded systems
- D. SCADA

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by CyberPark17 at May 30, 2024, 12:31 a.m.

Comments

✉️ dbrowndiver 3 days, 10 hours ago

Selected Answer: B

In this scenario, Choice B is the correct answer. Containers are the correct answer because they are specifically designed to provide flexibility and scalability in constantly changing environments. Containers allow for rapid deployment and scaling, making them ideal for dynamic applications that need to adapt to frequent changes and updates. Furthermore containers are particularly well-suited for microservices architectures, continuous integration/continuous deployment (CI/CD) pipelines, and environments that need to rapidly adapt to change. Technologies like Docker and Kubernetes have made containers popular for modern application deployment.

upvoted 4 times

✉️ Syl0 1 month ago

RTOS - real time OS

SCADA - supervisory control and data acquisition

upvoted 1 times

✉️ c469c8e 1 month, 1 week ago

lacking context

upvoted 2 times

 **Shaman73** 4 months ago

Selected Answer: B

B containers

upvoted 1 times

 **c18525f** 4 months ago

B containers

upvoted 1 times

 **CyberPark17** 4 months, 1 week ago

answer is D, Containers, they provide a consistent and isolated environment for applications to run, regardless of the underlying infrastructure. They are highly portable and can be quickly deployed, making them a flexible solution for dynamic environments where applications need to be scaled, updated, or moved frequently. Real-time operating systems (RTOS) are designed for predictable and deterministic tasks, while embedded systems and SCADA are more specialized and may not be as adaptable to rapidly changing conditions.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 87 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 87

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following incident response activities ensures evidence is properly handled?

- A. E-discovery
- B. Chain of custody Most Voted
- C. Legal hold
- D. Preservation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Punjistetics](#) at May 10, 2024, 1 a.m.

Comments

✉ **986d14e** 1 month, 2 weeks ago

Selected Answer: B

The answer is B. E-discovery has nothing to do with this.
upvoted 3 times

✉ **93a09c9** 2 months ago

Selected Answer: B

The answer is B. E-discovery has nothing to do with this.
upvoted 2 times

✉ **dbrowndiver** 2 months ago

In this scenario, choice B is correct . Chain of custody is the correct answer because it is specifically designed to ensure that evidence is properly handled, tracked, and documented throughout the incident response process. This approach ensures the integrity and admissibility of evidence in legal settings by maintaining a clear and reliable record of its handling.
upvoted 3 times

Etc_Shadow28000 3 months, 3 weeks ago

Selected Answer: B

B. Chain of custody

Chain of custody is the process that ensures evidence is properly handled and documented throughout its lifecycle. It tracks the evidence from the time it is collected, through its transportation, storage, and presentation in court, ensuring that it has not been altered or tampered with. Maintaining a proper chain of custody is critical for ensuring the integrity and admissibility of the evidence in legal proceedings.

Therefore, the correct answer is:

B. Chain of custody
upvoted 4 times

Shaman73 4 months ago

Selected Answer: B

B. Chain of custody
upvoted 1 times

SHADTECH123 4 months, 3 weeks ago

Selected Answer: B

Chain of custody refers to the process of documenting the handling of evidence from the time it is collected until it is presented in court. This documentation includes details on who collected the evidence, how it was collected, transported, stored, and any transfers of possession
upvoted 3 times

Abcd123321 4 months, 3 weeks ago

Selected Answer: B

Chain of Custody

Documented and verifiable record that tracks the handling, transfer, and preservation of digital evidence from the moment it is collected until it is presented in a court of law
upvoted 1 times

Yoez 4 months, 4 weeks ago

Selected Answer: B

for me is B
upvoted 3 times

shady23 4 months, 4 weeks ago

Selected Answer: B

B. Chain of custody
upvoted 2 times

Punjistetics 4 months, 4 weeks ago

Selected Answer: B

The correct answer is B. Chain of custody.

Chain of custody refers to the documentation and processes used to maintain control and accountability of evidence during an investigation. It ensures that evidence is properly handled, preserved, and protected from tampering, alteration, or loss.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 88 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 88

Topic #: 1

[\[All SY0-701 Questions\]](#)

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?

- A. Standardizing security incident reporting
- B. Executing regular phishing campaigns
- C. Implementing insider threat detection measures
- D. Updating processes for sending wire transfers

[Most Voted](#)

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (91%) 9%

by [Shaman73](#) at June 6, 2024, 12:30 p.m.

Comments

✉ [Etc_Shadow28000](#) Highly Voted 3 days, 9 hours ago

[Selected Answer: D](#)

D. Updating processes for sending wire transfers

Updating the processes for sending wire transfers would most likely prevent this type of activity in the future. This could include implementing additional verification steps, such as requiring multiple levels of approval, verifying new payment instructions through a separate communication channel, or implementing a callback procedure to confirm the authenticity of the instructions.

Therefore, the correct answer is:

D. Updating processes for sending wire transfers
upvoted 7 times

✉ [dbrowndiver](#) Most Recent 3 days, 9 hours ago

[Selected Answer: D](#)

In this scenario, the option should be D because updating processes for sending wire transfers is the best choice, it directly tackles the procedural weakness that allowed the fraudulent transaction to occur. Implementing verification and approval procedures can prevent similar incidents by ensuring that all payment instructions are authenticated and verified before any money is transferred, thereby reducing the risk of fraud.

upvoted 2 times

 **EfaChux** 1 month, 2 weeks ago

Selected Answer: B

The accounting clerk acted in ignorance. more phishing campaigns would have prevented the transfer

upvoted 1 times

 **3330278_111** 1 month, 1 week ago

It doesn't really prevent it the same way that updating a process for sending a wire transfer would. What phishing campaigns do is reduce the likelihood of it happening again, which isn't what the question is asking for

upvoted 1 times

 **3396ee7** 3 months, 3 weeks ago

A is the correct answer

upvoted 1 times

 **Shaman73** 4 months ago

Selected Answer: D

D. Updating processes for sending wire transfers

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 89 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 89

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration Most Voted
- C. Baseline
- D. Policy enforcement

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [e5c1bb5](#) at May 11, 2024, 12:34 a.m.

Comments

✉ [e5c1bb5](#) Highly Voted 6 months, 1 week ago

Selected Answer: B

A makes no sense

B orchestration and automation are treated as the same in the exam objectives so not sure on this one

C establishing a baseline (confused on this one) a baseline for what? if it means a baseline for account creation then yes, if it means a baseline like a policy then no..

D policy enforcement.. idk if you'd need to write a script for that as much as you'd rely on software..

going with B since the first part of the question doesn't mention automation/orchestration even though the question is very poorly worded.

upvoted 8 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: B

Orchestration provides a comprehensive approach to automating complex workflows, making it an excellent choice for efficiently managing account creation processes in large-scale environments. Orchestration is ideal for automating the creation of user accounts, as it can handle the

sequence of tasks required to set up accounts, such as creating usernames, assigning permissions, configuring email, and setting up directory services.

upvoted 3 times

 **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. Orchestration

upvoted 1 times

 **c80f5c5** 5 months, 2 weeks ago

Orchestration refers to the automated configuration, management, and coordination of complex computer systems, applications, and services. In the context of creating a script for account creation, orchestration is a good use case because it allows the systems administrator to automate the entire process of creating user accounts efficiently and accurately, thereby saving time and reducing human error.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 90 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 90

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

- A. Processor
- B. Custodian
- C. Subject Most Voted
- D. Owner

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (87%) 13%

by Ochopperfan at May 10, 2024, 6:31 p.m.

Comments

EOtero Highly Voted 4 months, 3 weeks ago

From Professor Messer study notes:

- Data subject
- Any information relating to an identified or identifiable natural person
 - An individual with personal data
 - This includes everyone
 - Name, ID number, address information, genetic makeup, physical characteristics, location data, etc.
 - You are the data subject
 - Laws and regulations
 - Privacy is ideally defined from the perspective of the data subject

Data owner

- Accountable for specific data, often a senior officer

- VP of Sales owns the customer relationship data
- Treasurer owns the financial information

I'm also going with C.

upvoted 7 times

✉️ **AutoroTink** Most Recent 3 days, 10 hours ago

Selected Answer: C

The Marketing Department Head or other senior-level manager is likely something like the Data Protection Officer or Owner, responsible for the data.

The Infrastructure Team are likely the Custodians.

The data is likely being collected and processed by lower-level employees and/or automated processes. These would be the Data Processors. That leaves the customer whose data is being collected. They aren't the owners of their own data (like others have stated), but they are the data subject. So C is the most accurate answer.

upvoted 3 times

✉️ **Etc_Shadow28000** 3 days, 10 hours ago

Selected Answer: C

C. Subject

In the context of data roles, the customer whose sensitive data is being collected, modified, and stored is referred to as the "Subject." The data subject is the individual to whom the data pertains.

Therefore, the correct answer is:

C. Subject

upvoted 4 times

✉️ **Fhaddad81** 1 month ago

D is the correct Answer as Data subject is who own the data while Owner is the customer that data subject given their data. Data subject is not mentioned on Udemy course !!

upvoted 1 times

✉️ **qacollin** 2 months ago

Selected Answer: C

chat gpt

upvoted 1 times

✉️ **dbrowndiver** 2 months ago

Selected Answer: C

In this scenario, the customers are the data subjects because the sensitive information collected, modified, and stored by the marketing department pertains to them. The customers are the individuals whose data is being processed.

upvoted 3 times

✉️ **Shaman73** 4 months ago

Selected Answer: C

C. Subject

upvoted 1 times

✉️ **hasquaati** 4 months, 3 weeks ago

Selected Answer: C

Answer is c. Technically the customer does own their own data, however in the Cybersecurity context the Owner is someone within the organization. According to ISO/IEC 27001, the data owner is responsible for ensuring the confidentiality, integrity, and availability of information assets.

upvoted 2 times

✉️ **Xavierallen9711** 4 months, 3 weeks ago

Selected Answer: D

Owner is the right answer

upvoted 1 times

✉️ **Yoez** 4 months, 4 weeks ago

Selected Answer: C

C. Subject

In this scenario, the customer is the subject of the sensitive data being collected, modified, and stored by the marketing department. The customer's data is being processed and managed by the marketing department, but the customer themselves is the subject of that data. They are the individuals to whom the data pertains.

upvoted 4 times

✉️ **e5c1bb5** 4 months, 4 weeks ago

Selected Answer: C

although not covered in study material ive looked at, the customer is definately not the processor or the controller. owners are usually senior management so thats out. going with subject.

upvoted 2 times

 **EOTERO** 4 months, 3 weeks ago

It is for Professor Messer's SY0-701 notes.

upvoted 1 times

 **Ochopperfan** 4 months, 4 weeks ago

Selected Answer: D

Why wouldn't the customer be the data owner? I don't remember Data Subject being apart of the 701 Course
upvoted 2 times

 **EOTERO** 4 months, 3 weeks ago

5.4 Summarize elements of effective security compliance.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 91 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 91

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes the maximum allowance of accepted risk?

- A. Risk indicator
- B. Risk level
- C. Risk score
- D. Risk threshold Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 6, 2024, 12:33 p.m.

Comments

  [dbrowndiver](#) 2 months ago

Selected Answer: D

This refers to the point or level of risk that an organization is willing to tolerate. Beyond this threshold, actions must be taken to mitigate or reduce the risk to an acceptable level. It defines the boundary between acceptable and unacceptable risk.

-The risk threshold is essentially the upper limit of risk that is deemed acceptable by an organization. It serves as a guideline for decision-making regarding risk management and response strategies.

-Organizations set risk thresholds based on their risk appetite and tolerance, helping them determine when to take action and allocate resources for risk mitigation.

upvoted 4 times

  [Shaman73](#) 4 months ago

Selected Answer: D

D. Risk threshold

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 92 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 92

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

- A. A worm is propagating across the network.
- B. Data is being exfiltrated. Most Voted
- C. A logic bomb is deleting data.
- D. Ransomware is encrypting files.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [MahiMahiMahi](#) at June 5, 2024, 8:43 p.m.

Comments

✉ **baronvon** 1 month, 3 weeks ago

Selected Answer: B

B. Data is being exfiltrated.

A large volume of DNS queries to external systems during non-business hours can indicate that data is being exfiltrated. Attackers often use DNS queries to covertly extract data from compromised systems, as DNS traffic is less likely to be scrutinized compared to other types of network traffic.
upvoted 2 times

✉ **dbrowndiver** 2 months ago

Selected Answer: B

The scenario describes an internal system sending unusual and large amounts of DNS queries to external systems, especially during non-business hours. This behavior is indicative of data exfiltration, where an attacker tries to move data out of the network covertly.
upvoted 3 times

✉ **Shaman73** 4 months ago

Selected Answer: B

B. Data is being exfiltrated.
upvoted 2 times

 **MahiMahiMahi** 4 months ago

Selected Answer: B

B. Data is being exfiltrated.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 93 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 93

Topic #: 1

[\[All SY0-701 Questions\]](#)

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

- A. Default credentials
- B. Non-segmented network
- C. Supply chain vendor
- D. Vulnerable software

[Most Voted](#)

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (41%) B (29%) C (29%)

by [Yoez](#) at May 11, 2024, 3 p.m.

Comments

✉ [Etc_Shadow28000](#) 3 months, 3 weeks ago

[Selected Answer: B](#)

B. Non-segmented network

Opening ports on a firewall for a new system introduces the risk that the new system might be deployed on a non-segmented network. This means that the new system and its traffic could potentially be exposed to other parts of the network, increasing the risk of lateral movement by an attacker if the system is compromised. Network segmentation helps in containing potential breaches and limiting access to sensitive areas of the network.

Therefore, the correct answer is:

B. Non-segmented network
upvoted 12 times

✉ [hasquaati](#) 4 months, 3 weeks ago

Selected Answer: C

I am thinking that opening firewall ports is a Layer 3 and Layer 4 issue and not a Layer 7 vulnerability, which is where the Vulnerable software would fit in. I would be more concerned about the Cloud provider which is why I am choosing C: Supply Chain Vendor.

upvoted 6 times

 **Ty13** Most Recent 3 days, 10 hours ago

Selected Answer: D

This is a really terrible question.

It could possibly be A because the software on the new system, with ports now being opened to the internet, might have a default username/password that an attacker could exploit.

But that would then mean that the software is vulnerable to those attacks to begin with.

upvoted 2 times

 **2fd1029** 3 days, 10 hours ago

Selected Answer: D

Given that the question specifically says "which is a risk in *the new system*" I would say that it can NOT be A or B because those are not risks with the provided system, they are risks with the corporate network in which the system is being deployed. It's a crapshoot between C & D depending on whoever wrote this vague question and decided what they wanted the answer to be. I would hazard to say D, because it most specifically relates to the system itself, and thus also the firewall ports that it will be whitelisted to communicate on.

upvoted 3 times

 **Hayder81** 3 weeks, 6 days ago

C. Supply chain vendor

upvoted 1 times

 **_denw** 1 month ago

Selected Answer: B

B. Non-segmented network

upvoted 1 times

 **850bc48** 1 month ago

Chat GPT says: When ports are opened on a firewall, it could expose the system to external threats, especially if the network is not properly segmented. A non-segmented network allows attackers who gain access to one part of the network to potentially move laterally across the network to other systems, increasing the risk of a breach.

A. Default credentials: This is a common risk but is not directly related to opening firewall ports.

C. Supply chain vendor: While this is an important risk, it is more related to the relationship with the SaaS provider rather than the direct consequence of opening firewall ports.

D. Vulnerable software: This is another risk, but it isn't as directly tied to the act of opening ports as network segmentation is. Therefore, Non-segmented network is the most relevant risk in this context.

upvoted 1 times

 **17f9ef0** 1 month ago

Selected Answer: B

It's B

upvoted 1 times

 **Dakshdabas** 1 month, 1 week ago

Selected Answer: C

C. Supply chain vendor

When deploying a system supported by a SaaS provider, you are relying on an external party to manage and secure the system. This introduces supply chain risks, as the security of your system now partially depends on the security practices of the SaaS provider. If the SaaS provider is compromised, it could impact your system and data.

A. Default credentials: While default credentials are a risk, they are generally more of a concern for the local system or devices rather than a SaaS provider.

B. Non-segmented network: This is a valid network security risk, but it is not specific to the SaaS context.

D. Vulnerable software: This is always a concern, but in the context of SaaS, the responsibility for managing software vulnerabilities often lies with the provider.

upvoted 1 times

 **tamcod** 1 month, 2 weeks ago

Every answer is a risk, opening ports allows for lateral movement, default credentials can be found online, supply chain is also a risk, do we know if their infrastructure is secure? Vulnerable software can be used to get into the system. These types of questions are awful.

upvoted 3 times

 **a4e15bd** 1 month, 3 weeks ago

The correct answer is D. While both Default credentials and Vulnerable Software are significant risk, but considering the specific context of opening ports on a firewall, Vulnerable Software sees to be the most critical because it directly relates to the potential exposure created by the newly opened ports.

upvoted 1 times

 **Kingamj** 1 month, 3 weeks ago

Selected Answer: B

A non-segmented network poses a risk by potentially exposing a broader range of network resources if the new system is compromised. Proper network segmentation helps mitigate this risk by isolating different parts of the network.

upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: D

Vulnerable software is the correct answer because:

- Direct Risk Connection: Opening firewall ports directly exposes the system's software to external threats. If the software has vulnerabilities, these can be exploited by attackers, especially when exposed to the internet or external networks.
- Exploitation Potential: Known vulnerabilities in software can be easily targeted by attackers using automated tools to scan and exploit open ports.
- Immediate Security Concern: The primary concern with opening ports is exposing internal systems to external attacks, making any vulnerabilities in the software a direct threat.

upvoted 2 times

 **f26ddcd** 3 months, 2 weeks ago

Selected Answer: D

Vulnerable software

upvoted 1 times

 **geocis** 3 months, 2 weeks ago

C.....A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

upvoted 1 times

 **Shaman73** 4 months ago

Selected Answer: D

I think D

upvoted 1 times

 **MAKOhunter33333333** 4 months, 2 weeks ago

Selected Answer: D

It asks about the risk inside the new system which makes me think what the new system is deploying,, software.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 94 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 94

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust Most Voted

B. AAA

C. Non-repudiation

D. CIA

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Shaman73](#) at June 6, 2024, 12:36 p.m.

Comments

  [dbrowndiver](#) Highly Voted 2 months ago

Selected Answer: A

Zero Trust is a security framework that aligns perfectly with the given requirements. It emphasizes strict access control, minimizing trust, and ensuring that all access requests are verified, making it an ideal choice for creating a secure environment.

upvoted 5 times

  [Shaman73](#) Most Recent 4 months ago

Selected Answer: A

A. Zero Trust

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 95 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 95

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following involves an attempt to take advantage of database misconfigurations?

- A. Buffer overflow
- B. SQL injection Most Voted
- C. VM escape
- D. Memory injection

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by MAKohunter33333333 at May 21, 2024, 2:46 p.m.

Comments

✉ **internslayer** 1 month, 3 weeks ago

My problem with this question is that it's not a misconfigured database that allows SQL injection, it's improperly sanitized user input fields in applications/web pages.

upvoted 3 times

✉ **dbrowndiver** 2 months, 1 week ago

Selected Answer: B

SQL injection is an attack that targets vulnerabilities in a database by injecting malicious SQL code into input fields. It takes advantage of misconfigured or improperly secured databases that do not validate or sanitize user input.

upvoted 2 times

✉ **Shaman73** 4 months ago

Selected Answer: B

B. SQL injection

upvoted 1 times

 **MAKOhunter33333333** 4 months, 2 weeks ago

Selected Answer: B

SQL Injection takes advantage of the misconfiguration of SQL databases and that do not validate input
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 96 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 96

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is used to validate a certificate when it is presented to a user?

A. OCSP Most Voted

B. CSR

C. CA

D. CRC

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (63%)

C (37%)

by 123456789User at May 31, 2024, 1:05 p.m.

Comments

✉ **c80f5c5** Highly Voted 4 months ago

CA issues and manages certificates.

OSCP - Online Certificate Status Protocol, a protocol that checks a certificate for validity and if its been revoked (by the CA).

The answer is OSCP. CA is like Congress, OSCP is like police. Congress records laws and writes them but don't actually enforce anything. Police enforce them

upvoted 25 times

✉ **2fd1029** Most Recent 3 weeks, 2 days ago

Selected Answer: A

Gotta be A. Can't be the CA because the CA issues the certs but isn't referred to for validating them, that's the CRL or OCSP.

upvoted 1 times

✉ **Cee007** 1 month ago

Selected Answer: A

A OCSP

upvoted 1 times

✉  **a4e15bd** 1 month, 3 weeks ago

It is A OCSP

This is a mechanism used to check the validity of a certificate in real time. When a certificate is presented, the user's system queries the OCSP responder to verify that the certificate is still valid and has not been revoked by CA.

The CA is responsible for issuing, revoking and managing digital certificates, but it does not perform the real time validation of the certificates.
upvoted 2 times

✉  **chasingsummer** 1 month, 3 weeks ago

Selected Answer: A

I don't think they are trying to trick us. I pick the simple answer.

upvoted 1 times

✉  **Crucible_Bro** 2 months ago

Selected Answer: A

A. Online Certificate Status Protocol is the actual protocol that is validating the request.
A CA simply manages those validations.

upvoted 1 times

✉  **dbrowndiver** 2 months ago

Selected Answer: A

When a certificate is presented to a user as written in the scenario(e.g., when visiting a secure website), the system can use OCSP to query the CA's OCSP responder. This helps determine whether the certificate is still valid or has been revoked.

-Real-Time Validation: Unlike Certificate Revocation Lists (CRLs), which are static lists of revoked certificates, OCSP provides dynamic, up-to-date information about the certificate's status, allowing for timely detection of compromised or invalid certificates.

Why this is the best fit: Security Assurance: By using OCSP, systems can ensure that a presented certificate is not only genuine but also has not been revoked due to compromise or other reasons. This real-time validation is critical for maintaining secure communications.

upvoted 2 times

✉  **WOW_ThatsCrazy** 3 months ago

Selected Answer: A

OCSP is used to validate the status of a digital certificate in real-time. When a certificate is presented to a user, the OCSP responder can be queried to check if the certificate is still valid or if it has been revoked. This provides a more efficient and timely method of certificate validation compared to traditional CRL (Certificate Revocation List) checks.

upvoted 2 times

✉  **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: A

A. OCSP (Online Certificate Status Protocol)

OCSP is used to validate a certificate when it is presented to a user by checking the certificate's revocation status. It provides real-time status information about the validity of a certificate, ensuring that it has not been revoked.

Therefore, the correct answer is:

A. OCSP

upvoted 2 times

✉  **drosas84** 4 months ago

Selected Answer: C

the question is tricky. It is basically asking what is "used" to validate a certificate when it is presented to a user. Meaning, what do you use to validate a certificate when giving it to a user to use? a CA.

An OCSP checks whether a certificate is valid or revoked, it doesn't validate a certificate.

This is how I read the question.

upvoted 4 times

✉  **a4e15bd** 2 months, 1 week ago

I think you are just contradicting yourself in the last part. If OCSP checks whether a certificate is valid or not, that is validating the certificate.

upvoted 1 times

✉  **edmondme** 4 months ago

Selected Answer: A

They are looking for the protocol OCSP

upvoted 1 times

✉  **Shaman73** 4 months ago

Selected Answer: A

A. OCSP

upvoted 1 times

✉  **123456789User** 4 months, 1 week ago

Selected Answer: C

Certificate Authority

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 97 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 97

Topic #: 1

[\[All SY0-701 Questions\]](#)

One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

- A. Virtualization
- B. Firmware Most Voted
- C. Application
- D. Operating system

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  123456789User at May 31, 2024, 1:08 p.m.

Comments

 **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: B

Firmware is the correct answer because a BIOS update addresses vulnerabilities at the firmware level. The BIOS is an essential component of the system's firmware, and updates to it are intended to fix security vulnerabilities, improve compatibility, and enhance overall system stability.
upvoted 4 times

 **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. Firmware
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 98 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 98

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is used to quantitatively measure the criticality of a vulnerability?

A. CVE

B. CVSS Most Voted

C. CIA

D. CERT

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Abcd123321](#) at May 13, 2024, 2:26 a.m.

Comments

✉ [leedsbarber](#) Highly Voted 6 months ago

Answer is B

- A - Common Vulnerabilities & Exposures is a dictionary of known threats.
 - B - Common Vulnerability Scoring System quantifies how critical a vulnerability is.
 - C - Confidentiality, Integrity & Availability is a security concept.
 - D - Computer Emergency Response Team - the title speaks for itself!
- upvoted 7 times

✉ [Abcd123321](#) Highly Voted 6 months, 1 week ago

Selected Answer: B

Common Vulnerability Scoring System (CVSS)

- Used to provide a numerical score reflecting the severity of a vulnerability (0 to 10)
- Scores are used to categorize vulnerabilities as none, low, medium, high, or critical

■ Scores assist in prioritizing remediation efforts but do not account for existing mitigations
upvoted 5 times

✉ **braveheart22** Most Recent ⓘ 1 week, 2 days ago

Selected Answer: B

B is the way to go.
CVSS (Common Vulnerability Scoring System) is the system specifically designed to quantitatively measure the criticality or severity of a vulnerability based on factors such as exploitability and potential impact. It provides a numerical score that helps organizations prioritize vulnerability management efforts.

upvoted 1 times

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: B

CVSS (Common Vulnerability Scoring System) is the correct answer because it is specifically designed to quantitatively measure the criticality of a vulnerability. CVSS provides a standardized scoring mechanism that helps organizations assess the severity and impact of vulnerabilities, allowing for effective prioritization and remediation efforts.

upvoted 3 times

✉ **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. CVSS

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 99 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 99

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- A. Configure all systems to log scheduled tasks.
- B. Collect and monitor all traffic exiting the network.
- C. Block traffic based on known malicious signatures.
- D. Install endpoint management software on all systems

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 6, 2024, 12:39 p.m.

Comments

  [dbrowndiver](#) 2 months ago

Selected Answer: D

Install endpoint management software on all systems is the correct answer because it offers a comprehensive solution for monitoring and managing workstations and servers. Endpoint management software provides visibility into unauthorized changes, detects unapproved software installations, and enforces security policies, making it the most effective choice for ensuring system integrity and compliance.

upvoted 3 times

  [Shaman73](#) 4 months ago

Selected Answer: D

D. Install endpoint management software on all systems

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 100 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 100

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

- A. Data in use
- B. Data in transit Most Voted
- C. Geographic restrictions
- D. Data sovereignty

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 6, 2024, 12:40 p.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: B

Data in transit is the correct answer because a VPN is specifically designed to protect data as it moves between two locations. By encrypting the data and securing the communication path, the VPN ensures that information remains confidential and secure during transmission, making it the most relevant choice for this scenario.

upvoted 4 times

✉ **Zach123654** 4 months ago

Selected Answer: B

GPT!!!

upvoted 1 times

✉ **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. Data in transit

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 101 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 101

Topic #: 1

[\[All SY0-701 Questions\]](#)

After reviewing the following vulnerability scanning report:

```
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
```

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption
```

```
PORT      STATE SERVICE REASON
23/tcp    open  telnet  syn-ack
| telnet encryption:
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

- A. It is a false positive. Most Voted
- B. A rescan is required.
- C. It is considered noise.
- D. Compensating controls exist.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (65%)

D (32%)

3%

by AutoroTink at May 17, 2024, 5:01 a.m.

Comments

mr_reyes Highly Voted 4 months, 2 weeks ago

Selected Answer: A

False Positive:

A false positive occurs when a vulnerability scanner incorrectly identifies a vulnerability that doesn't actually exist. In this case, the initial vulnerability report flagged the use of an insecure network protocol (Telnet) on the server at 192.168.14.6.

However, the follow-up test using Nmap with the telnet-encryption script revealed that the Telnet server supports encryption. Since encryption enhances security, the initial report was incorrect.

Therefore, the conclusion is that the initial report was a false positive.

upvoted 10 times

 **a4e15bd** 2 months, 1 week ago

Telnet itself is inherently insecure and it transmits data including passwords in plaintext making it vulnerable to interception and eavesdropping. While using encryption with telnet is not typical but it is possible, however there are other secure alternatives out there like SSH. So while it is true that Telnet is an unsecure protocol, having encryption is just a compensating control here. So the answer is D.

upvoted 7 times

 **420JhonnySins69** 3 weeks, 5 days ago

Option D is the more reasonable.

Compensating controls. is a secondary/supporting security control that prevents the vulnerability from being exploited. (encryption in this case)

False Positive: believes that there's a vulnerability but when physically checked is not there.
(Telnet is being used, the vulnerability of plain text is there.)

False positive

https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq_UDJgYoQGIW9viwM5hc4C7n&t=6652

Objective (4.3 Explain various activities associated with vulnerability management)

https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq_UDJgYoQGIW9viwM5hc4C7n&t=7199

upvoted 2 times

 **dbrownidiver**  2 months ago

Selected Answer: A

Why This Is a False Positive:

1. Understanding Telnet:

General Security Issues: Telnet typically transmits data in plaintext, making it susceptible to eavesdropping and other security vulnerabilities. This is why it is often flagged in security scans.

2. Encryption Support:

Security Enhancement: The presence of encryption changes the security profile of Telnet. If encryption is supported and properly implemented, the transmission of data is secure, counteracting the usual vulnerabilities associated with Telnet.

3. Initial Assessment:

Misinterpretation: The initial report indicated a vulnerability due to a general assumption that Telnet is insecure, without verifying the specific configuration that includes encryption.

4. Conclusion:

False Positive: Since the Telnet server supports encryption, the assumption of insecurity was incorrect. The vulnerability scanner flagged an issue based on typical characteristics rather than the actual configuration of this specific Telnet implementation.

upvoted 5 times

 **AriGarcia**  3 days ago

A) It's a false positive

Here's why:

The vulnerability report initially flagged the use of an insecure network protocol, Telnet, which by default does not support encryption.

However, the analyst performed an Nmap scan using the telnet-encryption script, which showed that the Telnet server does support encryption. Thus, since encryption is supported, the vulnerability flagged as "insecure" can be considered a false positive because the Telnet server is using secure practices.

upvoted 1 times

 **Ty13** 1 week, 5 days ago

Selected Answer: A

Another garbage question.

It's technically a false positive BECAUSE compensating controls exist.

upvoted 1 times

 **Twpbill** 3 weeks, 5 days ago

Selected Answer: D

It is not a false positive because it correctly identified a vulnerability. However, compensating controls exist to mitigate this vulnerability.

upvoted 1 times

 **Dakshdabas** 1 month, 1 week ago

Selected Answer: B

B. Rescan is required

In pointing out that the nmap scan result shows that the Telnet server "supports encryption," but it does not confirm that encryption is actively being used. It simply indicates that the server has the capability to support encryption, but whether or not it's actually enforced during connections

is another matter.

Given this clarification, the best course of action for the security analyst would likely be
B. A rescan is required.

Explanation:

Since the scan result only shows that the Telnet server supports encryption, but does not confirm that encryption is enforced, a rescan or further testing should be conducted to determine whether:

Encryption is actually being used for all Telnet sessions.

There is a configuration issue where encryption is supported but not enforced.

The rescan should focus on verifying if encryption is mandatory for Telnet connections. If it's not, the vulnerability remains valid and should be addressed.

upvoted 1 times

✉ **nyyankee718** 1 month, 1 week ago

Selected Answer: D

"supports encryption"

upvoted 1 times

✉ **a4e15bd** 1 month, 3 weeks ago

I am going to change my answer to A. False positive, because the initial report flagged Telnet as insecure, but the subsequent test showed that encryption which addresses the vulnerability is being used. This indicates the vulnerability was incorrectly reported. So, that makes it a false positive.

upvoted 1 times

✉ **scoobysnack209** 1 month, 3 weeks ago

The answer is D: Disable port 23 Telnet (unencrypted) and enable SSH port 22 (encrypted connection)

upvoted 1 times

✉ **EfaChux** 2 months ago

Selected Answer: D

Telnet supports encryption but its currently not encrypted, which means there's a vulnerability. Hence there needs to be compensating controls. D is the answer

upvoted 2 times

✉ **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: A

A. It is a false positive.

The initial vulnerability scan reported that the use of Telnet (an insecure network protocol) is a high severity issue. However, the follow-up nmap scan with the `telnet-encryption` script shows that the Telnet server supports encryption. Given that Telnet is typically insecure due to lack of encryption, the presence of encryption support indicates that the reported vulnerability might not be accurate.

Therefore, the security analyst would conclude that the reported vulnerability is a false positive.

upvoted 1 times

✉ **f26ddcd** 4 months, 1 week ago

Selected Answer: A

It is FP

upvoted 1 times

✉ **Boats** 4 months, 1 week ago

Selected Answer: D

Telnet transmits in clear text. In order to keep that from happening you have to have a compensating control. Therefore you encrypt it.

upvoted 3 times

✉ **SHADTECH123** 4 months, 3 weeks ago

Selected Answer: A

Here's the reasoning: The initial vulnerability report indicated a high severity issue due to the use of an insecure network protocol (Telnet). However, the follow-up scan using nmap with the telnet-encryption script showed that the Telnet server supports encryption. This means that while the default perception of Telnet is that it is insecure, the particular Telnet service in question has encryption enabled, mitigating the primary security concern associated with Telnet. Hence, the initial report can be considered a false positive because the Telnet service in question does not suffer from the typical vulnerability of using an insecure protocol.

upvoted 2 times

✉ **SHADTECH123** 4 months, 3 weeks ago

The key difference is:

Option A (It is a false positive): This indicates that the initial report of a high-severity vulnerability due to the use of an insecure protocol is incorrect because the Telnet service actually supports encryption.

Option D (Compensating controls exist): This would imply that while Telnet is inherently insecure, there are other measures in place to secure the communication, which is not the case here because the Telnet service itself is secured with encryption.

Therefore, since the Telnet service supports encryption and the vulnerability no longer exists in the context it was initially reported, the correct conclusion is that it is a false positive, not that compensating controls are mitigating the issue.

upvoted 1 times

✉️ **a4e15bd** 2 months, 1 week ago

Even with the encryption, telnet won't match the security of SSH. Encryption protects data in transit in this case, but what about authentication? Telnet lacks modern authentication mechanisms as SSH. So while telnet in this case is known to be unsecure, encryption is just a compensating control.

upvoted 1 times

✉️ **AutoTink** 4 months, 3 weeks ago

Selected Answer: D

The security analyst used the Nmap command with a specific script to test the Telnet service on a server. Telnet is traditionally known for transmitting data in plaintext, but the result of nmap states that "this time", telnet supports encryption. (hurray!)

Nmap: This is a network scanning tool that can discover devices and services on a computer network.

Nmap results:

PORT 23/tcp: The specific port (23) for TCP is open.

STATE open: The state of the port is open, meaning it is actively accepting connections.

SERVICE telnet: The service running on this port is Telnet.

REASON syn-ack: This indicates that the port is open because the server responded with a SYN-ACK packet during the TCP handshake.

| telnet encryption:: This is the result from the telnet-encryption script.

|_ Telnet server supports encryption: The underscore indicates the result of the script, confirming that the Telnet server supports encryption.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 103 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 103

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A. EAP
- B. DHCP
- C. IPSec Most Voted
- D. NAT

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at June 4, 2024, 7:28 a.m.

Comments

✉ [dbrowndiver](#) Highly Voted 2 months ago

Selected Answer: C

IPSec is ideal for establishing a secure connection between a security consultant's device and a client's network, ensuring confidentiality, integrity, and authenticity of data transmitted over the connection.

upvoted 5 times

✉ [Syl0](#) Most Recent 1 month ago

EAP - Extensible Authentication Protocol - Handles authentication of information

DHCP - Dynamic Host Configuration Protocol - Assign IP address

IPSec - Internet Protocol Security

NAT - Network Address Translation - Used to translate address

upvoted 1 times

✉ [Shaman73](#) 4 months ago

C. IPSec

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 104 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 104

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

- A. Software as a service
- B. Infrastructure as code Most Voted
- C. Internet of Things
- D. Software-defined networking

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 4, 2024, 7:29 a.m.

Comments

✉ [dbrowndiver](#) Highly Voted 2 months ago

Selected Answer: B

Infrastructure as Code (IaC) is the correct answer because it provides the necessary tools and practices for automating and simplifying the deployment of infrastructure resources in a cloud environment. IaC enables efficient and repeatable resource provisioning, making it the most effective solution for the systems administrator's needs.

upvoted 7 times

✉ [1f2b013](#) Most Recent 2 months ago

Selected Answer: B

IaC as it provides a means of automating deployment of infrastructure as a code.

upvoted 3 times

✉ [adderallpm](#) 3 months, 2 weeks ago

Infrastructure as code (IaC) is the ability to provision and support your computing infrastructure using code instead of manual processes and settings. Any application environment requires many infrastructure components like operating systems, database connections, and storage.

upvoted 3 times

 **Shaman73** 4 months ago

B. Infrastructure as code
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 105 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 105

Topic #: 1

[\[All SY0-701 Questions\]](#)

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

- A. Insider threat
- B. Email phishing
- C. Social engineering Most Voted
- D. Executive whaling

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (81%)

D (19%)

by [Shaman73](#) at May 31, 2024, 9:42 a.m.

Comments

✉ [EXAMM3R](#) Highly Voted 3 months, 1 week ago

Executive whaling is when the CFO is one being targeted, therefore the answer is C
upvoted 17 times

✉ [geocis](#) Highly Voted 3 months, 2 weeks ago

Answer is C....Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment.
The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.
upvoted 8 times

✉ [myazureexams](#) Most Recent 2 weeks, 5 days ago

[Selected Answer: C](#)

C- SOCIAL engineering

The user recognized the topic of social engineering from the security awareness training session. Executive whaling, also known as "whaling," is a specific type of social engineering attack where the attacker impersonates a high-ranking executive. In this scenario, the user identified a social engineering attempt, even if they didn't specify executive whaling.

upvoted 1 times

PAWarriors 1 month ago

Selected Answer: C

Correct answer is C.

The scenario described is social engineering. As mentioned by other members, "executive whaling" is a form of spear phishing that targets high-profile individuals, like CEOs or CFOs. In this case a regular "user" is the one that received the call a not a high-profile individual.

upvoted 1 times

Cyber_Texas 1 month ago

Selected Answer: C

It is C because someone is pretending to be someone else that would classify as social engineering

upvoted 1 times

Crucible_Bro 1 month, 3 weeks ago

Selected Answer: C

someone is pretending to be someone within the company with authority. Social engineering.

upvoted 1 times

dbrowndiver 2 months ago

Selected Answer: C

Suspicious caller impersonated someone with authority (CFO) to trick the user into providing credit card information. This is a classic example of social engineering, where the attacker exploits trust and urgency to extract sensitive data. The scenario matches the characteristics of a social engineering attack, as it involves manipulating the victim through a phone call rather than using technological methods or digital communication channels.

upvoted 5 times

Dlove 2 months, 1 week ago

Selected Answer: C

C. Social Engineering

We have to pay attention to the question because they can be very tricky. They didn't specifically target the CFO they simply mentioned the person and said they wanted credit card info. Based on the question that we have the correct answer is C

upvoted 5 times

Bimbo_12 2 months, 2 weeks ago

Selected Answer: C

C. Social engineering

Explanation:

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In this scenario, the suspicious caller was attempting to deceive the user into providing credit card information by falsely claiming to be acting on behalf of the Chief Financial Officer. This tactic is a classic example of social engineering, where the attacker uses social manipulation rather than technical hacking methods to obtain sensitive information.

It is not D because this is a type of phishing attack that specifically targets high-profile executives (also known as "whales") to steal sensitive information. While the scenario does involve the mention of a high-ranking executive, it is broader in scope and fits under the general category of social engineering rather than a specific whaling attack through email.

upvoted 4 times

TheMichael 2 months, 2 weeks ago

Selected Answer: C

How I understand it is Whaling is when they impersonate an executive, executive whaling is when they target an executive (spearfishing in a sense), and social engineering is a broad form of trickery to deceive whoever the target is (not specific) to divulge information.

upvoted 3 times

78fc3e 2 months, 2 weeks ago

Selected Answer: C

In CompTIA's lessons for 701, the only reference I could find for "whaling" is a definition of "targeting employees that have influential roles."

I'm going with C. Social engineering

upvoted 2 times

mnphobby 2 months, 3 weeks ago

C Whaling is send email to the Ceo

upvoted 3 times

b3a128a 2 months, 3 weeks ago

It has to be C because the caller is stating the CFO wants the information, he is not saying he is the CFO.. also the term is whaling, not executive whaling
upvoted 3 times

✉ **101e7ca** 2 months, 3 weeks ago

Selected Answer: C

For the 601 exam Whaling referred to the CEO being hit by a phishing attack...ie email. It targets a high value individual through email. This scenario says that someone called in to impersonate the CFO (high level individual) which is social engineering. There seems to be a term called Executive Phishing but not Executive Whaling.

This could be a CompTIA question where they mix the terms to catch you out. Doesn't help that in the real world we often use these terms interchangeably.

upvoted 3 times

✉ **AbdullahMohammad251** 3 months, 2 weeks ago

Selected Answer: D

Social engineering encompasses a wide variety of techniques and psychological tactics to exploit human vulnerabilities.

- Whaling: This is a type of social engineering attack that targets high-profile individuals by impersonating them to deceive other employees into divulging sensitive information or performing actions that compromise security.

-The scenario described clearly involved the impersonation of a CFO, which makes option D the correct answer.

upvoted 5 times

✉ **johnysmith** 3 months, 2 weeks ago

Selected Answer: D

Executive Whaling

upvoted 1 times

✉ **cdsu** 3 months, 2 weeks ago

C: Social enginerring

This involves impersonation of an executive, it is done via a phone call rather than an email

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 106 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 106

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

- A. Block access to cloud storage websites.
- B. Create a rule to block outgoing email attachments.
- C. Apply classifications to the data. Most Voted
- D. Remove all user permissions from shares on the file server.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (79%)

B (21%)

by [Shaman73](#) at June 4, 2024, 7:30 a.m.

Comments

✉ [dbrowndiver](#) Highly Voted 2 months ago

Selected Answer: C

Apply classifications to the data is the correct first step because it establishes a foundational understanding of what data is sensitive and needs protection. By classifying the data, the security administrator can ensure that subsequent DLP policies are effectively tailored to prevent the exfiltration of sensitive customer data, while minimizing unnecessary restrictions on non-sensitive data.

upvoted 6 times

✉ [Laura5859](#) Most Recent 3 weeks, 1 day ago

Selected Answer: C

You must apply classifications to the data, so the DLP will be able to identify sensitive data.

upvoted 1 times

✉ [nyyankee718](#) 2 months, 2 weeks ago

Selected Answer: C

its asking what to do FIRST/ How would users know what not to send out if data is not classified

upvoted 2 times

 **ccamarada** 2 months, 3 weeks ago

Selected Answer: C

first classify the information

upvoted 2 times

 **101e7ca** 2 months, 3 weeks ago

Selected Answer: B

Applying a DLP solution to prevent data being 'leaked' out of the company, usually through email, USB or tools like Steganography.

Once installed the first thing he should do is create a rule to either warn or block email attachments. It's nothing to do with cloud storage or server file permissions and we don't need data classification for DLP to work (although it might be a nice option).

upvoted 3 times

 **Justhereforcomptia** 1 month, 2 weeks ago

So you're gonna block all the end-users from sending attachments ? are you serious...

What should be done, is classify the files you have first then block the sensitive ones from being sent as attachments. Blocking everything doesn't make any sense in the context of this question.

Correct Answer is C

upvoted 2 times

 **adderallpm** 3 months, 2 weeks ago

DLP (Data Loss Prevention)

upvoted 3 times

 **Shaman73** 4 months ago

C. Apply classifications to the data.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 107 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 107

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

A. Compromise

B. Retention Most Voted

C. Analysis

D. Transfer

E. Inventory

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 4, 2024, 7:31 a.m.

Comments

✉ **edf622f** 2 weeks, 2 days ago

Sarbanes-Oxley Act. The answer is B.
upvoted 1 times

✉ **1f2b013** 2 months ago

Selected Answer: B
Retention
upvoted 1 times

✉ **dbrownidiver** 2 months ago

Selected Answer: B
The administrator is tasked with ensuring that transaction data is archived for the appropriate duration. This task involves adhering to retention schedules that dictate how long such data must be kept to meet compliance obligations.

Retention policies are critical for legal and compliance teams, as they help avoid legal issues related to data disposal and ensure that records are available for audits, investigations, or regulatory reviews.

upvoted 4 times

 **Shaman73** 4 months ago

B. Retention

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 108 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 108

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is working with a vendor to perform a penetration test. Which of the following includes an estimate about the number of hours required to complete the engagement?

A. SOW Most Voted

B. BPA

C. SLA

D. NDA

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by MAKOhunter33333333 at May 21, 2024, 9:25 p.m.

Comments

✉ MAKOhunter33333333 Highly Voted 6 months ago

Selected Answer: A

SOW: statement of work

BPA: business partnership agreement

SLA: service level agreement

NDA: no disclosure agreement

upvoted 8 times

✉ dbrowndiver Most Recent 3 months, 2 weeks ago

Selected Answer: A

In the context of a penetration test, the SOW would include an estimate of the number of hours required to conduct the test, along with detailed descriptions of the testing methodologies, deliverables, and any other project-related expectations.

upvoted 3 times

✉ Boethius 5 months, 2 weeks ago

A: SOW (statement of work)

The WO (Work Order) or SOW (Statement of Work) contain the details of a project and references the general terms in the MSA (Master Services Agreement). ~ Security + Get Certified Get Ahead by Darril Gibson and Joe Shelley

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 109 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 109

Topic #: 1

[\[All SY0-701 Questions\]](#)

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

- A. Insider threat
- B. Hacktivist
- C. Nation-state
- D. Organized crime Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  MAKOhunter33333333 at May 21, 2024, 9:27 p.m.

Comments

 **MAKOhunter33333333** Highly Voted 6 months ago

Selected Answer: D

Ransomware is blackmailing for monetary gain which is a CRIME. It also does not fit the criteria for any other threat actor listed.
upvoted 10 times

 **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: D

Organized crime is the correct answer because ransomware-as-a-service operations are primarily conducted by criminal organizations seeking to monetize cyberattacks. These groups offer ransomware tools and services to other criminals, reflecting the profit-driven, organized nature of these cybercrime enterprises.
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 110 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 110

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at June 4, 2024, 7:33 a.m.

Comments

✉ [geocis](#) Highly Voted 5 months ago

Correct Answer: D

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

upvoted 10 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: D

Peer reviews help catch malicious code before it is integrated into the production environment by having multiple sets of eyes on the changes, reducing the chance of any one developer slipping harmful code through the process.

upvoted 2 times

✉ [Shaman73](#) 5 months, 2 weeks ago

D. Peer review and approval

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 111 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 111

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 4, 2024, 7:34 a.m.

Comments

  [\[Removed\]](#) Highly Voted 5 months, 2 weeks ago

Correct answer is option: D
upvoted 19 times

  [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: D

By using an application allow list, employees cannot inadvertently install or run unauthorized software, including malware, because only approved applications are permitted to execute. This approach minimizes the risk of malware introduction through accidental downloads or installations.
upvoted 2 times

  [Shaman73](#) 5 months, 2 weeks ago

D. Application allow list
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 112 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 112

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking Most Voted
- D. Side loading

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by MAKOhunter33333333 at May 21, 2024, 9:30 p.m.

Comments

✉ **leedsbarber** Highly Voted 4 months ago

Selected Answer: C

My first thought was:

D - because jailbreaking only relates to iOS and rooting is Android. They didn't specify a device.

However...

The question relates to modifying the OS, not installing unofficial apps.

So, although no OS is specified, answer C does seem most logical.

It pays to take a little more time to dissect the wording of the question as much as possible.
upvoted 6 times

✉ **MAKOhunter33333333** Highly Voted 4 months, 2 weeks ago

Selected Answer: C

Jailbreaking is modding iOS and rooting is modding Android.
upvoted 5 times

 **ExamTopics701** (Most Recent) 2 weeks, 3 days ago

It can't be A or B.
upvoted 1 times

 **Laura5859** 3 weeks, 2 days ago

Selected Answer: C

Jailbreaking is defined by CompTIA as gaining full access to the iOS device by removing the limitations imposed by the Apple iOS operating system.
upvoted 1 times

 **dbrownidiver** 2 months ago

Selected Answer: C

Jailbreaking is the correct answer because it specifically involves modifying the operating system on mobile devices, which the company's Acceptable Use Policy aims to prohibit. By addressing jailbreaking, the company seeks to maintain the security and integrity of its mobile devices, preventing vulnerabilities associated with unauthorized OS modifications.
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 113 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 113

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Choose two.)

- A. Fencing
- B. Video surveillance
- C. Badge access Most Voted
- D. Access control vestibule Most Voted
- E. Sign-in sheet
- F. Sensor

[Hide Answer](#)

Suggested Answer: CD

Community vote distribution

CD (67%)

AC (33%)

by [Shaman73](#) at June 4, 2024, 7:35 a.m.

Comments

✉ [Shaman73](#) Highly Voted 4 months ago

- C. Badge access
 - D. Access control vestibule
- upvoted 7 times

✉ [koala_lay](#) Most Recent 3 weeks, 2 days ago

Selected Answer: CD

Agree to answer C & D
upvoted 1 times

✉ [Laura5859](#) 3 weeks, 2 days ago

Selected Answer: AC

The question asks how you can secure a facility. I feel like that refers to the entire campus, which would require physical barriers such as a fence and secure access to buildings. Secure building access can be accomplished with Badge Access.

upvoted 1 times

 **jsmthy** 1 week, 4 days ago

Fencing of this type is not in the sense of physical chain-link/picket fences, but the appliances to keep intruders out like firewalls and IPS.

upvoted 1 times

 **chasingsummer** 1 month, 1 week ago

Selected Answer: CD

C. Badge access and D. Access control vestibule.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 114 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 114

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

- A. Segmentation Most Voted
- B. Isolation
- C. Patching
- D. Encryption

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (89%) 11%

by [3056f7e](#) at May 10, 2024, 2:46 a.m.

Comments

✉ **MAKOhunter33333333** Highly Voted 6 months ago

Selected Answer: A

Mentions the org wants to store it on the network just separate from the main network, which is segmentation.
upvoted 6 times

✉ **MAKOhunter33333333** 6 months ago

CompTIA SY0-701 pg 13 states isolation cuts a system off from access to or from outside networks.

Segmentation places sensitive systems on separate networks where they MAY communicate with each other.
upvoted 3 times

✉ **famuza77** Most Recent 1 month ago

Selected Answer: B

it is Isolation
upvoted 1 times

 **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: A

Segmentation is the correct answer because it involves creating distinct network segments that control access and separate sensitive customer data from the main corporate network. Network segmentation is the most appropriate solution for ensuring that customer data is stored securely and not accessible to unauthorized users.

upvoted 2 times

 **drosas84** 5 months, 1 week ago

Selected Answer: A

Network segmentation involves dividing a network into subnets to control access and traffic flow. Network isolation is more severe, creating a standalone network with no connectivity to other parts of the network. It's a stringent form of segregation.

upvoted 4 times

 **hasquaati** 6 months ago

Selected Answer: A

Answer is A. While Isolation is a legitimate answer, that design is more relevant to machinery and manufacturing equipment.

upvoted 2 times

 **AutoroTink** 6 months, 1 week ago

Further notes: Isolation is a security measure that can be used to protect sensitive data which typically involves creating a completely separate environment, such as a different physical server or a standalone network, which can be more restrictive than segmentation. The question has the data still on the network, just in a separate part. So, Option A is still the best answer.

upvoted 3 times

 **AutoroTink** 6 months, 1 week ago

Selected Answer: A

While isolation is a broader concept that can include segmentation, it typically refers to completely separating a system or environment from others, which might be more extreme than necessary for this purpose. Segmentation can help in isolating the customer data from the main corporate network, ensuring that it is not accessible to unauthorized users

upvoted 1 times

 **Yoez** 6 months, 1 week ago

Selected Answer: B

The correct answer is:

B. Isolation

Isolation involves creating separate network segments or zones that restrict access between them. By isolating the network segment where customer data is stored from the main corporate network, the organization can prevent unauthorized users on the corporate network from accessing the sensitive customer data. This helps enhance security by limiting the potential attack surface and reducing the risk of unauthorized access or data breaches.

upvoted 1 times

 **shady23** 6 months, 1 week ago

Selected Answer: A

A. Segmentation

upvoted 1 times

 **3056f7e** 6 months, 1 week ago

B cause A only involves dividing a network into smaller segments to improve security and performance but may still allow communication between segments.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 115 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 115

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the most common data loss path for an air-gapped network?

- A. Bastion host
- B. Unsecured Bluetooth
- C. Unpatched OS
- D. Removable devices Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Yoez](#) at May 11, 2024, 7:04 p.m.

Comments

  [Yoez](#) Highly Voted  6 months, 1 week ago

Selected Answer: D

In an air-gapped network, which is physically isolated from other networks, the most common data loss path would typically be through removable devices (option D). These can include USB drives, external hard drives, or other storage devices that could be introduced into the network, intentionally or unintentionally, by users or external entities. This is because such devices can bypass the physical isolation of the air gap and introduce potential security vulnerabilities.

upvoted 5 times

  [dbrowndiver](#) Most Recent  3 months, 2 weeks ago

Selected Answer: D

Removable devices is the correct answer because they provide a direct, physical means to transfer data to and from an air-gapped network, making them the most common path for data loss. Removable devices circumvent the network's isolation by physically connecting it to other systems, posing a significant risk of data exfiltration.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 116 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 116

Topic #: 1

[\[All SY0-701 Questions\]](#)

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

- A. Impersonation
- B. Disinformation
- C. Watering-hole Most Voted
- D. Smishing

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at June 4, 2024, 7:36 a.m.

Comments

✉ **chasingsummer** 1 month, 1 week ago

Selected Answer: C

The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.
upvoted 1 times

✉ **dbrowndiver** 2 months ago

Selected Answer: C

Watering-hole is the correct answer because it describes the method used by the attacker to compromise a legitimate website frequented by the target group (in this case, the industry blog) and spread malware to visitors. This strategic targeting and delivery mechanism is characteristic of a watering-hole attack.

upvoted 2 times

✉ **4ddc874** 2 months, 1 week ago

Selected Answer: C

A watering-hole attack targets a specific group of people by compromising a website they frequently visit. In this case, the compromised industry blog acted as the "watering hole" for the employees
upvoted 2 times

 **Shaman73** 4 months ago

- C. Watering-hole
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 117 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 117

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

- A. Deploying a SASE solution to remote employees Most Voted
- B. Building a load-balanced VPN solution with redundant internet
- C. Purchasing a low-cost SD-WAN solution for VPN traffic
- D. Using a cloud provider to create additional VPN concentrators

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by 123456789User at May 23, 2024, 10:43 a.m.

Comments

✉ **geocis** Highly Voted 3 months, 3 weeks ago

Answer is A.....SASE (Secure Access Service Edge) is a comprehensive networking and security approach that combines wide-area networking (WAN) capabilities with security features. It provides secure access to applications and data, including encrypted tunnel access to the data center, while also offering monitoring capabilities for remote employee internet traffic. By implementing a SASE solution, the organization can reduce traffic on the VPN and internet circuit by routing traffic intelligently through the cloud, closer to the users. This approach helps optimize performance and security, addressing the scaling issues effectively.

upvoted 7 times

✉ **a4e15bd** Most Recent 1 month, 3 weeks ago

The correct answer is A. Deploying SASE Solution..
Secure Access Service Edge (SASE) is a network architecture framework that combines cloud-based security technologies with wide area network capabilities. The goal of SASE is to securely connect users, systems, and endpoints to applications and services anywhere

upvoted 1 times

✉ **dbrowndiver** 2 months ago

Selected Answer: A

Deploying a SASE solution to remote employees is the best choice because it provides a holistic approach to secure remote access by reducing traffic, offering encrypted tunnel access, and monitoring internet traffic. SASE integrates necessary networking and security functions into a cloud-based solution, making it ideal for modern remote work environments.

upvoted 4 times

 **123456789User** 4 months, 2 weeks ago

Selected Answer: A

Deploying a SASE solution to remote employees.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 118 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 118

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement Most Voted
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 7:37 a.m.

Comments

✉ **Glacier88** 1 month, 2 weeks ago

Selected Answer: A

Financial services are heavily regulated.
upvoted 1 times

✉ **Shaman73** 4 months ago

• A. Regulatory requirement
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 119 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 119

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A. Integrity
- B. Availability
- C. Confidentiality** (Most Voted)
- D. Non-repudiation

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Shaman73](#) at May 31, 2024, 9:44 a.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: C

Human resources (HR) data typically includes sensitive information such as employee records, personal data, salaries, and other confidential details. Implementing the principle of least privilege ensures that only authorized HR personnel have access to this sensitive information, maintaining its confidentiality.

Access Control: By granting access only to those who require it to perform their job functions, the organization minimizes the risk of unauthorized access, data breaches, and information leaks.

The primary goal of applying least privilege to HR files is to protect sensitive data from unauthorized access, aligning directly with the confidentiality aspect of information security.

upvoted 3 times

  [Shaman73](#) 5 months, 3 weeks ago

C. Confidentiality

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 120 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 120

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Choose two.)

- A. The device has been moved from a production environment to a test environment.
- B. The device is configured to use cleartext passwords.
- C. The device is moved to an isolated segment on the enterprise network.
- D. The device is moved to a different location in the enterprise.
- E. The device's encryption level cannot meet organizational standards. Most Voted
- F. The device is unable to receive authorized updates. Most Voted

[Hide Answer](#)

Suggested Answer: EF

Community vote distribution

EF (86%)

14%

by [Shaman73](#) at June 4, 2024, 7:39 a.m.

Comments

✉ [Jamie888](#) 3 weeks ago

Selected Answer: BE

Practice test in pluralsight say its B and E
upvoted 1 times

✉ [dbrowndiver](#) 2 months ago

Selected Answer: EF

When evaluating whether a network device should be decommissioned, security vulnerabilities, compliance with organizational standards, and the ability to maintain the device are critical considerations. Options E and F highlight situations where a device is not able to meet these essential requirements.

E. The device's encryption level cannot meet organizational standards and F. The device is unable to receive authorized updates are the correct reasons for recommending the decommissioning of a network device. These conditions indicate significant security and compliance risks that cannot be addressed through reconfiguration alone, necessitating the removal of the device to protect the organization's network and data.

upvoted 2 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: EF

- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

These two cases justify decommissioning a network device:

- Encryption Level: If a device's encryption level cannot meet the organization's standards, it poses a significant security risk and should be decommissioned.
- Authorized Updates: If a device is unable to receive authorized updates, it becomes vulnerable to known exploits and cannot be maintained securely, thus it should also be decommissioned.

Therefore, the correct answers are:

- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

upvoted 4 times

 **Shaman73** 4 months ago

- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 121 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 121

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is required to perform a risk assessment on an annual basis. Which of the following types of risk assessments does this requirement describe?

- A. Continuous
- B. Ad hoc
- C. Recurring** Most Voted
- D. One time

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [Shaman73](#) at June 4, 2024, 7:40 a.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: C

Recurring risk assessments are those that are scheduled to take place at regular intervals, such as annually, semi-annually, or quarterly. This type of assessment ensures that risks are regularly evaluated, allowing the company to stay informed about potential vulnerabilities and threats and adjust its risk management strategies accordingly. o Without the ability to receive updates, a device cannot be secured against emerging threats, making it a liability to the organization's security posture.

upvoted 2 times

  [Shaman73](#) 5 months, 2 weeks ago

- C. Recurring

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 122 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 122

Topic #: 1

[\[All SY0-701 Questions\]](#)

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

A. Compensating

B. Detective Most Voted

C. Preventive

D. Corrective

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 4, 2024, 7:40 a.m.

Comments

✉ **opeyemi777** 4 weeks, 1 day ago

Selected Answer: B

Detective

upvoted 1 times

✉ **dbrowndiver** 2 months ago

Selected Answer: B

Detective is the correct answer because reviewing log files after a ransomware attack is an example of a detective control. It is used to identify, analyze, and understand security incidents post-occurrence, providing valuable information for future prevention and response strategies.

upvoted 2 times

✉ **Ina22** 2 months, 2 weeks ago

Its B : Detective

upvoted 1 times

 **Shaman73** 4 months ago

- B. Detective
- upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 123 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 123

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following exercises should an organization use to improve its incident response process?

A. Tabletop Most Voted

B. Replication

C. Failover

D. Recovery

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 7:41 a.m.

Comments

✉️ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: A

Tabletop is the correct answer because tabletop exercises are specifically designed to evaluate and improve incident response processes by allowing teams to simulate responses to hypothetical incidents. This exercise provides valuable insights into the effectiveness of the current response plan and identifies areas for improvement, enhancing the organization's overall incident response capabilities.

upvoted 3 times

✉️ **Shaman73** 5 months, 2 weeks ago

- A. Tabletop

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 124 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 124

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?

- A. Generators and UPS
- B. Off-site replication Most Voted
- C. Redundant cold sites
- D. High availability networking

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 4, 2024, 7:42 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: B

Earthquake Protection: In earthquake-prone areas, having data and systems replicated off-site ensures that even if the primary site is compromised, the organization can recover its operations from the remote location with minimal downtime and data loss.

Data and System Availability: Off-site replication provides a means to restore operations quickly, as the backup data is up-to-date and can be accessed or moved to a disaster recovery site.

Off-site replication is crucial for disaster recovery planning, particularly in areas susceptible to natural disasters. It ensures business continuity by safeguarding data and systems in a secure location away from the primary site's risks.

upvoted 3 times

✉ **cdsu** 5 months ago

Answer B:

Copying data to a geographically distant location. This ensures that data is preserved even if the primary site is compromised by an earthquake

upvoted 3 times

✉ **Shaman73** 5 months, 2 weeks ago

- B. Off-site replication
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 125 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 125

Topic #: 1

[\[All SY0-701 Questions\]](#)

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation Most Voted
- D. Replacement

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (96%) 4%

by Yoez at May 11, 2024, 7:27 p.m.

Comments

✉ KrazyMonkey Highly Voted 4 months, 3 weeks ago

Selected Answer: C

I've not heard of patching legacy devices... Professor Messer would be disappointed.
upvoted 17 times

✉ CyberSecurity24 Highly Voted 4 months ago

Selected Answer: C

Patching is a common method for addressing vulnerabilities. However, in the case of legacy devices, patches may no longer be provided, or applying new patches may be difficult. Therefore, it is not suitable as a quick mitigation method, making C. Segmentation the correct answer.
upvoted 9 times

✉ dbrowndiver Most Recent 2 months ago

Selected Answer: C

Legacy IoT Devices: These devices often lack the ability to be quickly patched or replaced due to hardware limitations or operational constraints. Segmentation offers a rapid response by limiting access and isolating these devices from critical network resources.

Access Control: By segmenting the network, you can apply stricter access controls and monitoring, ensuring that any potential compromise of the IoT devices does not affect the broader network.

upvoted 3 times

SHADTECH123 4 months, 3 weeks ago

Selected Answer: C

Segmentation would best mitigate the network access vulnerability in the OS of legacy IoT devices quickly. By segmenting the network, you can isolate the vulnerable devices from the rest of the network, thereby limiting potential access and reducing the risk of exploitation. This is often faster than patching or replacing the devices, especially if patches are not immediately available or replacement is not feasible in the short term.

upvoted 6 times

AutoroTink 4 months, 3 weeks ago

Selected Answer: C

I retract my previous answer. You can't do patching on legacy stuff...MY BAD!

upvoted 4 times

hasquaati 4 months, 3 weeks ago

Selected Answer: C

Key word is legacy device. Patches may not be available. Segmentation will also be a valid solution for legacy IoT devices. Answer is C.

upvoted 3 times

e5c1bb5 4 months, 3 weeks ago

Selected Answer: C

theres always trolls/mislead people. legacy devices arent supported anymore. segmentation is the way to go. theres always vulnerabilities in IOT devices. what do you do if you need to use them? SEGMENTATION.

upvoted 3 times

shady23 4 months, 3 weeks ago

Selected Answer: C

Question #: 729

Topic #: 1

[All SY0-601 Questions]

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

Patching doesn't work as it's legacy, Segregation is the quickest option of the remaining three.

upvoted 3 times

AutoroTink 4 months, 3 weeks ago

Selected Answer: B

Network segmentation could limit the potential impact of the vulnerability but does not address the vulnerability in the devices.

upvoted 1 times

Justhereforcomptia 1 month, 2 weeks ago

Legacy OS doesn't receive patches, so your answer is invalid.

upvoted 1 times

nesquick0 1 month, 4 weeks ago

its a legacy OS which it cannot recieve updates or be patched.

upvoted 1 times

Yoez 4 months, 4 weeks ago

Selected Answer: B

The option that would best mitigate the vulnerability quickly is patching (option B). Patching involves applying updates or fixes provided by the software vendor to address known vulnerabilities or weaknesses in the system. By promptly patching the OS of the legacy IoT devices, the vulnerability can be mitigated, reducing the risk of exploitation by malicious actors. This is typically the quickest and most direct way to address known vulnerabilities and enhance the security posture of the devices.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 126 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 126

Topic #: 1

[\[All SY0-701 Questions\]](#)

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

- A. Group Policy
- B. Content filtering
- C. Data loss prevention
- D. Access control lists Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by SHADTECH123 at May 18, 2024, 11:20 a.m.

Comments

✉ SHADTECH123 Highly Voted 6 months ago

Selected Answer: D

Access control lists (ACLs) should be used to restrict access to the data quickly. ACLs allow the administrator to specify which users or groups have permission to access certain files or directories on the file server, providing a straightforward and immediate way to enforce access controls and protect confidential data.

upvoted 9 times

✉ Nilab Most Recent 3 weeks, 5 days ago

Why can't be group policy?

upvoted 1 times

✉ 3dk1 3 weeks, 3 days ago

Because group policy applies to broader system policies (on workstations and servers), but does not directly manage file access permissions.

upvoted 1 times

 **dbrowndiver** 3 months, 2 weeks ago**Selected Answer: D**

In this scenario, D. Access control lists (ACLs) is the best choice because it provides a quick and precise way to adjust file permissions and restrict access to confidential data on a file server. ACLs allow administrators to implement immediate changes and ensure only authorized users have access to sensitive files.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

EXAM SY0-701 TOPIC 1 QUESTION 127 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 127

Topic #: 1

[\[All SY0-701 Questions\]](#)

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at June 4, 2024, 7:44 a.m.

Comments

Syl0 1 month ago

MOA - memorandum of Agreement
MOU - Memorandum of Understanding
SOW - Statement / Scope of Work
SLA - Service Level Agreement
upvoted 1 times

dbrowndiver 2 months ago

Selected Answer: D

In this scenario, the client demands 99.99% uptime for hosted security services. The SLA is the appropriate document to specify this uptime requirement and any associated metrics.

upvoted 1 times

Dean1065 3 months, 3 weeks ago

Selected Answer: D

D - SLA

upvoted 1 times

 **Shaman73** 4 months ago

• D. SLA

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 128 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 128

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

A. Certification Most Voted

B. Inventory list

C. Classification

D. Proof of ownership

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  MAKOhunter33333333 at May 22, 2024, 1:17 a.m.

Comments

 **MAKOhunter33333333** Highly Voted 6 months ago

Selected Answer: A

Third-party certificate of destruction, proof it was actually disposed
upvoted 10 times

 **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: A

For a classified storage array, certification is critical to ensure that sensitive data has been irretrievably destroyed, preventing unauthorized access or data breaches.

The certification serves as evidence that the company complied with legal and regulatory requirements regarding the handling and disposal of classified materials. This can be important for audits or investigations.

Certification provides assurance and documentation that the storage array was disposed of securely, mitigating risks associated with the handling of classified information.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 129 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 129

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

- A. Geographic dispersion
- B. Platform diversity
- C. Hot site
- D. Load balancing

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 7:46 a.m.

Comments

[geocis](#) Highly Voted 5 months ago

Answer: A

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity

upvoted 6 times

[3dk1](#) Most Recent 3 weeks, 3 days ago

Selected Answer: A

this one easy

upvoted 1 times

[dbrownidiver](#) 3 months, 2 weeks ago

Natural Disaster Protection: By storing backup data in geographically dispersed locations, the company ensures that a natural disaster in one region does not affect the backup data in another region.

Regulatory Compliance: Many regulations require companies to have disaster recovery strategies that protect data integrity and availability, which geographic dispersion effectively addresses. Geographic dispersion directly addresses the risk of complete data loss due to a natural disaster by ensuring that data is stored in multiple locations, making it the most appropriate solution for this scenario

upvoted 2 times

 **Shaman73** 5 months, 2 weeks ago

- A. Geographic dispersion

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 130 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 130

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.
- C. Check endpoint logs.
- D. Query the file's metadata.

[Most Voted](#)

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at May 31, 2024, 9:45 a.m.

Comments

✉ [geocis](#) Highly Voted 5 months ago

Answer D.....Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis.

upvoted 5 times

✉ [Shaman73](#) Highly Voted 5 months, 3 weeks ago

D. Query the file's metadata.
upvoted 5 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: D

In this scenario, choice "D" is correct. Query the file's metadata is the correct answer because metadata provides direct information about the file's creation date and possibly the creator. This method is the most efficient and effective way to gather the required details about a potentially malicious video file. By querying the file's metadata, the security analyst can access information about when the file was created and potentially who created it, assuming the creator's details were embedded or tagged during the file's creation.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 131 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 131

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

- A. Red
- B. Blue
- C. Purple Most Voted
- D. Yellow

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [123456789User](#) at May 23, 2024, 10:58 a.m.

Comments

✉ [123456789User](#) Highly Voted 5 months, 4 weeks ago

Selected Answer: C

Red = offensive
Blue = defensive
Yellow = builders
Purple = mix of offensive and defensive. Also the color you get when you mix red and blue.
upvoted 20 times

✉ [adderallpm](#) Highly Voted 5 months, 1 week ago

Grimace
upvoted 8 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: C

Purple teams combine the strengths of both offensive and defensive approaches to provide a holistic security strategy. This integration enhances the organization's ability to identify weaknesses, improve response capabilities, and implement effective security measures.

upvoted 1 times

 **Dlove** 4 months ago

Selected Answer: C

C. Purple

Purple teaming is a collaborative approach to cybersecurity that brings together red and blue teams to test and improve an organization's security posture.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 132 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 132

Topic #: 1

[\[All SY0-701 Questions\]](#)

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

- A. Patch availability Most Voted
- B. Product software compatibility
- C. Ease of recovery
- D. Cost of replacement

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by SHADTECH123 at May 18, 2024, 11:24 a.m.

Comments

✉ SHADTECH123 Highly Voted 6 months ago

Selected Answer: A

The most likely security implication that the security team would document is patch availability. End-of-life operating systems no longer receive security updates or patches from the vendor, which leaves them vulnerable to newly discovered exploits and vulnerabilities. This lack of ongoing support means that any security flaws found in the operating systems will not be addressed, increasing the risk of compromise.
upvoted 5 times

✉ dbrowndiver Most Recent 3 months, 2 weeks ago

Selected Answer: A

Patch availability is a critical concern for maintaining the security and integrity of systems. The absence of patches for EOL systems is a major security risk that the security team would likely document as a primary concern
upvoted 1 times

✉ Etc_Shadow28000 5 months, 1 week ago

Selected Answer: A

A. Patch availability

The primary security implication of using end-of-life operating systems is the lack of patch availability. End-of-life systems no longer receive security updates or patches from the vendor, making them vulnerable to known exploits and security vulnerabilities that will not be fixed. This poses a significant risk to the security of the kiosks and the overall network.

Therefore, the correct answer is:

A. Patch availability

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 133 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 133

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

- A. A full inventory of all hardware and software Most Voted
- B. Documentation of system classifications
- C. A list of system owners and their departments
- D. Third-party risk assessment documentation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  MAKOhunter33333333 at May 22, 2024, 1:21 a.m.

Comments

 **MAKOhunter33333333** Highly Voted 6 months ago

Selected Answer: A

Conducting inventory is part of risk management, so knowing what is in your environment will be very helpful to track and patch
upvoted 11 times

 **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: A

In this scenario, the best answer is "A". A full inventory of all hardware and software is the correct answer because it provides the essential information needed to accurately assess the risk posed by a new vulnerability. This inventory enables the security analyst to identify affected systems, prioritize responses, and measure the overall risk to the organization effectively.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 134 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 134

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime Most Voted
- C. Backout plan
- D. Change management boards

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  MAKOhunter33333333 at May 22, 2024, 1:27 a.m.

Comments

 **MAKOhunter33333333** Highly Voted 6 months ago

Selected Answer: B

Set time aside for IT to make changes, like a maintenance window, typically not during peak hours
upvoted 7 times

 **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: B

In this scenario, the best choice is "B". Scheduled downtime is the correct answer because it specifically involves setting a designated time for changes to occur, balancing the need for system maintenance with minimizing business impacts. Scheduled downtime ensures that updates and changes are performed in a controlled and predictable manner, reducing the risk of unplanned disruptions.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 136 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 136

Topic #: 1

[\[All SY0-701 Questions\]](#)

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

- A. End of business
- B. End of testing
- C. End of support Most Voted
- D. End of life

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (67%)

D (33%)

by [Shaman73](#) at June 4, 2024, 7:50 a.m.

Comments

✉ **Shaman73** Highly Voted 4 months ago

- D. End of life
upvoted 11 times

✉ **MYC199** Highly Voted 2 months, 2 weeks ago

Selected Answer: C

C. From the CompTIA study guide: End of life - while the equipment or device is no longer sold, it remains supported. End of support - the last date on which the vendor will provide support and/or updates.

I'm confused.
upvoted 5 times

✉ **nap61** Most Recent 2 days, 22 hours ago

Selected Answer: D

Extracted from The Official CompTIA Security+ Student Guide (Exam SY0-701), Lesson 8, Topic 8A, page 212-213
"The manufacturer or vendor no longer supports EOL systems, so they do not receive updates, including critical security patches."

" An EOL system is a specific product or version of a product that the manufacturer or vendor has publicly declared as no longer supported."
"End-of-life (EOL) hardware vulnerabilities arise when manufacturers cease providing product updates, parts, or patches to the firmware."
also no mention of "end of support (EOS)"
upvoted 1 times

✉ User92 3 days, 19 hours ago

Selected Answer: C

End of Life (EOL): This is when a product (like a device, software, or service) is no longer sold or produced by the manufacturer.

End of Support (EOS): This happens when the manufacturer or service provider officially stops providing support for the product.
upvoted 1 times

✉ Rock2roll02 1 week, 3 days ago

Answer is D

End of Life (EOL), which usually includes end of production and distribution, while EOS specifically refers to the halt in support services and updates from the vendor.

upvoted 1 times

✉ TonyStarChillingFromHeaven 1 week, 5 days ago

End of life (EOL): This is the date after which a product will no longer be sold or renewed. However, it might still receive some form of support, such as security patches. End of support (EOS): This date marks the complete cessation of all support services for the product.

upvoted 1 times

✉ a0bfa81 2 weeks, 3 days ago

Selected Answer: D

Answer D. End of life

upvoted 1 times

✉ bufffalobilll 2 weeks, 5 days ago

Selected Answer: C

specifically around updates, EOS is correct

upvoted 1 times

✉ Laura5859 2 weeks, 6 days ago

Selected Answer: D

CompTIA defines End of Life as the manufacturer no longer supporting these devices, which includes no longer providing updates or critical security patches.

upvoted 2 times

✉ Hayder81 3 weeks, 6 days ago

D. End of life

upvoted 2 times

✉ Syl0 1 month ago

Selected Answer: D

End of Life... because it is being decommissioned.

upvoted 2 times

✉ a4e15bd 1 month, 2 weeks ago

D. End of Life

Here is why:

End of support refers to when the manufacturer stops providing updates, patches and technical support for a product, but the product may still be used and it won't receive any further assistance or updates.

End of Life: Refers to a stage where the product is no longer sold, maintained or supported by the manufacturer. This device is typically decommissioned or retired.

End of support would only apply if the device was still in use but not longer receiving updates, in our scenario where decommissioning is involved, End of Life is the right answer.

upvoted 4 times

✉ nesquick0 1 month, 3 weeks ago

Selected Answer: C

I'll go with C (End of support)

upvoted 1 times

✉ nesquick0 1 month, 3 weeks ago

Selected Answer: C

End of Support (discontinued), while End of life may receive critical patches.
So C (End of Support) is correct.

upvoted 1 times

 **idy** 2 months, 1 week ago

End of life (EOL): This is the date after which a product will no longer be sold or renewed. However, it might still receive some form of support, such as security patches. End of support (EOS): This date marks the complete cessation of all support services for the product.

Answer is C

upvoted 3 times

 **j777** 2 months, 1 week ago

I believe it's going to be D: When a device or software reaches EOL, it means that it is no longer supported by the manufacturer, which includes no longer receiving updates, patches, or any other form of support.

upvoted 1 times

 **xekiva3329** 2 months, 2 weeks ago

Selected Answer: C

Answer: C

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 137 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 137

Topic #: 1

[\[All SY0-701 Questions\]](#)

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

A. Encryption at rest Most Voted

B. Masking

C. Data classification

D. Permission restrictions

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Shaman73](#) at May 31, 2024, 9:46 a.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: A

When a laptop is stolen, encryption at rest ensures that the data remains secure and inaccessible to the thief, as they would need the decryption key to access the files.

Data Protection: Encryption at rest provides a robust layer of security for sensitive data, making it a common requirement for organizations handling confidential information.

The primary concern with stolen laptops is unauthorized access to the data stored on them. Encryption at rest is the most effective way to prevent data loss in this scenario, as it keeps the data secure even if the device falls into the wrong hands.

upvoted 4 times

  [Shaman73](#) 5 months, 3 weeks ago

A. Encryption at rest

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 138 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 138

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by MAKOhunter33333333 at May 22, 2024, 3:23 a.m.

Comments

✉ 499c5c4 Highly Voted 5 months, 3 weeks ago

A reflected denial of service (DoS) attack occurs when an attacker sends forged requests to a server, causing the server to respond to the spoofed IP address (the target) with a large volume of traffic. In the context of DNS, this often involves DNS amplification attacks, where small DNS queries result in large responses being sent to the target. This matches the described symptoms of minimal resource usage on the DNS server but a flood of inbound traffic. The best description of the observed situation, where the DNS server is overwhelmed by inbound traffic with minimal DNS queries, is that it is experiencing a reflected denial of service attack. Therefore, the correct answer is:

D. Reflected denial of service
upvoted 9 times

✉ MAKOhunter33333333 Highly Voted 6 months ago

Selected Answer: D

1. Unable to reach external websites, denial of service
2. Flooded with traffic
3. The traffic is not coming from with in via verifying with network logs

DOS is best option based on those details

upvoted 6 times

 **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: D

Minimal Resource Usage: The DNS server's CPU, disk, and memory usage are minimal, indicating that the server itself is not processing a large number of queries. However, the network interface is flooded with traffic, which is a key indicator of a reflected DoS attack.

Flooded Network Interface: The flooding of the network interface with inbound traffic without a corresponding increase in actual DNS query processing suggests that the server is receiving unsolicited responses, characteristic of a reflected DoS attack.

Why this is the best choice, because the symptoms match a reflected DoS, where the server is overwhelmed by traffic that it did not initiate, preventing legitimate users from accessing external websites due to the congestion

upvoted 1 times

 **MAKOhunter33333333** 6 months ago

1. Unable to reach external websites, denial of service
2. Flooded with traffic
3. The traffic is not coming from within via verifying with network logs

DOS is best option based on those details

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 139 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 139

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

A. RBAC Most Voted

B. ACL

C. SAML

D. GPO

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by MAKOhunter33333333 at May 22, 2024, 3:25 a.m.

Comments

✉ MAKOhunter33333333 Highly Voted 4 months, 2 weeks ago

Selected Answer: A

Role-based access control (RBAC) restricts users to only access data based on their job responsibilities.
upvoted 9 times

✉ AutoroTink Highly Voted 4 months, 2 weeks ago

Selected Answer: A

RBAC: Role-Based Access Control (Permissions based on roles. Others include: MAC, DAC, Rule-based, ABAC)
ACL: Access Control List (Popular with configuring firewalls)
SAML: Security Assertion Markup Language (used alongside SSO, authentication)
GPO: Group Policy Objective (used in hardening, to dictate policies, user rights, and audit settings)
upvoted 6 times

✉ Syl0 Most Recent 1 month ago

RBAC - Rule Based Access Control

ACL - Access Control List

SAML - Security Assertion Markup Language

GPO - Group Policy Object

upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: A

In this question the best choice is "A". RBAC (Role-Based Access Control) is correct because it allows the systems administrator to prevent unauthorized access by defining roles and assigning permissions based on user responsibilities. RBAC simplifies the access management process and ensures that users only have access to the data necessary for their roles.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 140 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 140

Topic #: 1

[\[All SY0-701 Questions\]](#)

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Choose two.)

A. Federation Most Voted

B. Identity proofing

C. Password complexity Most Voted

D. Default password changes

E. Password manager

F. Open authentication

[Hide Answer](#)

Suggested Answer: AC

Community vote distribution

AC (100%)

by 35f7aac at June 1, 2024, 7:32 p.m.

Comments

✉ dbrowndiver Highly Voted 3 months, 2 weeks ago

Selected Answer: AC

"A". Federation and "C". are the correct answers. Federation facilitates access to multiple systems using a single intranet profile, and password complexity ensures that the passwords used are strong and secure. These concepts work together to safeguard intranet accounts and streamline user access across various company-owned websites.

upvoted 5 times

✉ TheMichael Most Recent 4 months ago

Selected Answer: AC

Answer: A and C

Federation establishes trust with a third-party that manages authentication, potentially providing a more secure solution for internal company systems. In this scenario the company is the third party that grants access to other company-owned websites.

The answer is not Open authentication because Open authentication allows you to log into any other company-owned websites with your password, not intranet profile. Open authentication is less secure so a company would be less likely to use it in this fashion which also makes A and C make more sense.

upvoted 3 times

 **NoobusAurelius** 4 months ago

I agree with NadirM_18 C and F makes sense because it only states Company owned websites, not company systems/apps.

upvoted 2 times

 **NadirM_18** 4 months, 1 week ago

Seems like this could be CF as this is within the same company.

upvoted 1 times

 **NadirM_18** 3 months, 3 weeks ago

The key difference between SSO and FIM is while SSO is designed to authenticate a single credential across various systems within one organization, federated identity management systems offer single access to a number of applications across various enterprises.

upvoted 1 times

 **c80f5c5** 5 months, 2 weeks ago

This one is tricky because federation and open auth are very similar. I think OAuth might be for third party applications (like signing into a game with your facebook account) and not multiple company owned platforms like the question asks

upvoted 3 times

 **35f7aac** 5 months, 2 weeks ago

I guess what makes me thing OAuth is because OAuth supports SSO which is what I think is being hinted at here. I wish this question was worded better.

upvoted 2 times

 **35f7aac** 5 months, 2 weeks ago

OK. I'm going to change to Federation because i just found this on Okta's site. "SAML is independent of OAuth, relying on an exchange of messages to authenticate in XML SAML format, as opposed to JWT. It is more commonly used to help enterprise users sign in to multiple applications using a single login."

upvoted 1 times

 **35f7aac** 5 months, 2 weeks ago

Hmm. Why not F instead of A? Question says "other company-owned websites". I thought Federation applies more to independent organizations connecting together.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 141 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 141

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

- A. SIEM Most Voted
- B. DLP
- C. IDS
- D. SNMP

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 7:55 a.m.

Comments

adderallpm Highly Voted 5 months, 1 week ago

Security information and event management
upvoted 5 times

dbrownidiver Most Recent 3 months, 2 weeks ago

Selected Answer: A

SIEM is the correct answer because SIEM systems are specifically designed to collect, centralize, and analyze logs from multiple sources, providing security alerting and monitoring capabilities essential for detecting and responding to potential threats.
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 142 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 142

Topic #: 1

[\[All SY0-701 Questions\]](#)

A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

Something you know -

Something you have -

Something you are -

Which of the following would accomplish the manager's goal?

- A. Domain name, PKI, GeoIP lookup
- B. VPN IP address, company ID, facial structure
- C. Password, authentication token, thumbprint Most Voted
- D. Company URL, TLS certificate, home address

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at June 4, 2024, 7:55 a.m.

Comments

✉ **nesquick0** 1 month, 4 weeks ago

Selected Answer: C

C obviously
upvoted 2 times

✉ **420JhonnySins69** 3 weeks, 4 days ago

But I know my VPN IP address by memory.

VPN IP address (something that I know), Company ID)

I'm my home address.

upvoted 1 times

 **Shaman73** 4 months ago

- C. Password, authentication token, thumbprint

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 143 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 143

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation Most Voted

B. Isolation

C. Hardening

D. Decommissioning

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (53%)

B (31%)

C (16%)

by [Punjistetics](#) at May 10, 2024, 1:14 a.m.

Comments

✉ [Etc_Shadow28000](#) Highly Voted 3 months, 3 weeks ago

Selected Answer: A

A. Segmentation

Segmentation is the best approach to handle a critical business application running on a legacy server. By segmenting the legacy server from the rest of the network, you can limit the potential impact of any vulnerabilities associated with the legacy system. This approach allows the critical application to continue running while minimizing the risk to the rest of the network.

Therefore, the correct answer is:

A. Segmentation

upvoted 13 times

✉ [AutoroTink](#) Highly Voted 4 months, 3 weeks ago

Selected Answer: C

Hardening involves implementing security measures to protect the application from threats while maintaining its availability. Segmentation and isolation can also be part of a security strategy, they are more about limiting access or separating the legacy system from other network segments,

which might not be feasible for a critical business application that requires interaction with other systems.
upvoted 6 times

 **a4e15bd** 2 months ago

hardening involves measures such as patches, removing unnecessary services, and tightening configurations to reduce vulnerabilities. While hardening is crucial, it may not be sufficient on its own for handling a legacy server due to the inherent limitations and risks of older systems. Isolation, might be better strategy because it minimizes the exposure of the lacy server to the rest of the network and reduce potential impact of any security issues on other systems.

upvoted 1 times

 **User92** Most Recent 3 days, 10 hours ago

Selected Answer: A

The keyword here is "critical business application", "B" is the best choice for maximum security. However, a "critical business application" needs to balance security with resource efficiency (compensating mechanism), so I would go with "A".

upvoted 1 times

 **Laura5859** 4 days, 16 hours ago

Selected Answer: B

The Official CompTIA Security+ Study Guide (Exam SY0-701) pg 32 has an explanation mark that says: "One strategy for dealing with unsupported apps that cannot be replaced is to try to isolate them from other systems. The idea is to reduce opportunities for a threat actor to access the vulnerable app and run exploit code. Using isolation as a substitute for patch management is an example of a compensating control."

upvoted 1 times

 **Laura5859** 4 days, 16 hours ago

The Official CompTIA Security+ Study Guide (Exam SY0-701) has an explanation mark that says:

"One strategy for dealing with unsupported apps that cannot be replaced is to try to isolate them from other systems. The idea is to reduce opportunities for a threat actor to access the vulnerable app and run exploit code. Using isolation as a substitute for patch management is an example of a compensating control."

upvoted 1 times

 **Ty13** 1 week, 3 days ago

Selected Answer: B

B. Isolation

Segmenting a network means breaking the network into smaller subnets, like one for HR, one for Payroll, one for Management, etc. The idea being that you can end connections to one segment entirely in the event of a compromise, without impacting other segments.

Isolation is just the next step further - if a device is old and unsupported, like Windows XP, then you'd want to have it completely on its own where it can't touch the rest of the network inappropriately.

upvoted 1 times

 **koala_lay** 3 weeks, 1 day ago

Selected Answer: A

Agree to answer: A. segmentation

upvoted 1 times

 **baronvon** 1 month, 1 week ago

Selected Answer: B

B. Isolation

The reason for this comes from the CompTIA Security+ study guide:

"In cases where the organization simply must continue using an unsupported operating system, best practice dictates isolating the system as much as possible, preferably not connecting it to any network, and applying as many compensating security controls as possible, such as increased monitoring and implementing strict network firewall rules."

upvoted 3 times

 **a4e15bd** 1 month, 2 weeks ago

Isolation is used to completely separate a system from the network which is ideal if the primary goal is to eliminate any potential risk of legacy server compromising other systems. It is more extreme measure, typically applied when the application doesn't need to communicate with other systems or when the risk is deemed too high.

Segmentation on the other hand is used to limit the legacy applications communication to only necessary interactions which still protects the rest of the network but allows the application to function normally. It is more nuanced approach allowing for controlled interactions while still reducing risk.

So A. Segmentation is the best option because it provides a balance between security and functionality allowing the legacy system to continue operating within a restricted and monitored environment.

upvoted 3 times

 **nesquick0** 1 month, 3 weeks ago

Selected Answer: C

C. Hardening

upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: B

Not Fully Isolated: While segmentation improves security, it doesn't offer the complete separation provided by isolation. If the legacy server is compromised, segmentation might not prevent the spread of threats as effectively as isolation.

Complex Implementation: Requires careful planning to ensure correct segmentation, which can introduce complexity without providing the full benefits of isolation.

upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: B

Isolation is the best approach for handling a critical business application on a legacy server. It involves separating the legacy system from the rest of the network, thereby reducing the risk of security breaches affecting the broader network while still allowing the application to function as needed.

Isolation: This approach involves creating a separate environment for the legacy system, preventing it from directly interacting with other network components. Isolation minimizes exposure to threats and limits the potential impact of vulnerabilities.

In this Scenario Application: Security Risk Mitigation: By isolating the legacy server, the company can protect its network from potential vulnerabilities that the outdated system might introduce. This is crucial for critical applications that cannot be immediately upgraded or replaced. Isolation allows the application to continue running without immediate disruption, maintaining business continuity while planning for future upgrades or replacements. Why this is best over the other choices: Isolation balances the need to keep the application operational while protecting the rest of the network from potential risks associated with legacy systems.

upvoted 3 times

 **NoobusAurelius** 2 months, 2 weeks ago

Answer is A. Segmentation, if you read the question it says critical Business application, isolating the server would impact its ability to interact with other systems on the Network and therefore Business Operations will be affected. Hardening has the potential to affect server performance and being a legacy server it may not be compatible with current software, hardware or other hardening techniques. Decommissioning could be an option if the application can be migrated out of hours to a brand new server, but that isn't really what the question is alluding to.

upvoted 1 times

 **WOW_ThatsCrazy** 3 months ago

Selected Answer: B

Isolation is the process of separating the legacy system from the rest of the network to reduce the risk of vulnerabilities being exploited. This approach allows the legacy application to continue operating while minimizing its exposure to potential threats.

Segmentation is similar but generally applies to creating separate network segments for security. However, isolation goes further by limiting interactions strictly to what is necessary.

upvoted 1 times

 **cdsu** 3 months, 2 weeks ago

B. Isolation

...managing a critical business application on a legacy server. By separating the legacy server from the rest of the network to prevent potential threats from spreading. This way effective in protecting the critical application from vulnerabilities inherent to the legacy system.

upvoted 1 times

 **Dean1065** 3 months, 3 weeks ago

Selected Answer: A

A. Segmentation is one of the only things you can do for legacy systems.

upvoted 1 times

 **Shaman73** 4 months ago

• B. Isolation

Segmentation, wenn die Application mehrere Systeme bräuchte; Härtung geht nicht mehr; Decommissioning noch nicht....

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 144 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 144

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A. VM escape
- B. SQL injection
- C. Buffer overflow Most Voted
- D. Race condition

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at June 4, 2024, 7:58 a.m.

Comments

✉ **Shaman73** Highly Voted 5 months, 2 weeks ago

- C. Buffer overflow
upvoted 5 times

✉ **dbrowndiver** Most Recent 3 months, 2 weeks ago

Selected Answer: C

The scenario specifically mentions overwriting a register with a malicious address, which is a hallmark of a buffer overflow attack. This technique is commonly used to redirect the program to execute malicious instructions, making buffer overflow the most relevant vulnerability here. In a buffer overflow attack, the attacker might overwrite a register or a return address on the stack with a malicious address, redirecting the program's control flow to execute arbitrary code.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 145 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 145

Topic #: 1

[\[All SY0-701 Questions\]](#)

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

- A. Retain the emails between the security team and affected customers for 30 days.
- B. Retain any communications related to the security breach until further notice. Most Voted
- C. Retain any communications between security members during the breach response.
- D. Retain all emails from the company to affected customers for an indefinite period of time.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Shaman73](#) at June 4, 2024, 7:58 a.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: B

Retain any communications related to the security breach until further notice is the correct answer. This approach ensures that all relevant evidence is preserved in compliance with the legal hold, covering the full scope of communications and documents needed for the lawsuit. It aligns with the purpose of a legal hold, which is to safeguard all potential evidence until the legal proceedings are complete.

upvoted 2 times

  [Shaman73](#) 5 months, 2 weeks ago

- B. Retain any communications related to the security breach until further notice.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 146 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 146

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes the process of concealing code or text inside a graphical image?

- A. Symmetric encryption
- B. Hashing
- C. Data masking
- D. Steganography Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at May 31, 2024, 9:47 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: D

Steganography is the correct answer because it specifically involves the process of concealing code or text inside a graphical image, allowing information to be hidden in plain sight. This technique is unique in its ability to embed data within another medium, making it distinct from other security and privacy techniques like encryption, hashing, or data masking.

upvoted 2 times

✉ **Shaman73** 5 months, 3 weeks ago

D. Steganography

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 147 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 147

Topic #: 1

[\[All SY0-701 Questions\]](#)

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

- A. Vishing
- B. Smishing Most Voted
- C. Pretexting
- D. Phishing

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [jennyka76](#) at June 29, 2024, 4:17 p.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: B

Smishing is the correct answer because the attack is conducted via SMS text messages, and the goal is to manipulate the employee into taking action (purchasing gift cards) based on fraudulent communication. Smishing precisely captures the medium and technique used in this type of social engineering attack.

upvoted 2 times

  [jennyka76](#) 4 months, 3 weeks ago

Answer - B

Smishing, a combination of the words "SMS" and "phishing", is a type of cybercrime that uses deceptive text messages to trick people into sharing sensitive information or downloading malware. Smishing messages may appear to be from a reputable company, such as a bank, and may include a link or phone number to entice the recipient into clicking or calling. If the victim interacts with the message as intended, they may be led to a fraudulent website where they enter personal or financial information, or they may unknowingly download malicious software onto their device. If they call a number, the attacker may try to trick them into providing information verbally or incurring charges.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 148 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 148

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

A. Mitigate Most Voted

B. Accept

C. Transfer

D. Avoid

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 7:59 a.m.

Comments

✉ [Etc_Shadow28000](#) Highly Voted 3 months, 3 weeks ago

Selected Answer: A

A. Mitigate

When a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the first risk management strategy an enterprise should adopt is to mitigate the risks. This involves implementing measures to reduce the risk to an acceptable level. Mitigation can include steps such as patching vulnerabilities, applying compensating controls, segmenting the network, and hardening the application and its environment.

Therefore, the correct answer is:

A. Mitigate

upvoted 6 times

✉ [Syl0](#) Most Recent 1 month ago

Selected Answer: A

Mitigate 1st since it is a legacy application and is critical
upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: A

Critical Legacy Application: The application is crucial for business operations, so removing it (avoiding) or accepting the risk without any action could have severe implications.
Preventative Controls Needed: Since preventative controls are not yet implemented, mitigation would involve applying these controls to enhance security and reduce risk exposure.
This why it is the best choice: Mitigation is the most appropriate strategy for addressing risks associated with critical applications, especially when controls can be applied to minimize potential threats.

upvoted 2 times

 **Shaman73** 4 months ago

A. Mitigate

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 149 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 149

Topic #: 1

[\[All SY0-701 Questions\]](#)

Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule. Which of the following best describes this form of security control?

A. Physical Most Voted

B. Managerial

C. Technical

D. Operational

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at May 31, 2024, 9:47 a.m.

Comments

✉ [d4a5620](#) 1 month ago

Selected Answer: A

A) Physical: This is a physical security control because it involves physical barriers and measures to control access to the facility, such as checking photo IDs and using an access control vestibule.

B) Managerial: Managerial controls are policies, procedures, and guidelines established by an organization to ensure security compliance and oversight. This scenario is more focused on physical actions than managerial oversight.

C) Technical: Technical controls involve systems and software (e.g., firewalls, encryption) that secure data and systems electronically. The scenario here involves people and physical infrastructure, not technology.

D) Operational: Operational controls are implemented by people in their day-to-day activities, such as security training or incident response. While the scenario involves operational tasks, the primary focus is on physical security measures.

In summary, physical controls like ID checks and vestibules are examples of barriers to control access to secure areas, making A) Physical the best choice.

upvoted 2 times

 **Shaman73** 4 months, 1 week ago

A. Physical

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 150 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 150

Topic #: 1

[\[All SY0-701 Questions\]](#)

The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening?

- A. Using least privilege
- B. Changing the default password Most Voted
- C. Assigning individual user IDs
- D. Reviewing logs more frequently

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (60%) C (20%) A (20%)

by [Shaman73](#) at June 4, 2024, 8:01 a.m.

Comments

✉ **Shaman73** Highly Voted 4 months ago

B. Changing the default password
upvoted 8 times

✉ **Ty13** Most Recent 1 week, 3 days ago

Selected Answer: B
Answer is B.

It's the *local* admin account. A and C wouldn't work here because those are talking specifically about non-local accounts.

To put it another way, go check your home router - if it's old enough, there's like a 99% chance the default username/password is just admin/admin. It's hard-coded so if you ever physically reset the device then the creds will always default back.
upvoted 1 times

✉ **Fhaddad81** 2 weeks, 5 days ago

I will select C since its local administrator with default permission and should not be used remotely and best practice to assign individual user for each IT admin should manage this device

upvoted 1 times

 **chasingsummer** 2 weeks, 6 days ago

Selected Answer: C

I think you need to have separate account for VPN and separate account for management.

Option C makes the most sense; Assigning individual user IDs

upvoted 1 times

 **420JhonnySins69** 3 weeks, 1 day ago

Selected Answer: A

I'm just want to vote for A, because it seems the most reasonable.

upvoted 1 times

 **d4a5620** 4 weeks ago

idk if it's my ADHD or what but I had to re-read this question like 5 times and I still don't completely understand what they're asking lol

upvoted 4 times

 **internslayer** 1 month, 3 weeks ago

This is why I hate Sec+ questions. It should be assumed that part of assigning individual user accounts would be to disable a shared local admin account. Using shared accounts is bad practice!!

upvoted 1 times

 **dbrowndiver** 2 months ago

Selected Answer: B

Many devices and applications come with default administrator credentials that are intended to be changed immediately after installation. Failure to change these passwords leaves systems vulnerable to unauthorized access. By changing the default password for the local administrator account, the company would significantly reduce the risk of unauthorized access. Attackers often attempt to use default credentials to gain entry, so ensuring these are changed is a fundamental security practice.

upvoted 2 times

 **c80f5c5** 4 months ago

i guess you could assume both administrative accounts have the same default login

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 151 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 151

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the best way to secure an on-site data center against intrusion from an insider?

- A. Bollards
- B. Access badge Most Voted
- C. Motion sensor
- D. Video surveillance

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 4, 2024, 8:02 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: B

Access badge is the correct answer because it provides a direct method of controlling and monitoring access to the data center, ensuring that only authorized personnel can enter. Access badges are an effective way to prevent insider threats by restricting access based on roles and permissions, making them the best choice for securing an on-site data center against intrusion from insiders.

upvoted 2 times

✉ **jem003** 4 months, 1 week ago

Selected Answer: B

Access Badge: This allows for controlled and monitored entry into the data center. Only authorized personnel with a valid badge can enter, which helps to prevent unauthorized access. Access badges can be integrated with identity management systems, providing a log of who accessed the data center and when, which is crucial for auditing and accountability.

upvoted 2 times

✉ **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. Access badge
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 152 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 152

Topic #: 1

[\[All SY0-701 Questions\]](#)

An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

A. Role-based Most Voted

B. Discretionary

C. Time of day

D. Least privilege

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 4, 2024, 8:02 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: A

Role-based is the correct answer because the issue arises from the engineer's account not being updated to include the new role associated with the new team's shared folders. Role-Based Access Control is the framework in place that determines access based on roles assigned to users, making it the most relevant explanation for the engineer's access issue.

upvoted 2 times

✉ **Shaman73** 5 months, 2 weeks ago

Selected Answer: A

A. Role-based
upvoted 3 times

✉ **Shaman73** 5 months, 2 weeks ago

• A. Role-based

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 153 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 153

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Choose two.)

- A. Channels by which the organization communicates with customers
- B. The reporting mechanisms for ethics violations
- C. Threat vectors based on the industry in which the organization operates Most Voted
- D. Secure software development training for all personnel
- E. Cadence and duration of training events Most Voted
- F. Retraining requirements for individuals who fail phishing simulations

[Hide Answer](#)

Suggested Answer: CE

Community vote distribution

CE (100%)

by AutoroTink at May 14, 2024, 8:22 a.m.

Comments

Etc_Shadow28000 Highly Voted 3 months, 3 weeks ago

Selected Answer: CE

- C. Threat vectors based on the industry in which the organization operates
- E. Cadence and duration of training events

When formulating a training curriculum plan for a security awareness program, it is crucial to focus on:

- Threat vectors based on the industry in which the organization operates (C): Understanding the specific threats that are most relevant to the industry helps tailor the training content to address the most pressing risks and vulnerabilities that employees might face.
- Cadence and duration of training events (E): Establishing an appropriate schedule and duration for training ensures that employees receive regular, ongoing education to keep security top-of-mind and adapt to evolving threats.

Therefore, the correct answers are:

- C. Threat vectors based on the industry in which the organization operates
 - E. Cadence and duration of training events
- upvoted 7 times

 Th3irdEye  4 months, 3 weeks ago

Selected Answer: CE

C you need to know what to train against
E training schedule is one of the most important aspects of the curriculum

The chosen answer with talking about ethics violations is unrelated to security training.
Retraining requirements are important too but less so than C and E.

upvoted 5 times

 Jacket  3 weeks, 1 day ago

C. Threat vectors based on the industry in which the organization operates:

Understanding the specific threats that are relevant to your industry is critical. Different industries face unique risks (e.g., phishing attacks in finance, insider threats in healthcare). Training should be tailored to address these industry-specific threats to ensure the most relevant and effective education for employees.

E. Cadence and duration of training events:

The frequency and length of training sessions are essential to ensure that the training is both effective and engaging. Regular, well-timed training helps reinforce security principles, ensuring employees are constantly aware of evolving threats and practices without feeling overwhelmed.

upvoted 1 times

 dbrowndiver 2 months ago

Selected Answer: CE

opt C. Threat vectors based on the industry in which the organization operates and opt E. Cadence and duration of training events are the correct answers. These factors ensure that the training is relevant, engaging, and effective by focusing on the specific threats the organization faces and maintaining consistent reinforcement through well-planned training sessions.

upvoted 1 times

 Shaman73 4 months ago

Selected Answer: CE

C. Threat vectors based on the industry in which the organization operates Most Voted
E. Cadence and duration of training events Most Voted

upvoted 1 times

 edmondme 4 months ago

Selected Answer: CE

ethics issues are unrelated to security trainings. Also setting a cadence is another important factor

upvoted 2 times

 c80f5c5 4 months ago

Selected Answer: CE

Threat vectors and training schedule sounds more important to me than the others

upvoted 1 times

 AutoroTink 4 months, 3 weeks ago

Selected Answer: CE

If I was to make a curriculum, I'd want to know the biggest "what" that we would teach, and "when" and "how often" we'd be teaching it. The others are great, but not as important as these two things.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 154 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 154

Topic #: 1

[\[All SY0-701 Questions\]](#)

A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfil?

- A. Privacy
- B. Integrity
- C. Confidentiality
- D. Availability Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at May 31, 2024, 9:48 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: D

Availability is the correct answer because deploying a load balancer enhances the availability of applications and services by distributing traffic, providing redundancy, and ensuring continued access to resources even in the event of server failures. This project directly supports the availability aspect of the security triad.

upvoted 3 times

✉ **Dlove** 4 months ago

D. Availability

Load balancing in cloud computing distributes traffic and workloads to ensure that no single server or machine is under-loaded, overloaded, or idle. Load balancing optimizes various constrained parameters such as execution time, response time, and system stability to improve overall cloud performance. Therefore it allows the systems more availability.

upvoted 2 times

✉ **Shaman73** 5 months, 3 weeks ago

D. Availability
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 155 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 155

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

A. Deploying PowerShell scripts

B. Pushing GPO update Most Voted

C. Enabling PAP

D. Updating EDR profiles

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 6, 2024, 12:50 p.m.

Comments

adderallpm Highly Voted 5 months ago

Group Policy Objects (GPOs) provides an infrastructure for centralized configuration management of the Windows operating system and applications that run on the operating system. GPOs are a collection of settings that define what a system will look like and how it will behave for a defined group of computers or users.

upvoted 7 times

dbrowndiver Most Recent 3 months, 2 weeks ago

Selected Answer: B

Pushing GPO update is the correct answer because it allows the systems administrator to implement a new password policy across all systems quickly and efficiently through centralized management. GPOs provide the necessary tools to enforce security settings consistently throughout the enterprise environment.

upvoted 3 times

Shaman73 5 months, 2 weeks ago

Selected Answer: B

B. Pushing GPO update
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 156 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 156

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

- A. ARO
- B. RTO
- C. RPO
- D. ALE Most Voted
- E. SLE

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by SHADTECH123 at May 28, 2024, 11:45 a.m.

Comments

✉ SHADTECH123 Highly Voted 5 months, 3 weeks ago

Selected Answer: D

ALE (Annual Loss Expectancy) represents the expected monetary loss for an asset due to a risk over a year. It is calculated by multiplying the Annual Rate of Occurrence (ARO) by the Single Loss Expectancy (SLE). This provides a clear picture of the financial impact of a risk over time.
upvoted 14 times

✉ NinjaTrain Highly Voted 3 months, 3 weeks ago

ARO: Annual Rate of Occurrence
RTO: Recovery Time Objective
RPO: Recovery Point Objective
ALE: Annual Loss Expectancy
SLE: Single Loss Expectancy
upvoted 11 times

✉ dbrowndiver Most Recent 3 months, 2 weeks ago

Selected Answer: D

ALE (Annualized Loss Expectancy) is the correct answer because it combines both the potential impact of a single event and the frequency of that event occurring to provide a comprehensive financial estimate. This allows an organization to effectively compare the long-term costs of risk transfer strategies against the expected impact of the risk.

upvoted 2 times

 **Shaman73** 5 months, 2 weeks ago**Selected Answer: D**

D. ALE

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 157 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 157

Topic #: 1

[\[All SY0-701 Questions\]](#)

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

- A. Key stretching
- B. Tokenization
- C. Data masking
- D. Salting Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (88%) 13%

by [Shaman73](#) at June 6, 2024, 12:51 p.m.

Comments

✉ **dbrowndiver** Highly Voted 2 months ago

Selected Answer: D

Salting is the correct answer because it involves adding a random string to a password before hashing to strengthen security. This technique effectively prevents precomputed hash attacks, making it a critical component of modern password protection strategies.

upvoted 5 times

✉ **jsmthy** Most Recent 1 week, 4 days ago

Selected Answer: A

Key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources it takes to test each possible key.

Salting does not add to the length of the password and does not stop attackers from brute-forcing the key as the salt is added after the password is submitted.

Tokenization and Data masking will not prevent brute-force attacks for the same reason. They are processes that don't alter a weak password.

upvoted 1 times

 **Shaman73** 4 months ago**Selected Answer: D**

D. Salting
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 158 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 158

Topic #: 1

[\[All SY0-701 Questions\]](#)

A technician is deploying a new security camera. Which of the following should the technician do?

- A. Configure the correct VLAN.
- B. Perform a vulnerability scan.
- C. Disable unnecessary ports.
- D. Conduct a site survey. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (89%) 11%

by AutoroTink at May 8, 2024, 7:54 a.m.

Comments

✉ Etc_Shadow28000 Highly Voted 3 months, 3 weeks ago

Selected Answer: D

D. Conduct a site survey.

Before deploying a new security camera, conducting a site survey is crucial. A site survey helps determine the optimal placement of the camera, assesses environmental factors, ensures there are no blind spots, and verifies that the camera will effectively cover the desired area. It also helps in planning for network connectivity, power supply, and other logistical considerations.

Therefore, the correct answer is:

D. Conduct a site survey.

upvoted 5 times

✉ AutoroTink Highly Voted 5 months ago

Selected Answer: D

A site survey is essential to determine the best locations for camera installation, ensuring optimal coverage and signal strength. It involves assessing the physical environment to identify any potential issues that could affect the camera's performance, such as obstructions, lighting

conditions, and power source availability.

- A. Configure the correct VLAN: While important for network segmentation, it's not the first step in physical deployment.
- B. Perform a vulnerability scan: This is more relevant for assessing the security of existing systems, not the initial placement of a camera.
- C. Disable unnecessary ports: This is a security measure for network devices, but it doesn't address the physical aspects of camera deployment.
upvoted 5 times

 **Ty13** Most Recent 1 week, 2 days ago

Are they deploying a new camera to replace an old one? If so, it's C, because they wouldn't need to conduct a site survey if they already have optimal locations set.

Is it just the thought of "Hey, I want to get a camera in the parking garage."? Then it would be D.

upvoted 1 times

 **93a09c9** 2 months ago

Selected Answer: D

A site survey is ALWAYS the first step before installing any system or component.

upvoted 1 times

 **dbrownidiver** 2 months ago

Selected Answer: D

Conduct a site survey is the correct answer because it is the critical first step in deploying a new security camera. It ensures that the camera is installed in the right location and covers the necessary areas effectively. Once the site survey is completed, other actions such as VLAN configuration, vulnerability scanning, and port management can follow to ensure optimal performance and security.

upvoted 1 times

 **cdsu** 3 months, 2 weeks ago

Answer: D

...physical placement first

upvoted 3 times

 **Shaman73** 4 months ago

Selected Answer: D

D. Conduct a site survey.

upvoted 2 times

 **f71cbb0** 4 months, 2 weeks ago

Selected Answer: C

C should be better answer than D. Deploying is not the same installing.

If a technician were "installing" a new security camera, then the best answer would be (D) conduct a site survey.

upvoted 3 times

 **SHADTECH123** 4 months, 3 weeks ago

Selected Answer: D

Conducting a site survey involves assessing the physical environment where the security camera will be installed. This includes identifying optimal camera placement, ensuring sufficient coverage, assessing lighting conditions, and identifying potential sources of interference. It helps ensure that the security camera is deployed effectively to meet the organization's surveillance requirements.

upvoted 3 times

 **Yoez** 4 months, 3 weeks ago

Selected Answer: D

I would say D

upvoted 3 times

 **shady23** 4 months, 4 weeks ago

Selected Answer: D

D. Conduct a site survey.

The keyword in the question that makes option D correct is "deploying a new security camera."

Conducting a site survey is crucial when deploying new security cameras because it allows the technician to assess various factors such as the physical environment, potential obstacles, optimal camera placement, coverage areas, and lighting conditions. This ensures that the security camera is installed in the most effective location to fulfill its surveillance objectives.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 159 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 159

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is experiencing a web services outage on the public network. The services are up and available but inaccessible. The network logs show a sudden increase in network traffic that is causing the outage. Which of the following attacks is the organization experiencing?

- A. ARP poisoning
- B. Brute force
- C. Buffer overflow
- D. DDoS Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 6, 2024, 12:52 p.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: D

DDoS is the correct answer because the sudden increase in network traffic leading to a web services outage is characteristic of a Distributed Denial of Service attack. This type of attack overwhelms the target's resources, making services inaccessible, even though they are still operational. DDoS attacks specifically aim to disrupt access by flooding the target with excessive traffic, matching the symptoms described in the scenario.

upvoted 3 times

  [Shaman73](#) 5 months, 2 weeks ago

Selected Answer: D

D. DDoS

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 160 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 160

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following threat actors is the most likely to be motivated by profit?

- A. Hacktivist
- B. Insider threat
- C. Organized crime Most Voted
- D. Shadow IT

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at May 31, 2024, 9:49 a.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: C

Profit is the main driver for organized crime, making them the most likely threat actor motivated by financial incentives. They are structured to exploit opportunities that result in monetary rewards. Therefore, Organized crime is the correct answer because organized crime groups are primarily driven by the pursuit of financial gain. They engage in cyber activities designed to steal, extort, or otherwise generate profit, making them the most profit-motivated threat actor in this context.

upvoted 3 times

✉ **Shaman73** 5 months, 3 weeks ago

C. Organized crime

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 161 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 161

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Choose two.)

- A. Application
- B. Authentication
- C. DHCP
- D. Network Most Voted
- E. Firewall Most Voted
- F. Database

[Hide Answer](#)

Suggested Answer: DE

Community vote distribution

DE (85%)

Other

by [Shaman73](#) at June 6, 2024, 12:53 p.m.

Comments

[Shaman73](#) Highly Voted 5 months, 2 weeks ago

[Selected Answer: DE](#)

- D. Network
 - E. Firewall
- upvoted 7 times

[c7b3ff0](#) Most Recent 1 month ago

[Selected Answer: BE](#)

Since this is specifically asking about identifying the impacted host, I chose B and E.
B. Authentication - This log helps identify any unauthorized access or unusual login attempts related to compromised hosts.
E. Firewall - provide insights into incoming and outgoing traffic patterns, detecting comms with the C2 server to help identify the affected host.

upvoted 1 times

 **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: CE

C. DHCP and E. Firewall logs are the correct answers because they provide essential information to trace network communications and identify the specific host(s) impacted by the command-and-control server connection. Firewall logs help pinpoint unusual outbound connections, such as those from internal hosts to a suspicious external server, thus identifying potential breaches. DHCP logs map IP addresses to devices, while firewall logs reveal the network traffic patterns, making them both crucial for this analysis. DHCP logs are crucial for linking IP addresses seen in network activity to actual devices, especially in dynamic environments where IP addresses frequently change.

upvoted 1 times

 **101e7ca** 3 months, 4 weeks ago

Selected Answer: DE

"command-and-control server" is the problem, attacker has accessed the network and taken control of a machine. We should check the inbound and outbound traffic logs. These will be on the Router(Network) and network Firewall.

upvoted 2 times

 **Bimbo_12** 3 months, 4 weeks ago

Selected Answer: DE

To identify the impacted host in a cybersecurity incident involving a command-and-control server, the most relevant logs to analyze would be:

C. DHCP and E. Firewall

: Firewall logs capture network traffic and can show which internal hosts communicated with external IP addresses, including the command-and-control server.

By analyzing firewall logs, you can identify the internal IP addresses that initiated or received communication with the command-and-control server, helping to pinpoint the impacted host.

If you have already identified suspicious network traffic (e.g., connections to a C2 server) in firewall or network logs, the next step is often to determine which device was responsible for that traffic.

DHCP logs are necessary for this step because they map IP addresses to specific devices. Without this mapping, knowing the IP address alone is insufficient, especially in environments where IP addresses are dynamically assigned.

By consulting DHCP logs, you can quickly identify the physical or virtual device behind the suspicious activity.

upvoted 2 times

 **cdsu** 4 months, 4 weeks ago

Answer:

C. DHCP

E. Firewall

C: Impacted host. To trace back any suspicious network activity to a specific device

E: Firewall logs contain records of all incoming and outgoing traffic

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 162 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 162

Topic #: 1

[\[All SY0-701 Questions\]](#)

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

- A. Defensive
- B. Passive
- C. Offensive
- D. Physical Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 6, 2024, 12:55 p.m.

Comments

 [96bc5c8](#) 6 days, 20 hours ago

kjgjhkg

upvoted 1 times

 [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: D

o The scenario specifically involves testing the ability to physically enter a secure area, which aligns perfectly with the definition of a physical penetration test.

upvoted 1 times

 [Shaman73](#) 5 months, 2 weeks ago

Selected Answer: D

D: Physical

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 163 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 163

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator uses a key to encrypt a message being sent to a peer in a different branch office. The peer then uses the same key to decrypt the message. Which of the following describes this example?

- A. Symmetric Most Voted
- B. Asymmetric
- C. Hashing
- D. Salting

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (80%)

C (20%)

by 123456789User at May 23, 2024, 3:15 p.m.

Comments

✉ nesquick0 1 month, 4 weeks ago

Selected Answer: A

A. Symmetric
upvoted 2 times

✉ Dlove 2 months, 2 weeks ago

Selected Answer: A

A. Symmetric same key to encrypt and decrypt
upvoted 3 times

✉ c80f5c5 4 months ago

Selected Answer: A

symmetric
upvoted 3 times

 **Shaman73** 4 months, 1 week ago

A. Symmetric
upvoted 3 times

 **MAKOhunter33333333** 4 months, 1 week ago

Selected Answer: A

The same key for both processes
upvoted 4 times

 **shady23** 4 months, 2 weeks ago

Selected Answer: C

Symmetric Encryption
In this type of encryption, there is only one key, and all parties involved use the same key to encrypt and decrypt information.
upvoted 4 times

 **drosas84** 3 months, 4 weeks ago

then why did you choose C when it should be A?
upvoted 2 times

 **SHADTECH123** 4 months, 1 week ago

You stated your Selected Answer to be "C" - Hashing, but explained Symmetric encryption, I guess it's a typo
upvoted 3 times

 **123456789User** 4 months, 2 weeks ago

Selected Answer: A

Symmetric: Same key is used to encrypt as is used to decrypt.
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 164 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 164

Topic #: 1

[\[All SY0-701 Questions\]](#)

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

- A. Port security Most Voted
- B. Web application firewall
- C. Transport layer security
- D. Virtual private network

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (80%)

C (20%)

by MAKOhunter33333333 at May 22, 2024, 4:17 p.m.

Comments

✉ dbrowndiver 2 months ago

Selected Answer: A

Port security is a feature available on network switches that helps secure access to the physical network by restricting which devices can connect to each network port based on their MAC address.

Port Security: This is a network security feature that restricts input to an interface by limiting and identifying MAC addresses of the devices allowed to access the port. It can be configured to block devices that do not match the allowed list.

-Control Over Physical Access: By enabling port security on the network jacks, the organization can ensure that only authorized devices with specific MAC addresses are allowed to connect. Any unauthorized devices, such as a visitor's laptop, would be blocked from accessing the network.

-Dynamic or Static Configuration: Port security can dynamically learn and store allowed MAC addresses or use a predefined list, providing flexibility in securing physical network ports.

This why it is the best answer: Port security directly addresses the issue of unauthorized access through physical network connections by controlling which devices can use the network ports. It prevents unauthorized devices from gaining network access, making it the most appropriate solution for this scenario.

upvoted 4 times

✉ Andrewyounan 2 months, 2 weeks ago

Selected Answer: C

I go more for TLS which is part of EAP-TLS used with 802.1X on the NAC to authenticate.
On the other hand, Port Sec. you'll need to either identify the MAC address or Sticky MAC address, so it makes sense to go with C. ### Maybe I'm over-thinking ### :D
upvoted 3 times

 **tamdod** 1 month, 2 weeks ago

On Port security, you shut the port off so no one can use it.
upvoted 1 times

 **Shaman73** 4 months ago

Selected Answer: A

A. Port security
upvoted 4 times

 **MAKOhunter33333333** 4 months, 2 weeks ago

Selected Answer: A

Port security / 802.1x / NAC
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 165 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 165

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Choose two.)

A. Data retention

B. Certification Most Voted

C. Destruction

D. Classification

E. Sanitization Most Voted

F. Enumeration

[Hide Answer](#)

Suggested Answer: BE

Community vote distribution

BE (56%)

AE (29%)

Other

by AutoroTink at May 14, 2024, 8:28 a.m.

Comments

✉ cf83993 Highly Voted 2 months ago

Selected Answer: BE

Bro you don't reissue something after you destroy it do you? We're talking about a laptop here not an ex ;)
upvoted 14 times

✉ Th3irdEye Highly Voted 4 months, 3 weeks ago

Selected Answer: AE

Destruction would make the device not usable again. Certification might make sense here if a third party was being used to sanitize the drive but usually third parties are used to destroy drives and certification is given for destruction.

I think Data retention and Sanitization makes the most sense. You want to make sure you save any critical data before you erase the drive.

upvoted 7 times

 **nillie** Most Recent 4 days, 13 hours ago

Selected Answer: CE

The best combination of data handling activities for the administrator to perform when reissuing a former employee's laptop are:

C. Destruction and E. Sanitization

Destruction: Ensures that any sensitive or personal data from the previous user is permanently removed and cannot be recovered.

Sanitization: Refers to thoroughly cleaning the device by securely wiping the data to prevent unauthorized access. This prepares the laptop for safe reissue to a new user.

These two activities are critical for preventing any sensitive data leakage from the former employee while ensuring that the device is clean and secure for the next user.

upvoted 1 times

 **Ty13** 1 week, 2 days ago

Selected Answer: AE

Retention and Sanitize.

Think about it. An employee leaves - you backup any pertinent company data (Retention) and reimage the computer (Sanitize).

- You would not Certify it, because that's only if the drive needed to be destroyed.
- You would not Destroy it because that's really only important for sensitive things, not Judy the Customer Service agent.
- You would not Enumerate it (gathering info for vulnerabilities)
- Classification is typically more important for data rather than devices.

upvoted 2 times

 **ImpactTek** 2 weeks, 1 day ago

The answer is C&E. Destruction here refers to destroying data not the laptop.

upvoted 1 times

 **koala_lay** 3 weeks, 1 day ago

Selected Answer: BE

Agree to answer B E

upvoted 1 times

 **baronvon** 1 month, 1 week ago

Selected Answer: AE

A and E

Sanitization refers to the process of removing or cleaning data from a device to ensure that it cannot be recovered by unauthorized individuals. This typically includes methods such as wiping or formatting the storage media

While decommissioning and disposal are important, organizations often have to retain data or systems as well. Retention may be required for legal purposes with set retention periods determined by law, or retention may be associated with a legal case due to a legal hold

upvoted 4 times

 **tamdod** 1 month, 1 week ago

What about any data that may need to be retained? Should we not retain the data then sanitized it for reuse?

upvoted 1 times

 **Hayder81** 1 month, 2 weeks ago

B, E it's being reused. So, you need to sanitize and certify

upvoted 2 times

 **a4e15bd** 1 month, 2 weeks ago

C. Destruction

E. Sanitization

upvoted 2 times

 **pedrwc7** 1 month, 3 weeks ago

A. Data retention

• retain data

B. Certification

• Audit log of either Sanitization, Disposal or Destruction

C. Destruction

• Destruction goes beyond Sanitization ensures physical devices are unusable. It means you destroy it in pieces.

D. Classification

• Base on value and sensitivity of the data.

E. Sanitization

• Sanitization is thorough process to ensure the data is inaccessible and irretrievable, however, it can be reused.

F. Enumeration

•

upvoted 3 times

 **dbrowndiver** 2 months ago

When reissuing a laptop, it's crucial to ensure that all previous data is irretrievably removed, and the device is clean and secure for the next user. Destruction and Sanitization are two key processes involved in handling data securely in this context.

Opt. C. Destruction: This process involves permanently destroying data so it cannot be recovered. It is often used when data is no longer needed and must be securely eliminated.

Destruction is crucial to prevent data leakage or unauthorized access to old data. It provides peace of mind that the data is gone and cannot be retrieved.

Opt.E. Sanitization: This process involves cleaning a device to remove data and make it safe for reuse. Techniques include overwriting, degaussing, and cryptographic erasure.

Preparing for Reuse: Sanitization makes sure that all traces of previous data are removed, and the device is in a clean state, ready for new usage. Sanitization ensures that any residual data from the former employee is thoroughly erased, making the laptop safe and secure for the next user.

upvoted 3 times

 **EfaChux** 2 months ago

If it is for recycling then it would be destruction and certification and for reuse, it will be sanitization and certification

upvoted 1 times

 **Bimbo_12** 2 months, 2 weeks ago

Selected Answer: EF

Saitization for sure as the Security Admin needs to get rid of the old data.

Destruction is counterproductive as the Laptop is to be reissued.

Enumeration makes sense because it needs to be noted for in some form of inventory.

upvoted 1 times

 **nyyankee718** 2 months ago

Enumeration in iT security is related to probing not inventory

upvoted 2 times

 **cdsu** 3 months, 2 weeks ago

Answer:

C. Destruction

E. Sanitization

upvoted 1 times

 **drosas84** 3 months, 3 weeks ago

Selected Answer: BE

B/E it's being reused. So you need to sanitize and certify that it has been wiped clean.

upvoted 2 times

 **e56400d** 3 months, 4 weeks ago

I just did a large laptop resale at my company. In order to sell our old user's company laptops we had the wipe/sanitize the data and provide the certificate that the computer is wipe.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 166 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 166

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

A. Backout plan Most Voted

B. Impact analysis

C. Test procedure

D. Approval procedure

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Abcd123321](#) at May 20, 2024, 9:47 p.m.

Comments

✉ [Abcd123321](#) Highly Voted 6 months ago

Selected Answer: A

What is a backout plan?

A backout plan is a predefined strategy to reverse and recover from changes made to a system if the changes produce undesirable results. It's a safety measure that ensures data integrity and system availability. See also: backup, recovery time objective, mean time to recovery.

upvoted 8 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: A

Backout plan is the correct answer because it provides a detailed strategy for reverting changes in the event of a performance issue. This document ensures that the system can be restored to its working state, addressing the critical need for a reliable rollback mechanism during change management.

upvoted 2 times

 **Shaman73** 5 months, 2 weeks ago

Selected Answer: A

A. Backout plan
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 167 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 167

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

- A. Serverless
- B. Segmentation
- C. Virtualization Most Voted
- D. Microservices

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by MAKohunter33333333 at May 22, 2024, 4:21 p.m.

Comments

✉ **Exemplary** 20 hours, 24 minutes ago

Proud of all of you for not taking the bait!
upvoted 1 times

✉ **Syl0** 1 month ago

It only says reduce the number of physical servers, it didn't say it doesn't want servers....
upvoted 1 times

✉ **dbrowndiver** 2 months ago

Selected Answer: C
Virtualization is the correct answer because it enables the reduction of physical servers by allowing multiple virtual servers to operate on a single physical machine. Virtualization optimizes resource usage and simplifies management, aligning perfectly with the company's goal of minimizing physical infrastructure.
upvoted 3 times

✉️ **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: C

C. Virtualization

Virtualization is the architecture best suited for reducing the number of physical servers in use. It allows multiple virtual machines (VMs) to run on a single physical server, maximizing the utilization of hardware resources and reducing the need for multiple physical servers.

Therefore, the correct answer is:

C. Virtualization

upvoted 4 times

✉️ **Shaman73** 4 months ago

Selected Answer: C

C. Virtualization

upvoted 2 times

✉️ **MAKOhunter33333333** 4 months, 2 weeks ago

Selected Answer: C

Remove physical servers > transition to virtualization for services like the cloud.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 168 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 168

Topic #: 1

[\[All SY0-701 Questions\]](#)

A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring Most Voted
- D. User behavior analytics

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Shaman73](#) at June 6, 2024, 12:59 p.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: C

File Integrity Monitoring is the correct answer because it specifically addresses the need to monitor and detect unauthorized modifications to sensitive data. FIM ensures that any changes to files containing PII are identified and alerted, maintaining data integrity and protecting against unauthorized alterations.

upvoted 2 times

✉ **Dlove** 4 months ago

Selected Answer: C

C. File Integrity Monitoring

File integrity monitoring is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline.

upvoted 2 times

✉ **Shaman73** 5 months, 2 weeks ago

Selected Answer: C

C. File integrity monitoring
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 169 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 169

Topic #: 1

[\[All SY0-701 Questions\]](#)

Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked. Which of the following changes would allow users to access the site?

- A. Creating a firewall rule to allow HTTPS traffic
- B. Configuring the IPS to allow shopping
- C. Tuning the DLP rule that detects credit card data
- D. Updating the categorization in the content filter

[Most Voted](#)

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Shaman73](#) at June 6, 2024, 1 p.m.

Comments

✉ **3dk1** 3 weeks, 3 days ago

they went easy on us with this one
upvoted 1 times

✉ **dbrowndiver** 3 months, 2 weeks ago

[Selected Answer: D](#)

Updating the categorization in the content filter is the correct answer because it directly addresses the misclassification of the retail website as a gambling site. By correcting the categorization, users will be able to access the site without further issues, resolving the problem efficiently and effectively.

upvoted 4 times

✉ **ezmoney** 4 months, 2 weeks ago

D. Updating the categorization in the content filter
By updating the categorization in the content filter to accurately reflect the nature of the retail website (shopping instead of gambling), the content filter will allow users to access the site without being blocked.

upvoted 3 times

 **Shaman73** 5 months, 2 weeks ago

Selected Answer: D

Updating the categorization in the content filter

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 170 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 170

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following most impacts an administrator's ability to address CVEs discovered on a server?

- A. Rescanning requirements
- B. Patch availability Most Voted
- C. Organizational impact
- D. Risk tolerance

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 6, 2024, 1:01 p.m.

Comments

✉ [Etc_Shadow28000](#) Highly Voted 5 months, 1 week ago

Selected Answer: B

B. Patch availability

Patch availability most impacts an administrator's ability to address Common Vulnerabilities and Exposures (CVEs) discovered on a server. If patches are not available to fix the vulnerabilities, the administrator cannot remediate the issues, regardless of other factors.

Therefore, the correct answer is:

B. Patch availability
upvoted 6 times

✉ [dbrowndiver](#) Most Recent 3 months, 2 weeks ago

Selected Answer: B

Patch availability is the most critical factor in an administrator's ability to address CVEs on a server because it directly determines whether a known vulnerability can be fixed through updates or patches provided by software vendors. Patch Availability refers to whether a vendor has released a

software update or patch that addresses a specific vulnerability identified by a CVE. Without a patch, the administrator cannot remediate the vulnerability through standard update processes.

upvoted 3 times

 **Shaman73** 5 months, 2 weeks ago

Selected Answer: B

B. Patch availability

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 171 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 171

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- B. Having a backout plan when a patch fails Most Voted
- C. Using a spreadsheet for tracking changes
- D. Using an automatic change control bypass for security updates

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Shaman73](#) at June 6, 2024, 1:01 p.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: B

o When applying patches or making system changes, there's always a risk of unforeseen issues. An effective backout plan allows for a quick and organized response, ensuring that systems can be returned to their last known good state, thereby maintaining business continuity and reducing the potential impact on operations.

upvoted 3 times

  [Shaman73](#) 5 months, 2 weeks ago

Selected Answer: B

Having a backout plan when a patch fails

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 172 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 172

Topic #: 1

[\[All SY0-701 Questions\]](#)

The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?

- A. WAF utilizing SSL decryption
- B. NGFW utilizing application inspection Most Voted
- C. UTM utilizing a threat feed
- D. SD-WAN utilizing IPSec

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Shaman73](#) at June 6, 2024, 1:02 p.m.

Comments

✉ **Syl0** 1 month ago

WAF - Web App Firewall
NGFW - Next Generation Firewall
UTM - Unified Threat Management
SD-WAN - Software defined Wide area network
upvoted 1 times

✉ **dbrowndiver** 2 months ago

NGFW utilizing application inspection is the correct answer because it provides the necessary application-level awareness to detect and block HTTP traffic over non-standard ports, such as port 53. The NGFW's advanced inspection capabilities allow it to enforce security policies that prevent unauthorized data exfiltration, making it an essential component of modern network security infrastructure.

upvoted 3 times

✉ **dbrowndiver** 2 months ago

NGFW utilizing application inspection is the correct answer because it provides the capability to identify and block unauthorized applications and traffic using non-standard ports, such as HTTP traffic over port 53. Its advanced inspection capabilities make it well-suited to detect and prevent data exfiltration methods that involve protocol and port misuse.

upvoted 1 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: B

B. NGFW utilizing application inspection

A Next-Generation Firewall (NGFW) utilizing application inspection could have identified and blocked the use of HTTP over port 53. NGFWs have advanced capabilities that allow them to inspect and identify traffic based on the application layer, not just the port and protocol, enabling them to detect and prevent non-standard use of ports for malicious activities.

Therefore, the correct answer is:

B. NGFW utilizing application inspection

upvoted 4 times

 **Shaman73** 4 months ago

Selected Answer: B

B. NGFW utilizing application inspection

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

EXAM SY0-701 TOPIC 1 QUESTION 173 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 173

Topic #: 1

[\[All SY0-701 Questions\]](#)

An enterprise is working with a third party and needs to allow access between the internal networks of both parties for a secure file migration. The solution needs to ensure encryption is applied to all traffic that is traversing the networks. Which of the following solutions should most likely be implemented?

- A. EAP
- B. IPSec Most Voted
- C. SD-WAN
- D. TLS

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [edmondme](#) at June 5, 2024, 8:20 p.m.

Comments

[edmondme](#) Highly Voted 5 months, 2 weeks ago

Selected Answer: B

If you need to secure communication between networks or remote sites, IPsec is a suitable choice. On the other hand, if you are primarily concerned with securing web-based communication, TLS is the preferred option.

upvoted 8 times

[dbrowndiver](#) Highly Voted 3 months, 2 weeks ago

Selected Answer: B

IPSec is the correct answer because it provides comprehensive encryption for all IP traffic between the internal networks of both parties, ensuring secure file migration. IPSec's ability to encrypt, authenticate, and ensure the integrity of all data packets makes it the most suitable solution for protecting communications between the enterprise and the third party.

upvoted 5 times

[Shaman73](#) Most Recent 5 months, 2 weeks ago

Selected Answer: B

B. IPSec

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 174 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 174

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?

- A. DLP Most Voted
- B. SNMP traps
- C. SCAP
- D. IPS

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 6, 2024, 1:03 p.m.

Comments

✉️ **Syl0** 1 month ago

SNMP - Simple Network Management Protocol is for network devices.
SCAP - Security Content Automation Protocol
IPS - Intrusion Prevention System
DLP would be the one that focuses on Data because it is Data Loss Prevention
upvoted 2 times

✉️ **dbrowndiver** 2 months ago

Selected Answer: A
DLP is the correct answer because it is specifically designed to detect, monitor, and prevent the unauthorized transfer of sensitive data, such as fingerprinted files, outside the organization. DLP solutions provide the necessary tools to ensure data security by generating alerts and blocking unauthorized data exfiltration attempts.
upvoted 2 times

✉️ **adderallpm** 3 months, 2 weeks ago

Data Loss Prevention

upvoted 3 times

 **Shaman73** 4 months ago

Selected Answer: A

A. DLP

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 175 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 175

Topic #: 1

[\[All SY0-701 Questions\]](#)

A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

- A. Hashes Most Voted
- B. Certificates
- C. Algorithms
- D. Salting

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [Shaman73](#) at June 6, 2024, 1:04 p.m.

Comments

✉ **dbrowndiver** 3 months, 2 weeks ago

Selected Answer: A

Hashes is the correct answer because they provide a straightforward and reliable method for verifying the integrity of downloaded files. By comparing the hash of a downloaded file with the hash provided on the website, users can ensure that the file has not been altered, confirming its integrity and authenticity.

upvoted 2 times

✉ **Dlove** 4 months ago

Selected Answer: A

A. Hashes

Since hashes provide a way to verify that a file has not been altered by comparing the hash of the downloaded file with the hash provided by the developer, they are the correct choice.

upvoted 2 times

 **Shaman73** 5 months, 2 weeks ago**Selected Answer: A**

A. Hashes
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 176 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 176

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?

- A. Tokenization
- B. Hashing Most Voted
- C. Obfuscation
- D. Segmentation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (70%) A (15%) D (15%)

by [aed0e20](#) at June 1, 2024, 5:48 a.m.

Comments

✉ **dbrowndiver** Highly Voted 2 months ago

Selected Answer: B

When passwords are hashed, the database stores only the hash values instead of the actual passwords. This means that even if the database is breached, the attackers cannot easily obtain the original passwords.

Hashing is a one-way function, meaning it is computationally infeasible to reverse-engineer the original input from the hash. This ensures that password data is secure even if exposed.

Hashing significantly mitigates the risk of credential theft by ensuring that password data remains protected, making it the most effective choice for securing a log-in database against potential breaches.

Hashing is the correct answer because it effectively limits the impact of a database breach by storing only hashed versions of passwords, thereby protecting sensitive credential information. Hashing ensures that even if the log-in database is compromised, the passwords remain secure and difficult for attackers to reverse-engineer.

upvoted 5 times

✉ **a4e15bd** 1 month, 2 weeks ago

What about other information that is stored in a login database like User IDs or emails, security questions and answer, MFA, account status etc. Hashing isn't going to protect those. The only thing hashing protects in case of a breach is passwords only. This is why it can not be the best

choice here. Tokenization is the correct answer.

upvoted 1 times

 **35f7aac** Highly Voted  4 months, 1 week ago

Why not C? What if they do get the data?

Data obfuscation is the process of disguising confidential or sensitive data to protect it from unauthorized access. Data obfuscation tactics can include masking, encryption, tokenization, and data reduction. Data obfuscation is commonly used to protect sensitive data such as payment information, customer data, and health records.

upvoted 5 times

 **jsmthy** 1 week, 4 days ago

Obfuscation is generally correct, but when it comes to passwords and log-in information, it is best to store it in a non-reversible method. Therefore, hashing is the best choice out of the options presented.

upvoted 1 times

 **Ty13** Most Recent  1 week, 4 days ago

Selected Answer: B

B. Hashing

Use Tokenization for payments and credit cards - the data needs to be retrievable, so you'd replace the sensitive info (your CC numbers) with a non-sensitive token to act as a dummy. If you use Apple/Android Pay, the CC you save on your phone is tokenized so the actual numbers can't be stolen.

Hashing is for log-in databases and such where you need to secure the info.

upvoted 2 times

 **RIDA_007** 2 weeks, 1 day ago

The answer is Hashing! The key is Log in and hashing is used for Authentication.

During login, the system combines the entered password with the stored hashes. If the result matches the stored hash, the login is successful

upvoted 1 times

 **SpikeyOG** 3 weeks, 3 days ago

Selected Answer: D

The correct answer is segmentation. From the CompTIA study guide, Segmentation is a method of securing data by dividing networks, data, and applications into isolated components to improve sensitive data protection, limit the impact of a breach, and improve network security

upvoted 3 times

 **nnyankee718** 3 weeks, 4 days ago

Selected Answer: B

log-in database is the key in the question, which is related to hashing

upvoted 3 times

 **17f9ef0** 1 month ago

Selected Answer: A

Answer is A

upvoted 2 times

 **a4e15bd** 1 month, 2 weeks ago

A. Tokenization

Here is why: Tokenization replaces sensitive information with tokens that have no meaningful value outside the tokenization system. The original data is stored securely elsewhere. If a database with tokenized data is breached, the sensitive information remains protected. Keep in mind, hashing only protects stored passwords which is by converting them into a fixed size string of characters that are irreversible, but what about all the other data that is also stored in a login database like usernames or emails, security questions and answers, multi-factor authentication, account status or last login information. Hashing is not going to protect all that.

This is why although hashing is a great choice for securing passwords, it is not the best option considering the context of a login database and hence tokenization is the correct answer!

upvoted 3 times

 **sgtan** 2 months, 1 week ago

Selected Answer: A

For "log-in" database, using tokenization to replace sensitive data with non-sensitive placeholder can secure the log-in data information.

upvoted 2 times

 **sgtan** 2 months, 1 week ago

Selected Answer: D

For "log-in" database, using tokenization to replace sensitive data with non-sensitive placeholder can secure the log-in data information.

upvoted 1 times

 **sgtan** 2 months, 1 week ago

I mean "A. Tokenization". I mis-checked it.

upvoted 1 times

 **Andrewyounan** 2 months, 2 weeks ago

Selected Answer: B

Just for clarification "log-in database" means username and password. Because it took me a minute to process it's not database-SQL
upvoted 2 times

 **Etc_Shadow28000** 3 months, 3 weeks ago

Selected Answer: B

B. Hashing

Hashing is the most likely recommendation for protecting a log-in database. By hashing passwords, the organization ensures that even if the database is breached, the actual passwords are not exposed in plaintext. Hashing converts passwords into a fixed-size string of characters, which is not reversible, thus protecting user credentials.

Therefore, the correct answer is:

B. Hashing
upvoted 2 times

 **drosas84** 3 months, 4 weeks ago

Selected Answer: B

If you said anything besides B, you need to go back and hit the books. Keyword in the question is "log-in". What do you use to login? ID and password right? So hashing your ID and password will turn them into a string of nondescript text that cannot be reversed or decoded. Hashing log-in passwords will limit potential impact.

upvoted 3 times

 **drosas84** 3 months, 4 weeks ago

I'm changing my answer. It should be A tokenization because after reading the question again, it says "log-in database" in the event of a breach. So the breach happened. How can they secure the log-in data information? By using tokenization to replace sensitive data with non-sensitive placeholder. For example, your password can be replaced with random letters or numbers.

upvoted 1 times

 **Shaman73** 4 months ago

Selected Answer: B

B. Hashing
upvoted 2 times

 **jotanyik** 4 months ago

A. Tokenization
upvoted 1 times

 **aed0e20** 4 months, 1 week ago

D. Segmentation

Segmentation involves dividing a network into smaller, isolated segments to limit the potential impact of a breach. By segmenting the network, the organization can contain the breach within a specific segment, preventing it from spreading to other parts of the network, including the log-in database. This approach helps to minimize the scope of the breach and reduce the likelihood of unauthorized access to sensitive data.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 177 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 177

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

- A. Virus
- B. Trojan
- C. Spyware
- D. Ransomware Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by MAKOhunter33333333 at May 30, 2024, 2:54 p.m.

Comments

✉ MAKOhunter33333333 Highly Voted 5 months, 3 weeks ago

Selected Answer: D

Files are populating a message, nothing else would except ransomware to let the victim know. Also, .ryk is a file extension for Ransomware Ryuk
upvoted 9 times

✉ dbrowndiver Highly Voted 3 months, 2 weeks ago

Selected Answer: D

Ransomware encrypts files on a victim's system and displays a message demanding payment to decrypt the files or restore access. It often renames files with specific extensions to indicate encryption. File Extension (.ryk): The presence of a .ryk extension on files is indicative of the Ryuk ransomware, which is known to encrypt files and append this extension to indicate they have been affected. Display Message: Ransomware usually displays a message (ransom note) informing victims of the encryption and providing instructions for paying the ransom. The symptoms described (files with a .ryk extension and a ransom message) strongly suggest a ransomware infection, as this pattern matches known ransomware behaviors, especially related to Ryuk.

upvoted 5 times

 **Shaman73** Most Recent 5 months, 2 weeks ago**Selected Answer: D**D. Ransomware
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 178 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 178

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator is advised that an external web server is not functioning properly. The administrator reviews the following firewall logs containing traffic going to the web server:

Date	Time	SourceIP	SPort	Flag	DestIP	DPort
2023-01-25	01:45:09.102	98.123.45.100	4560	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	95.123.45.101	3361	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	99.123.45.102	3662	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	89.123.45.103	5663	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	98.123.45.104	4064	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	80.123.45.105	4365	SYN	100.50.20.7	443

Which of the following attacks is likely occurring?

- A. DDoS Most Voted
- B. Directory traversal
- C. Brute-force
- D. HTTPS downgrade

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by MAKOhunter33333333 at May 30, 2024, 2:51 p.m.

Comments

✉️ **dbrowndiver** Highly Voted 3 months, 2 weeks ago

[Selected Answer: A](#)

(100.50.20.7) on port 443. This pattern is typical of a SYN flood DDoS attack, where attackers overwhelm a server with SYN requests to deplete its resources.

Simultaneous Connections: All requests occur simultaneously (01:45:09.102), suggesting a coordinated attack, which is a hallmark of DDoS attacks. DDoS is the correct answer because the logs display multiple SYN requests from different IP addresses to the same server in a short time, indicative of a SYN flood DDoS attack aimed at overwhelming the server and causing disruption.

upvoted 5 times

 MAKOhunter33333333 Highly Voted  5 months, 3 weeks ago

Selected Answer: A

DDOS via syn attack

upvoted 5 times

 ezmoney Most Recent  4 months, 2 weeks ago

all of those SYN messages prove this is a DDos attack.

upvoted 3 times

 Shaman73 5 months, 2 weeks ago

Selected Answer: A

A. DDoS

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 179 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 179

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?

- A. Recovery point objective
- B. Mean time between failures
- C. Recovery time objective
- D. Mean time to repair Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [Shaman73](#) at June 6, 2024, 1:06 p.m.

Comments

  [dbrowndiver](#) 3 months, 2 weeks ago

Selected Answer: D

Mean Time to Repair (MTTR) is the correct answer because it directly relates to calculating the time needed to resolve hardware issues and restore the server to full functionality. MTTR is a critical metric for understanding and improving maintenance processes, ensuring efficient recovery from hardware failures.

upvoted 3 times

  [Shaman73](#) 5 months, 2 weeks ago

Selected Answer: D

D. Mean time to repair

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 180 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 180

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

- A. Monitor
- B. Sensor
- C. Audit
- D. Active Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [45fb97](#) at Aug. 7, 2024, 2 a.m.

Comments

 [a4e15bd](#) 2 months ago

D. Active

In active mode, an intrusion prevention system not only monitors network traffic for suspicious activity but also take immediate action to block or mitigate detected threats based on its signatures. This proactive approach ensures that identified threats are automatically blocked or neutralized providing a real-time protection for the environment.

upvoted 4 times

 [45fb97](#) 2 months ago

Selected Answer: D

Active

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 181 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 181

Topic #: 1

[\[All SY0-701 Questions\]](#)

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

A. XDR

B. SPF

C. DLP Most Voted

D. DMARC

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (67%)

D (33%)

by RoRoYourBoat at Aug. 8, 2024, 11:51 p.m.

Comments

✉ March2023 1 month ago

Selected Answer: C

C for sure

upvoted 1 times

✉ Syl0 1 month ago

XDR - Extended Detection and Response

SPF - Sender Policy Framework - for Email to identify who can send to the domain

DLP - Data Loss Prevention

DMARC - similar as SPF, helps with email

upvoted 1 times

✉ Glacier88 1 month, 1 week ago

Selected Answer: C

DLP solutions are specifically designed to identify and prevent the unauthorized movement of sensitive data within and outside an organization. They can monitor data in real-time, detect suspicious activity, and take actions like blocking data transfers or alerting administrators.

upvoted 1 times

 **Ina22** 1 month, 3 weeks ago

DLP is the answer

upvoted 2 times

 **Justhereforcomptia** 1 month, 3 weeks ago

Selected Answer: C

DLP is the right option, it stops data from being exfiltrated from your environment.

upvoted 1 times

 **TheDorse** 1 month, 3 weeks ago

Selected Answer: C

DLP solutions are specifically designed to monitor, detect, and prevent unauthorized data transfers or leaks outside the organization. DLP can identify sensitive data and enforce policies to prevent it from being exfiltrated, making it the most effective solution for mitigating the risk of data exfiltration.

upvoted 1 times

 **RoRoRoYourBoat** 2 months ago

Selected Answer: D

Answer D: EDR is used designed to detect, investigate, and respond to advanced threats to prevent them from spreading across the network.

upvoted 2 times

 **Dunbahhh** 1 month, 4 weeks ago

I think you meant to say question 182 is EDR. EDR isn't an option for this question.

upvoted 5 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 182 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 182

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- A. IDS
- B. ACL
- C. EDR Most Voted
- D. NAC

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Muhammad_Umair](#) at Aug. 11, 2024, 9:55 a.m.

Comments

✉ **Syl0** 1 month ago

IDS - Intrusion Detection System
ACL - Access Control List
EDR - Endpoint Detection and Response
NAC - Network Access Control
upvoted 1 times

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: C

C. EDR (Endpoint Detection and Response) is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network.

EDR solutions provide advanced threat detection, response, and mitigation capabilities for endpoints. They monitor endpoint activities for signs of malicious behavior, provide visibility into threats, and can respond to and contain security incidents.

upvoted 2 times

✉ **Muhammad_Umair** 1 month, 3 weeks ago

Endpoint Detection and Response (EDR) is an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response. D

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 183 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 183

Topic #: 1

[\[All SY0-701 Questions\]](#)

Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?

A. Availability

B. Confidentiality Most Voted

C. Integrity

D. Non-repudiation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  RoRoYourBoat at Aug. 8, 2024, 11:53 p.m.

Comments

 **baronvon** 1 month, 2 weeks ago

Selected Answer: B

B. Confidentiality is the security concept that ensures client files are only accessible to employees who need to know the information and have specified roles in the company. It focuses on protecting information from unauthorized access and ensuring that only those with proper authorization can view or handle the data.

upvoted 1 times

 **RoRoYourBoat** 2 months ago

Selected Answer: B

Confidentiality. This security concept ensures that sensitive information is only accessible to those who are authorized and have a legitimate need to know.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 184 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 184

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes the category of data that is most impacted when it is lost?

- A. Confidential
- B. Public
- C. Private
- D. Critical Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [nesquick0](#) at Aug. 10, 2024, 11:55 a.m.

Comments

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: D

D. Critical data is the category most impacted when it is lost. Critical data is essential for the core operations of an organization, and its loss can lead to significant operational disruptions, financial losses, or damage to the organization's reputation.

upvoted 1 times

✉ **nesquick0** 1 month, 4 weeks ago

Selected Answer: D

D. Critical, because critical data must be always available.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 185 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 185

Topic #: 1

[\[All SY0-701 Questions\]](#)

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

- A. Business email
- B. Social engineering Most Voted
- C. Unsecured network
- D. Default credentials

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (70%)

A (30%)

by [c80f5c5](#) at Aug. 6, 2024, 1:16 p.m.

Comments

✉ [c80f5c5](#) Highly Voted 2 months ago

Selected Answer: A

Business email compromise (BEC) is an email-based social engineering attack

Social engineering refers to all the techniques used to coerce or talk a victim into revealing information that someone can use to perform malicious activities and render an organization or individual vulnerable to further attacks

Answer: A- Business email
upvoted 6 times

✉ [ofolan](#) Highly Voted 1 month ago

Selected Answer: B

B. Social engineering

Social engineering involves manipulating individuals into divulging confidential information or performing actions that compromise security. In this case, the email containing suspicious links is an example of a phishing attempt, where attackers try to deceive the employee into clicking on malicious links that may lead to fraudulent sites or compromise their credentials.

upvoted 5 times

 **Twphill** Most Recent 3 weeks, 6 days ago

Selected Answer: B

Social engineering is an attack vector, while Business email is an attack surface. If it said Business Email Compromise, that would be an attack vector.

upvoted 2 times

 **PAWarriors** 1 month ago

Selected Answer: A

The correct answer is A.

> This is an example of Business Email Compromise (BEC). BEC is a type of phishing attack that usually targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious actions on behalf of the attacker.

In this scenario the email came from human resources, indicating that this is a BEC.

upvoted 1 times

 **Ambaj** 1 month ago

Selected Answer: B

B. Social engineering

upvoted 3 times

 **17f9ef0** 1 month ago

Selected Answer: B

Answer is B

upvoted 2 times

 **a73231e** 1 month, 1 week ago

I think that this question is a bit tricky in its language and its options of available answers. I would agree with A if it actually said "Business Email Compromise" but it simply says business email. B would be the correct answer because it's actually mentioning a form of attack. Attack vector is literally referring to what kind of attack is being shown.

upvoted 1 times

 **Glacier88** 1 month, 1 week ago

Selected Answer: B

Social engineering: This refers to techniques used to manipulate people into performing actions or divulging confidential information. In this case, the attacker is using a legitimate-looking email from human resources to trick the new employee into clicking on malicious links.

Business email compromise (BEC): While BEC can involve emails from legitimate-looking senders, it typically targets high-profile individuals or organizations for financial gain. In this case, the target is a new employee, and the goal seems to be to compromise their system.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 186 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 186

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

- A. SLA Most Voted
- B. MOU
- C. MOA
- D. BPA

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by RoRoYourBoat at Aug. 8, 2024, 11:55 p.m.

Comments

✉ Twphill 3 weeks, 6 days ago

MOU because it "describes the understanding". The question doesn't really ask for a formal document about expected levels of service.
upvoted 4 times

✉ Syl0 1 month ago

MOU - Memorandum of Understanding
MOA - Memorandum of Agreement
SLA - Service Level Agreement
BPA - Business Partner Agreement
upvoted 1 times

✉ baronvon 1 month, 2 weeks ago

Selected Answer: A

A. SLA (Service Level Agreement)

An SLA is a formal document that outlines the expected level of service between a company and a client. It specifies the agreed-upon performance

metrics, such as response times, service availability, and other key aspects of service delivery, including the time needed to provide resources and meet service expectations.

upvoted 1 times

 **RoRoYourBoat** 1 month, 4 weeks ago

Selected Answer: A

A. SLA (Service Level Agreement). An SLA is a formal agreement between a service provider and a client that outlines the specific services to be provided, the expected level of service, and the time frame for delivery

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 187 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 187

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the best type of site for this company?

- A. Cold
- B. Tertiary
- C. Warm
- D. Hot Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  Rj99 at Aug. 15, 2024, 9:56 p.m.

Comments

 **baronvon** 1 month, 2 weeks ago

Selected Answer: D

D. Hot

A hot site is a fully operational backup facility that mirrors the company's primary site and is ready to take over operations immediately in the event of a disaster. It includes all necessary hardware, software, and network configurations, allowing the company to quickly resume normal business activities with minimal downtime.

upvoted 1 times

 **Rj99** 1 month, 3 weeks ago

D. Hot is the answer

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 188 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 188

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?

- A. Deterrent
- B. Corrective
- C. Compensating Most Voted
- D. Preventive

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (62%)

D (38%)

by RoRoYourBoat at Aug. 8, 2024, 11:56 p.m.

Comments

✉️ **RoRoYourBoat** Highly Voted 1 month, 4 weeks ago

Selected Answer: C

C, compensating.
upvoted 5 times

✉️ **BluezClues** Most Recent 3 days, 20 hours ago

Selected Answer: C

The correct answer is C. Compensating.

When a critical legacy server is segmented into a private network, the security control being used is likely **compensating**. This is because the legacy server may not support modern security features, and network segmentation is implemented as a workaround to mitigate risks and protect it from external threats. A compensating control is used to achieve a level of security equivalent to the one required when it is not possible to implement the primary control.

The other options:

- A. Deterrent is designed to discourage malicious actions, such as warning signs or legal warnings.
- B. Corrective is aimed at fixing issues after an incident has occurred.

- D. Preventive is used to stop attacks from happening in the first place, but in this case, segmentation is compensating for the server's inherent vulnerabilities.

Thus, network segmentation is a "compensating" control.

upvoted 1 times

✉ **goku5786** 4 days, 5 hours ago

Selected Answer: D

D. Preventive

upvoted 1 times

✉ **nillie** 4 days, 12 hours ago

Selected Answer: C

The most likely security control being used when a critical legacy server is segmented into a private network is:

C. Compensating

A compensating control is implemented when the primary control (such as patching or updating a legacy server) is not feasible. Segmenting the legacy server into a private network is a compensating control because it mitigates risk by limiting the server's exposure without requiring changes to the server itself, which might not be possible due to its legacy status.

upvoted 1 times

✉ **a0bfa81** 1 week, 2 days ago

Selected Answer: D

Segmenting a critical legacy server into a private network is a preventive security control. It helps to protect the server from unauthorized access and potential attacks by isolating it from the rest of the network, thereby reducing the risk of security breaches. Preventive controls are designed to stop security incidents before they occur.

upvoted 1 times

✉ **jsmthy** 1 week, 2 days ago

Selected Answer: C

compensating, because the best preventative action is to remove the server altogether. You are mitigating the risk by segmenting a vulnerable legacy server.

upvoted 1 times

✉ **chasingsummer** 2 weeks, 6 days ago

Selected Answer: D

D. Preventive

upvoted 1 times

✉ **koala_lay** 2 weeks, 6 days ago

Selected Answer: D

Agree to D. Preventive

Segmenting a critical legacy server into a private network is a preventive measure designed to reduce the risk of unauthorized access and protect sensitive data by controlling traffic to and from the server.

upvoted 1 times

✉ **Glacier88** 1 month, 1 week ago

Selected Answer: D

Preventive controls: These controls are designed to prevent security incidents from occurring in the first place. By segmenting the critical legacy server into a private network, the organization is taking steps to prevent unauthorized access or attacks on that system.

Compensating controls: Compensating controls are used to mitigate the risks associated with other security controls that are not in place or are ineffective. While segmentation could be considered a compensating control in some cases, it's primarily a preventive control in this scenario.

upvoted 1 times

✉ **BugG5** 1 month, 3 weeks ago

D - preventive. Segmentation of a critical legacy server into a private network is primarily aimed at preventing unauthorized access and ensuring the server's security. This control falls under the category of Preventive Controls, as its primary goal is to prevent an incident from occurring. Preventive controls attempt to prevent an incident from occurring by restricting access, implementing barriers, or enforcing policies. In this case, segmenting the critical legacy server into a private network serves as a preventive measure to restrict access and prevent potential security breaches.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 189 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 189

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best describes the practice of researching laws and regulations related to information security operations within a specific industry?

- A. Compliance reporting
- B. GDPR
- C. Due diligence Most Voted
- D. Attestation

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by Kingamj at Aug. 13, 2024, 2:46 p.m.

Comments

✉ nillie 4 days, 12 hours ago

Selected Answer: C

The best term to describe the practice of researching laws and regulations related to information security operations within a specific industry is:

C. Due diligence

Due diligence refers to the process of thoroughly investigating and ensuring that an organization's practices, especially in information security, comply with applicable laws, regulations, and industry standards. It involves identifying and understanding the legal requirements to avoid risks and ensure proper adherence to security policies.

upvoted 1 times

✉ Kingamj 1 month, 3 weeks ago

Selected Answer: C

C. Due diligence.

Due diligence in the context of information security operations involves researching and understanding the laws, regulations, and standards that apply to a specific industry to ensure compliance and manage risks effectively. It's a key practice for identifying and addressing legal and regulatory requirements related to information security.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 190 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 190

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

- A. Reporting structure for the data privacy officer
- B. Request process for data subject access Most Voted
- C. Role as controller or processor
- D. Physical location of the company

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (60%)

B (40%)

by [a4e15bd](#) at Aug. 7, 2024, 3:12 a.m.

Comments

✉️ **User92** 21 hours, 36 minutes ago

Selected Answer: C

Role as controller or processor is crucial because it fundamentally shapes the organization's responsibilities and obligations under data protection laws like the GDPR.

upvoted 1 times

✉️ **nillie** 4 days, 12 hours ago

Selected Answer: C

The most important consideration for an organization to evaluate as it establishes and maintains a data privacy program is:

C. Role as controller or processor

Understanding whether the organization is acting as a data controller or a data processor is crucial because it determines the organization's responsibilities under various data privacy regulations, such as the GDPR. Controllers are responsible for deciding how and why personal data is

processed, while processors handle data on behalf of controllers. Each role has different obligations regarding data protection, subject access requests, and overall compliance.

upvoted 1 times

 **Glacier88** 1 month, 1 week ago

Selected Answer: C

Controller or processor: This is a fundamental distinction in data protection law. Controllers are responsible for determining the purposes and means of processing personal data, while processors process data on behalf of controllers. The organization's role as a controller or processor will significantly impact its data privacy obligations and responsibilities.

Reporting structure for the data privacy officer: While this is important, it's not as crucial as understanding the organization's role as a controller or processor. The reporting structure can be adjusted as needed, but the fundamental legal obligations will remain the same.

Request process for data subject access: This is a critical aspect of data privacy compliance, but it should be established based on the organization's role as a controller or processor and the applicable laws and regulations.

Physical location of the company: While geographic location can be relevant, it's not the most important factor. The organization's role as a controller or processor and the applicable laws and regulations will have a greater impact on its data privacy obligations.

upvoted 1 times

 **Yoming** 1 month, 2 weeks ago

Selected Answer: B

B. This answer is at the heart of the matter. What is an approved, secure process for accessing data. All other answers are secondary or irrelevant

upvoted 1 times

 **nesquick0** 1 month, 3 weeks ago

Selected Answer: B

B. Request Process for data access

upvoted 1 times

 **a4e15bd** 2 months ago

B. Request process for data subject access.

This is one of the most important considerations because it involves how individuals can access, correct or delete their personal data as required by data protection regulations such as GDPR.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 191 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 191

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted. Which of the following logs would the analyst most likely look at next?

- A. IPS
- B. Firewall Most Voted
- C. ACL
- D. Windows security

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [a4e15bd](#) at Aug. 8, 2024, 2:12 a.m.

Comments

✉ **Glacier88** 1 month, 1 week ago

Selected Answer: B

While the endpoint logs themselves are deleted, the firewall logs might still provide valuable information. Firewalls typically record network traffic, including outbound connections, which could help the analyst identify the destination of the suspicious communication. By examining the firewall logs, the analyst might be able to determine the IP address of the command-and-control server and gather other relevant information about the incident.

upvoted 1 times

✉ **Kingamj** 1 month, 3 weeks ago

Selected Answer: B

Since the logs on the endpoint were deleted, the security analyst would likely turn to firewall logs. Firewall logs can provide information about network traffic, including outbound connections that may indicate communication with a command-and-control server. These logs can help the analyst identify suspicious traffic patterns or unauthorized communication that bypassed endpoint defenses.

upvoted 3 times

 **1edea48** 2 months ago

This isn't correct. The answer has to be C. In the question, it specifically states that the logs on the endpoint were deleted. That tells me that someone had access to those logs, which means there might have very well been tampering on the endpoint. The ACL has the ability to show us who was able to access those logs and when they were deleted.

upvoted 2 times

 **850bc48** 2 weeks, 6 days ago

I agree with this, if there's an issue at the endpoint, why wouldn't I check the access logs associated.

upvoted 1 times

 **a4e15bd** 2 months ago

B. Firewall

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 192 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 192

Topic #: 1

[\[All SY0-701 Questions\]](#)

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

A. Business continuity Most Voted

B. Physical security

C. Change management

D. Disaster recovery

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Yoming](#) at Aug. 18, 2024, 12:39 p.m.

Comments

 [a0bfa81](#) 1 week, 3 days ago

Selected Answer: A

A business continuity plan describes how an organization will maintain its operations and continue functioning in the event of a significant disruption or global incident. It covers strategies for ensuring that critical business functions remain operational despite various types of emergencies or disasters. therefore the answer is A.

upvoted 1 times

 [Yoming](#) 1 month, 2 weeks ago

Selected Answer: A

This comprehensive document analyzes risks to business operations. The BCP considers the impact, recovery and mitigation options from a natural disaster.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 193 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 193

Topic #: 1

[\[All SY0-701 Questions\]](#)

A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?

- A. Hot
- B. Cold
- C. Warm Most Voted
- D. Geographically dispersed

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Yoming](#) at Aug. 18, 2024, 12:46 p.m.

Comments

✉ [a4e15bd](#) 1 month, 2 weeks ago

Selected Answer: C

c. warm
upvoted 1 times

✉ [Yoming](#) 1 month, 3 weeks ago

Selected Answer: C

A warm site serves as a compromise between an immediate failover resource and an empty shell that must be built
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 194 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 194

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

- A. Virtualization and isolation of resources Most Voted
- B. Network segmentation
- C. Data encryption
- D. Strong authentication policies

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (67%) C (22%) 11%

by [a4e15bd](#) at Aug. 8, 2024, 2:24 a.m.

Comments

✉ **nillie** 4 days, 12 hours ago

Selected Answer: A

The security team should ensure that all of the following are in place, but the most comprehensive answer that addresses cloud-based services is:

- A. Virtualization and isolation of resources

In a cloud-based environment, virtualization and isolation of resources are critical to maintaining security best practices. Virtualization allows multiple workloads to run on the same physical infrastructure while keeping them isolated from each other, which is a foundational practice in cloud environments to prevent data leakage or unauthorized access between different tenants or applications.

upvoted 1 times

✉ **Glacier88** 1 month, 1 week ago

Selected Answer: A

Virtualization and isolation of resources: This ensures that each application or tenant within the cloud environment is running in its own isolated virtual environment, preventing unauthorized access or interference from other users.

Network segmentation: While network segmentation is a valuable security measure, it's not as directly related to the security of the on-premises software application itself. It's more about protecting the overall network infrastructure.

Data encryption: Data encryption is crucial for protecting sensitive data both at rest and in transit, but it's not the primary concern for ensuring a secure cloud-based environment.

Strong authentication policies: Strong authentication policies are essential for controlling access to the cloud environment, but they don't address the isolation and protection of resources within that environment.

upvoted 2 times

 **Yoming** 1 month, 2 weeks ago

Selected Answer: B

Network segmentation would provide a barrier between the hosting software and internal company resources

upvoted 1 times

 **RobJob** 2 weeks ago

I'm not sure how network segmentation can be applicable when it is a cloud environment.

upvoted 1 times

 **EfaChux** 1 month, 3 weeks ago

Selected Answer: C

Setting up a private cloud means your data will be traveling over the internet, encryption seems like a best practice to me when compared to virtualization and isolation which could already be in place for the on-premise architecture

upvoted 2 times

 **Crucible_Bro** 1 month, 3 weeks ago

Selected Answer: A

I'm not overly smart about this type of thing, but I *feel* like this is one of those trick questions. In order to get any sort of cloud services up you'll need virtualization. The isolation of resources may be part of the security aspect but I am not entirely sure. D is probably a stronger answer but I don't necessarily disagree with A.

upvoted 3 times

 **a4e15bd** 1 month, 4 weeks ago

D. Strong authentication policies. Ensuring a strong user authentication is crucial to prevent unauthorized access to the cloud environment. This forms the first line of defense in securing the system.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 195 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 195

Topic #: 1

[\[All SY0-701 Questions\]](#)

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

- A. End user training
- B. Policy review
- C. URL scanning Most Voted
- D. Plain text email

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (50%)

C (50%)

by Ina22 at Aug. 10, 2024, 4:41 p.m.

Comments

✉️ nillie 4 days, 12 hours ago

Selected Answer: A

The security practice that helped the manager identify the attack is:

- A. End user training

End user training teaches employees how to recognize phishing attempts and other malicious activities. In this case, the manager's awareness of hovering over links to check for suspicious URLs before clicking is a direct result of effective security awareness training. This is a key aspect of preventing social engineering attacks, like phishing.

upvoted 1 times

✉️ jsmthy 1 week, 2 days ago

Selected Answer: C

The manager is scanning a URL. End-user training may make the practice of checking URLs more prevalent, but it is not the security practice being demonstrated.

upvoted 1 times

 **ChillingSpree** 3 days, 22 hours ago

URL Scanning is something you'd typically set up with a NGFW. It is a technology and not something a human does in the context of this subject.

upvoted 1 times

 **rabid_adobo** 1 month, 1 week ago

A. GPT

upvoted 1 times

 **Ina22** 1 month, 3 weeks ago

A. End user training

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 196 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 196

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

- A. Validate the code signature.
- B. Execute the code in a sandbox.
- C. Search the executable for ASCII strings.
- D. Generate a hash of the files.

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [a4e15bd](#) at Aug. 8, 2024, 2:32 a.m.

Comments

[a4e15bd](#) Highly Voted 1 month, 4 weeks ago

A. Validate the code signature

Code signing is a process where the software vendor signs the executable code with a digital certificate. This certificate verifies the identity of the software vendor and ensures that the code has not been altered since it was signed. By validating the code signature, the company can confirm the authenticity and integrity of the software.

upvoted 6 times

[nillie](#) Most Recent 4 days, 12 hours ago

Selected Answer: A

The best way for the company to confirm that the software came from the vendor is:

A. Validate the code signature.

Code signing uses digital signatures to confirm the identity of the software publisher and ensure that the code has not been altered since it was signed. By validating the code signature, the company can verify that the software is authentic and comes from the trusted vendor.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 197 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 197

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

- A. Installing HIDS on the system
- B. Placing the system in an isolated VLAN Most Voted
- C. Decommissioning the system
- D. Encrypting the system's hard drive

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (80%)

C (20%)

by qacollin at Aug. 7, 2024, 6:30 p.m.

Comments

✉ Dharmesh16 Highly Voted 1 month, 4 weeks ago

Selected Answer: B

techniques would increase "enterprise" security. you can use system but system can't connect with other devices on network
upvoted 6 times

✉ a4e15bd Highly Voted 1 month, 4 weeks ago

B. Placing the system in an isolated VLAN

Give that the system is critical for processing customer transactions, decommissioning immediately might impact business continuity. The next best approach is to place the system in an isolated VLAN.

upvoted 6 times

✉ nillie Most Recent 4 days, 12 hours ago

Selected Answer: B

The best technique to increase enterprise security in this situation is:

B. Placing the system in an isolated VLAN

By placing the system in an isolated VLAN, the organization can reduce the risk of the outdated system being exploited by limiting its network exposure and controlling access to and from the critical system. This helps to minimize the impact that vulnerabilities in the end-of-life operating system could have on the broader network.

upvoted 1 times

Glacier88 1 month, 1 week ago

Selected Answer: B

Placing the system in an isolated VLAN: This will physically separate the critical system from the rest of the network, reducing the risk of unauthorized access or attacks.

Installing HIDS on the system: While an HIDS can detect and alert on suspicious activity, it might not be enough to mitigate the risks associated with an end-of-life operating system, which lacks security updates and patches.

Decommissioning the system: This is a potential solution if the system can be replaced with a more secure alternative. However, if the system is critical for business operations, decommissioning it might not be feasible.

Encrypting the system's hard drive: Encryption can protect the data stored on the system, but it doesn't address the security vulnerabilities associated with an end-of-life operating system.

upvoted 1 times

Migzz 1 month, 3 weeks ago

Why would you "Decommission the system" when it is critical for transitions? The answer is B, Isolate it until you're ready to make the relevant changes or ready to replace it.

upvoted 4 times

qacollin 1 month, 4 weeks ago

Selected Answer: C

Yes, decommissioning the system is generally the most effective approach for addressing the security risks associated with running an end-of-life operating system.

GPT

upvoted 2 times

Justhereforcomptia 1 month, 3 weeks ago

You cannot do this as it's business critical

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 198 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 198

Topic #: 1

[\[All SY0-701 Questions\]](#)

The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?

- A. Penetration test
- B. Internal audit Most Voted
- C. Attestation
- D. External examination Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

B (50%)

D (50%)

by [a4e15bd](#) at Aug. 8, 2024, 2:48 a.m.

Comments

nillie 4 days, 12 hours ago

Selected Answer: B

The CISO should use:

B. Internal audit

An internal audit is a structured assessment of the company's security policies, processes, and controls to ensure they meet both internal standards and external regulatory requirements. This will help the CISO understand how well the company's security policies align with the requirements imposed by regulators.

upvoted 2 times

Ty13 1 week, 2 days ago

Selected Answer: B

B. Internal Audit

I know people want to select D because... it sounds right. External audit to compare against external regulations. But there's a part being overlooked: 'would like to gain an understanding'. Which you don't NEED a third party to confirm, because the company already KNOWS those regulations. But you WOULD need an external audit if there was a large breach and the regulatory agencies wanted to know how it happened.

What is being asked, effectively, is "Can an internal audit team verify that we meet external regulations?"

upvoted 2 times

RIDA_007 2 weeks ago

Selected Answer: D

An external examination (also known as an external audit or external review)

upvoted 1 times

NONS3c 2 weeks, 6 days ago

Selected Answer: B

even GPT Said

upvoted 1 times

Cyber_Texas 1 month ago

D external examination is best here

upvoted 1 times

myazureexams 1 month, 1 week ago

Selected Answer: D

It is D period. And for the exam, make the association "External with External" DONE

upvoted 4 times

Glacier88 1 month, 1 week ago

Selected Answer: D

External examination: An external examination, conducted by an independent third party, can provide an objective assessment of the company's security policies and practices against external regulatory requirements. This can help the CISO identify any gaps or areas for improvement.

Penetration test: While penetration tests can identify vulnerabilities in the company's security infrastructure, they don't directly assess compliance with external regulations.

Internal audit: Internal audits can assess the company's adherence to internal policies and procedures, but they might not provide a comprehensive view of compliance with external regulations.

Attestation: Attestation is a formal process of providing assurance about a specific claim or assertion. While it might involve compliance with regulations, it doesn't necessarily provide a full assessment of the company's security policies and practices.

upvoted 1 times

baronvon 1 month, 1 week ago

Selected Answer: B

B. Internal audit

An internal audit allows the CISO to assess how the company's security policies align with the requirements imposed by external regulators. This process involves reviewing and evaluating the company's policies, procedures, and controls to ensure compliance with regulatory standards.

upvoted 2 times

Dlove 1 month, 3 weeks ago

Selected Answer: D

D. External Examination

An external examination involves a review or assessment conducted by an independent third party, often to evaluate how an organization's policies, procedures, and practices align with regulatory requirements or industry standards. This process is crucial for identifying gaps between the company's internal security policies and the requirements imposed by external regulators. It provides the CISO with an unbiased understanding of the organization's compliance status.

upvoted 1 times

a4e15bd 1 month, 4 weeks ago

B. Internal Audit

An internal audit involves a thorough review of the company's policies and procedures to ensure they meet the regulatory requirements and industry standards.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 199 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 199

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

- A. Espionage
- B. Data exfiltration
- C. Nation-state attack
- D. Shadow IT Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by MarDog at Aug. 13, 2024, 8:42 p.m.

Comments

✉ nillie 4 days, 12 hours ago

Selected Answer: D

The scenario described is:

D. Shadow IT

Shadow IT refers to the use of technology, systems, or services by employees without the approval or knowledge of the IT department. In this case, the research and development department is bypassing the company's VPN, potentially using unauthorized methods to access company-related services and systems. This can pose security risks, as these systems may not adhere to the company's security policies and protocols.

upvoted 1 times

✉ jsmthy 1 week, 2 days ago

Selected Answer: D

Using unauthorized software, eh Dave? The scenario may imply the use of an unofficial VPN for the sake of carrying out Espionage or Data Exfiltration, but there is no sign of it. The threat is the VPN rather the user or the data. Additionally, it doesn't seem like the nation-state attack

would fit since the hallmarks of such an attack aren't present (lots of funding, firmware-level bugs, unique spyware, social engineering).
upvoted 1 times

 **MarDog** 1 month, 3 weeks ago

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 200 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 200

Topic #: 1

[\[All SY0-701 Questions\]](#)

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT Most Voted

- B. Insider threat
- C. Data exfiltration
- D. Service disruption

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [Dlove](#) at Aug. 9, 2024, 6:21 p.m.

Comments

  [Dlove](#) Highly Voted 1 month, 4 weeks ago

Selected Answer: A

A. Shadow IT

Shadow IT is when an employee uses information technology (IT) systems without the approval of an organization's IT department.
upvoted 6 times

  [FrozenCarrot](#) Most Recent 4 weeks ago

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 201 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 201

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

- A. To track the status of patching installations Most Voted
- B. To find shadow IT cloud deployments
- C. To continuously monitor hardware inventory
- D. To hunt for active attackers in the network

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [a4e15bd](#) at Aug. 8, 2024, 2:57 a.m.

Comments

  [a4e15bd](#) Highly Voted  2 months ago

Answer A is correct:

Daily vulnerability scans help ensure that all the endpoints are up to date with security patches and identify any vulnerabilities that may have been introduced due to unpatched software. This regular scanning helps in monitoring and verifying the effectiveness of patch management process.

upvoted 5 times

  [FrozenCarrot](#) Most Recent  4 weeks ago

Selected Answer: A

Results of vulnerability scans are CVEs.

upvoted 1 times

  [qacollin](#) 1 month, 4 weeks ago

Selected Answer: A

A. GPT

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 202 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 202

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is classified as high availability in a cloud environment?

- A. Access broker
- B. Cloud HSM
- C. WAF
- D. Load balancer Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [a4e15bd](#) at Aug. 8, 2024, 3:01 a.m.

Comments

  [FrozenCarrot](#) 4 weeks ago

Selected Answer: D

Load balancer distribute traffic between servers, guarantee availability.
upvoted 1 times

  [qacollin](#) 1 month, 4 weeks ago

Selected Answer: D

D. GPT!
upvoted 2 times

  [a4e15bd](#) 2 months ago

D
Load balancer distributes incoming network traffic across multiple servers or instances ensuring that no single server becomes overwhelmed and helps maintain the availability of applications and services.
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 203 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 203

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following security measures is required when using a cloud-based platform for IoT management?

- A. Encrypted connection Most Voted
- B. Federated identity
- C. Firewall
- D. Single sign-on

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [a4e15bd](#) at Aug. 8, 2024, 3:11 a.m.

Comments

✉ [a4e15bd](#) Highly Voted 2 months ago

A

IOT devices often transmit sensitive data over networks and encryption ensures that this data is securely transmitted and protected from interception or tampering.

upvoted 5 times

✉ [qacollin](#) Most Recent 2 months ago

Selected Answer: A

A. GPT

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 204 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 204

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

- A. Unidentified removable devices Most Voted
- B. Default network device credentials
- C. Spear phishing emails
- D. Impersonation of business units through typosquatting

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [qacollin](#) at Aug. 9, 2024, 3:53 p.m.

Comments

✉ [qacollin](#) 1 month, 4 weeks ago

Selected Answer: A

A. GPT

upvoted 1 times

✉ [Lykkefcode](#) 2 weeks, 5 days ago

I think is incorrect. The question refers to an 'attack vector,' but option A describes an 'attack surface.' In my opinion, the correct answer should be option C. Spear phishing emails.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 205 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 205

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking Most Voted
- D. Tokenization

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [8 qacollin](#) at Aug. 9, 2024, 3:53 p.m.

Comments

✉️ **rrynzon** 3 weeks, 2 days ago

this is wrong, the correct answer is "tokenization"

upvoted 1 times

✉️ **850bc48** 2 weeks, 6 days ago

no because tokenization is basically when a randomly generated number is created in lieu of your actual card number, so that if your card is intercepted during a transaction, the attack doesn't get your actual number.

upvoted 2 times

✉️ **jafyyy** 1 month, 2 weeks ago

C. Masking - is used to protect sensitive information while still allowing authorized users to view a portion of the data like a credit card number.
upvoted 3 times

✉️ **Sol_tyty** 1 month, 2 weeks ago

GPT!!!

upvoted 2 times

 **qacollin** 1 month, 4 weeks ago

Selected Answer: C

C . GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 206 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 206

Topic #: 1

[\[All SY0-701 Questions\]](#)

The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?

A. Fines Most Voted

B. Reputational damage

C. Sanctions

D. Contractual implications

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by qacolin at Aug. 9, 2024, 3:55 p.m.

Comments

✉ **jsmthy** 1 week, 3 days ago

Selected Answer: A

Hit the executives where it hurts most.

upvoted 1 times

✉ **Glacier88** 1 month, 1 week ago

Selected Answer: A

Fines: Under GDPR, fines can be substantial, reaching up to 4% of a company's global annual turnover. This makes them a very direct and immediate consequence of non-compliance, emphasizing the financial risk associated with it.

Reputational damage: While this remains a significant concern, it may not be as immediately quantifiable as fines. Fines can serve as a concrete measure of the financial impact of non-compliance.

Sanctions: Sanctions are typically imposed by governments as a result of serious violations of laws or international agreements. They are not directly related to data privacy compliance.

Contractual implications: While non-compliance may have contractual implications, especially if there are specific data privacy clauses in contracts with customers or partners, it's not necessarily the most immediate or significant consequence.

upvoted 2 times

 **jafyyy** 1 month, 2 weeks ago

A. Fines are financial consequence of non-compliance with data privacy regulations

upvoted 1 times

 **qacollin** 1 month, 4 weeks ago

A. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 207 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 207

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following alert types is the most likely to be ignored over time?

- A. True positive
- B. True negative
- C. False positive Most Voted
- D. False negative

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [qacollin](#) at Aug. 9, 2024, 3:55 p.m.

Comments

  [jafyyy](#) 1 month, 2 weeks ago

C. False Positive - triggered when an event is NOT actually a threat.

True Positive - an actual threat

True Negative - no threat

False Negative - an actual threat isn't detected, dangerous type since threats go unnoticed.

upvoted 1 times

  [qacollin](#) 2 months ago

Selected Answer: C

C. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 208 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 208

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

- A. Memory injection
- B. Race condition
- C. Side loading
- D. SQL injection

[Hide Answer](#)

Suggested Answer: A

by [a4e15bd](#) at Aug. 8, 2024, 3:29 p.m.

Comments

✉ [a4e15bd](#) Highly Voted 1 month, 4 weeks ago

A is correct.

Memory injection allows the attackers to inject malicious code directly into the memory of a running process which can then be used to execute arbitrary commands or generate unauthorized network traffic.

Race Condition refers to two processes competing to modify the same resource which can lead to unpredictable behavior but is less likely to cause abnormal outbound traffic.

Side Loading refers to loading a malicious DLL into a legitimate process.

SQL injection involves injecting malicious SQL code into a database and is primarily concerned with database manipulation rather than generating outbound network traffic.

upvoted 10 times

✉ [Exemplary](#) 16 hours, 34 minutes ago

Just a quick note: Your definition of side loading is incorrect. Side loading involves installing software from third party or unauthorized sources, typically involving mobile devices. What you described is actually a DLL Injection.

upvoted 2 times

✉ [jafyyy](#) Most Recent 1 month, 2 weeks ago

A. Memory Injection

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 209 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 209

Topic #: 1

[\[All SY0-701 Questions\]](#)

An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

- A. Asset inventory Most Voted
- B. Network enumeration
- C. Data certification
- D. Procurement process

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by qacollin at Aug. 9, 2024, 4:07 p.m.

Comments

✉ PAWarriors 1 month ago

Selected Answer: A

Asset inventory is a list of all hardware, software, and systems within the organization. Maintaining an up-to-date asset inventory allows the systems administrator to easily identify which systems are running the critical application and need the patch
upvoted 1 times

✉ jafyyy 1 month, 2 weeks ago

A. Asset Inventory provides complete list of assets that need to be managed.
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 210 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 210

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following should a security operations center use to improve its incident response procedure?

A. Playbooks Most Voted

B. Frameworks

C. Baselines

D. Benchmarks

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qacollin](#) at Aug. 9, 2024, 4:08 p.m.

Comments

  **jafyyy** 1 month, 2 weeks ago

A. Playbooks
Its a step by step procedure outlining how to respond to specific types of incidents.
upvoted 3 times

  **StringerBarksdale** 1 month, 2 weeks ago

The answer is B
upvoted 2 times

  **qacollin** 2 months ago

Selected Answer: A
A. GPT
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 211 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 211

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

- A. Continuity of operations
- B. Capacity planning
- C. Tabletop exercise Most Voted
- D. Parallel processing

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [qacollin](#) at Aug. 9, 2024, 4:12 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

C. Tabletop exercise
upvoted 1 times

✉ **qacollin** 2 months ago

Selected Answer: C
C . GPT
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 212 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 212

Topic #: 1

[\[All SY0-701 Questions\]](#)

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

- A. Scalability
- B. Availability Most Voted
- C. Cost
- D. Ease of deployment

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qacollin](#) at Aug. 9, 2024, 4:13 p.m.

Comments

 [ServerBrain](#) 1 month ago

Selected Answer: B

to report health emergencies...

upvoted 1 times

 [jafyyy](#) 1 month, 2 weeks ago

B. Availability is crucial for patient safety in health emergencies.

upvoted 1 times

 [qacollin](#) 1 month, 4 weeks ago

B. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 213 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 213

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following agreement types defines the time frame in which a vendor needs to respond?

- A. SOW
- B. SLA Most Voted
- C. MOA
- D. MOU

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [qacollin](#) at Aug. 9, 2024, 4:13 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago
B. SLA (Service Level Agreement)
upvoted 1 times

✉ **qacollin** 2 months ago
Selected Answer: B
B. GPT
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 214 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 214

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a feature of a next-generation SIEM system?

- A. Virus signatures
- B. Automated response actions Most Voted
- C. Security agent deployment
- D. Vulnerability scanning

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [qacollin](#) at Aug. 9, 2024, 4:14 p.m.

Comments

  [FrozenCarrot](#) 3 weeks, 6 days ago

Selected Answer: B

next-gen SIEM platforms can dynamically analyze vast datasets in real time, enabling the identification of subtle, evolving threats that traditional systems might overlook.

upvoted 1 times

  [jafyyy](#) 1 month, 2 weeks ago

B. Automated Response Actions

upvoted 1 times

  [qacollin](#) 1 month, 4 weeks ago

Selected Answer: B

B. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 215 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 215

Topic #: 1

[\[All SY0-701 Questions\]](#)

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Choose two.)

A. Preventive

B. Deterrent Most Voted

C. Corrective

D. Directive

E. Compensating

F. Detective Most Voted

[Hide Answer](#)

Suggested Answer: BF

Community vote distribution

BF (70%)

BD (30%)

by [CJfromVA](#) at Aug. 10, 2024, 5:34 p.m.

Comments

✉ [internslayer](#) Highly Voted 1 month, 3 weeks ago

Selected Answer: BF

I believe it is B and F because the CCTV will give you the ability to monitor the data center and its presence and signs are a deterrent.
upvoted 6 times

✉ [User92](#) Most Recent 1 day, 21 hours ago

Selected Answer: BF

Deterrent: The signs serve as a deterrent by discouraging potential intruders or malicious activities through the awareness of surveillance.
Detective: The CCTV system itself acts as a detective control by monitoring and recording activities, which can be reviewed to detect and investigate incidents.
upvoted 1 times

 **baronvon** 1 month, 1 week ago

Selected Answer: BD

It's B and D

upvoted 2 times

 **Hayder81** 1 month, 2 weeks ago

I believe it is B and F

upvoted 1 times

 **CJfromVA** 1 month, 3 weeks ago

Selected Answer: BD

I believe and what I will go with.

B. Deterrent: The CCTV system and signs serve to deter potential unauthorized activities or behavior by making individuals aware that they are being monitored. The idea is that the possibility of being recorded will discourage malicious or inappropriate actions.

D. Directive: Posting signs about being filmed can also be considered a directive control. It communicates rules or policies to individuals about their behavior and the monitoring system in place, guiding how they should act within the data center.

upvoted 1 times

 **EfaChux** 1 month, 3 weeks ago

CCTV is detective, its there to detect incidents. Some CCTV are hidden so people may not even know its there so it doesn't stop them but it can see them and alert the security team.

upvoted 2 times

 **baronvon** 1 month, 1 week ago

The question says that they posts several signs about the possibility of being filmed, people may not know but they will act differently knowing they are being recorded

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 216 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 216

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following examples would be best mitigated by input sanitization?

- A. **Most Voted**
- B. nmap - 10.11.1.130
- C. Email message: "Click this link to get your free gift card."
- D. Browser message: "Your connection is not private."

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by Sole_tone at Aug. 8, 2024, 5:51 p.m.

Comments

✉ CJfromVA **Highly Voted** 2 months ago

Selected Answer: A

This question is the same on exam topics 601 #604 - The answer is in fact A and it shows "A. <script>alert('Warning!');</script>"

upvoted 11 times

✉ Sole_tone **Highly Voted** 2 months ago

the Answer is A but it doesn't show anything but what it should be showing is something like this.
<script>alert('Warning!');</script>

If you look in the 601 study guide that's what it shows

upvoted 7 times

 **jsmthy** Most Recent 1 week, 3 days ago**Selected Answer: A**

Your browser is like Ron Burgundy. Whatever shows up on the HTML file, it is going to read it and execute it.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 217 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 217

Topic #: 1

[\[All SY0-701 Questions\]](#)

An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

- A. Smishing
- B. Disinformation
- C. Impersonating Most Voted
- D. Whaling

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by Migzz at Aug. 10, 2024, 8:23 p.m.

Comments

✉ BugG5 Highly Voted 1 month, 3 weeks ago

Selected Answer: C

Impersonating involves pretending to be someone else, in this case, the Chief Executive Officer (CEO), to deceive the employee into taking a specific action (buying gift cards). The attacker is leveraging the authority and trust associated with the CEO's position to manipulate the employee.

Whaling: This phishing attack targets high-profile individuals, such as executives.

An attacker is 'posing' and not 'targeting' a CEO. Therefore its C

upvoted 8 times

✉ Glacier88 Most Recent 1 month, 1 week ago

Selected Answer: C

Smishing: Phishing via SMS messages.

Disinformation: Spreading false information.

Impersonating: Pretending to be someone else.

Whaling: Targeting high-profile individuals.

Given that the attacker is posing as the CEO, impersonating is the most accurate answer.

upvoted 2 times

 **Hayder81** 1 month, 2 weeks ago

Impersonating C

upvoted 1 times

 **jafyyy** 1 month, 2 weeks ago

C. Impersonating -

Given the target is an employee rather than a high-profile executive, most accurate technique used is Impersonating.

upvoted 1 times

 **ExamTopics2040** 1 month, 2 weeks ago

Whaling targets high-profile individuals within an organization, such as executives, CEOs, CFOs, or other senior management. so C is best answer

upvoted 2 times

 **Migzz** 1 month, 4 weeks ago

Answer is D whaling. Only because it involves a high-profile executive. If you look up the definition of whaling and compare it to C, whaling is a more suitable answer from a security plus exam standpoint.

upvoted 3 times

 **RIDA_007** 2 weeks ago

Posing as "CEO" the attacker pretending to be the CEO. Hence it's C.

upvoted 1 times

 **RobJob** 2 weeks, 1 day ago

Whaling is targeting high-profile executives not impersonating the,

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 218 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 218

Topic #: 1

[\[All SY0-701 Questions\]](#)

After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

A. False positive Most Voted

B. False negative

C. True positive

D. True negative

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qacollin](#) at Aug. 9, 2024, 4:21 p.m.

Comments

 [rrynzon](#) 3 weeks, 2 days ago

False Positive - Normal or expected activity is incorrectly identified as abnormal or unexpected. False Negative - Abnormal or unexpected activity is incorrectly identified as normal or expected. Therefore, B is the correct answer.

upvoted 1 times

 [jafyyy](#) 1 month, 2 weeks ago

A. False Positive - an alert for an event that is not a threat.

upvoted 1 times

 [qacollin](#) 1 month, 4 weeks ago

Selected Answer: A

A. GPT

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 219 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 219

Topic #: 1

[\[All SY0-701 Questions\]](#)

A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would best mitigate this type of attack?

- A. Load balancer
- B. Port security
- C. IPS
- D. NGFW

[Hide Answer](#)

Suggested Answer: B

by [Muhammad_Umair](#) at Aug. 14, 2024, 10:50 a.m.

Comments

Muhammad_Umair 1 month, 3 weeks ago

Port security is a feature on network switches that allows you to limit the number of MAC addresses that can be learned on a specific port. If the limit is exceeded, the switch can take predefined actions such as shutting down the port, restricting traffic, or generating alerts. This effectively prevents attackers from overwhelming the switch with a large number of MAC addresses, which could otherwise cause the switch to behave like a hub, sending traffic to all ports and potentially exposing sensitive data. (B)

upvoted 6 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 220 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 220

Topic #: 1

[\[All SY0-701 Questions\]](#)

A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

- A. SQLi
- B. Cross-site scripting
- C. Jailbreaking Most Voted
- D. Side loading

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (80%)

D (20%)

by Neno232 at Aug. 15, 2024, 2:56 p.m.

Comments

✉ NONS3c 3 weeks ago

Selected Answer: C

keyword said "enable new feature " for doing this action you should jailbreaking the mobile or root
upvoted 1 times

✉ 2fd1029 3 weeks, 2 days ago

Selected Answer: C

I think the answer is C, even though I first thought D. The reason I changed my mind is because at the end they also mention enabling new features, which sideloading doesn't necessarily let you do. Jailbreaking does.
upvoted 1 times

✉ MsZrogas 1 month ago

You must jailbreak the phone first before you can sideload apps.
upvoted 1 times

 **FrozenCarrot** 3 weeks, 6 days ago

No, you dont have to, for example, you can sideload apps by ADB on an android phone
upvoted 2 times

 **FrozenCarrot** 3 weeks ago

Sideload can also allow the installation of unauthorized apps, but jailbreaking typically provides deeper access to the system for more extensive modifications.
So i will go for C
upvoted 1 times

 **Sama001** 1 month, 1 week ago

Selected Answer: D

Side Loading: The process of installing applications on a device without the use of official software distribution channels.
upvoted 1 times

 **850bc48** 2 weeks, 6 days ago

to enable this you would need to jail break the device first.
upvoted 1 times

 **jafyyy** 1 month, 2 weeks ago

Jailbraking
upvoted 1 times

 **Neno232** 1 month, 3 weeks ago

Selected Answer: C
Jailbreaking is the answer.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 221 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 221

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following phases of an incident response involves generating reports?

- A. Recovery
- B. Preparation
- C. Lessons learned Most Voted
- D. Containment

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [qacollin](#) at Aug. 9, 2024, 4:59 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

C. Lessons Learned - focused on documentation and learning from the incident to improve future responses.
upvoted 1 times

✉ **qacollin** 2 months ago

Selected Answer: C
C. GPT
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 222 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 222

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following methods would most likely be used to identify legacy systems?

- A. Bug bounty program
- B. Vulnerability scan
- C. Package monitoring
- D. Dynamic analysis

[Hide Answer](#)

Suggested Answer: B

by [qacollin](#) at Aug. 9, 2024, 5 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

C. Vulnerability Scan - can identify legacy systems as it can include outdated software versions and unpatched systems.
upvoted 1 times

✉ **Cyberity** 1 month, 3 weeks ago

Shouldnt the answer be Package Monitoring ?
upvoted 1 times

✉ **jafyyy** 1 month, 2 weeks ago

Package monitoring is more focused on the status of individual software packages rather than identifying entire systems that are outdated or considered legacy.
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 223 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 223

Topic #: 1

[\[All SY0-701 Questions\]](#)

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

- A. Proxy server
- B. NGFW
- C. VPN
- D. Security zone

[Hide Answer](#)

Suggested Answer: C

by Rj99 at Aug. 16, 2024, 1:17 a.m.

Comments

jafyyy 1 month, 2 weeks ago

C. VPN - provides secure remote access assuring data transmitted between remote employees and company resources is encrypted and protected from interception.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 224 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 224

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company allows customers to upload PDF documents to its public e-commerce website. Which of the following would a security analyst most likely recommend?

- A. Utilizing attack signatures in an IDS
- B. Enabling malware detection through a UTM
- C. Limiting the affected servers with a load balancer
- D. Blocking command injections via a WAF

[Hide Answer](#)

Suggested Answer: B

by [a4e15bd](#) at Aug. 8, 2024, 5:07 p.m.

Comments

[a4e15bd](#) Highly Voted 2 months ago

B

PDFs can be used to deliver malware such as embedded scripts or exploits. Enabling malware detection through a UTM helps to scan and block malicious content within uploaded files before they reach the server.

upvoted 7 times

[jafyyy](#) Most Recent 1 month, 2 weeks ago

B. Enabling malware detection through a UTM - can scan uploaded files for malicious content.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 225 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 225

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?

- A. To reduce implementation cost
- B. To identify complexity
- C. To remediate technical debt
- D. To prevent a single point of failure Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [a4e15bd](#) at Aug. 21, 2024, 1:44 a.m.

Comments

Sol_tyty Highly Voted 1 month, 2 weeks ago

NO GPT COMMENT!!!! HALLELUJAH!!!!!!
upvoted 6 times

Sama001 Most Recent 1 month, 1 week ago

Selected Answer: D
D. To prevent a single point of failure
Other team members knowing how it works eliminates reliance on a single employee in case of script failure.
upvoted 1 times

c469c8e 1 month, 1 week ago

Script is still single point of failure
upvoted 1 times

jafyyy 1 month, 2 weeks ago

D. To prevent a single point of failure - ensures continuity and reduces reliance on any single individual.
upvoted 1 times

a4e15bd 1 month, 2 weeks ago

Selected Answer: D

D. Prevent Single Point of Failure
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 226 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 226

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

- A. Microservices
- B. Containerization Most Voted
- C. Virtualization
- D. Infrastructure as code

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [a4e15bd](#) at Aug. 8, 2024, 5:38 p.m.

Comments

✉ **a4e15bd** Highly Voted 2 months ago

B

Containerization allows multiple applications or services to run in isolated environments on the same underlying OS. Unlike, virtualization where each VM runs its own OS, containers share the host OS kernel but keep the applications isolated from one another. This significantly reduces the number of operating systems required while maintaining security and isolation between applications.

upvoted 5 times

✉ **jsmthy** Most Recent 1 week, 3 days ago

Selected Answer: B

Containerization allows fewer Operating Systems.

Sometimes this question comes with fewer physical servers, resulting in virtualization.

Take steps to ensure you read the question carefully.

upvoted 1 times

✉ **jafyyy** 1 month, 2 weeks ago

B. Containerization - is more appropriate as it allows multiple applications to run on a single OS, whereas virtualization involves running multiple OS on same physical hardware.

upvoted 1 times

 **scoobysnack209** 1 month, 2 weeks ago

B. Containerization like "docker" container.

upvoted 1 times

 **suleman1000** 1 month, 2 weeks ago

C. Virtualization

Explanation of the MCQ:

Virtualization is a technology that allows multiple virtual machines (VMs) to run on a single physical server's hardware. Each VM can run its own operating system and applications, effectively reducing the number of physical servers required and thus the number of individual operating systems managed in a physical sense. By using virtualization, a company can consolidate its server infrastructure, leading to reduced hardware costs, easier management, and potentially enhanced security due to a smaller physical footprint and centralized management.

upvoted 1 times

 **Justhereforcomptia** 1 month, 2 weeks ago

Virtualization doesn't reduce the number of operating systems.

Keyword "reduce the number of individual operating systems"

B is the correct answer, Containerization

upvoted 5 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 227 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 227

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Choose two.)

- A. Disable default accounts. Most Voted
- B. Add the server to the asset inventory.
- C. Remove unnecessary services. Most Voted
- D. Document default passwords.
- E. Send server logs to the SIEM.
- F. Join the server to the corporate domain.

[Hide Answer](#)

Suggested Answer: AC

Community vote distribution

AC (100%)

by  [qacollin](#) at Aug. 9, 2024, 5:06 p.m.

Comments

  [jafyyy](#) 1 month, 2 weeks ago

AC - these options ensure the server is secure before deployment.
upvoted 2 times

  [a4e15bd](#) 1 month, 2 weeks ago

Selected Answer: AC
A&C are correct
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 228 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 228

Topic #: 1

[\[All SY0-701 Questions\]](#)

A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following will be the best method to achieve this objective?

- A. Third-party attestation
- B. Penetration testing
- C. Internal auditing Most Voted
- D. Vulnerability scans

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [qacollin](#) at Aug. 9, 2024, 5:08 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

C. Internal Auditing
upvoted 1 times

✉ **qacollin** 2 months ago

Selected Answer: C
C. GPT
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 229 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 229

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following security concepts is accomplished with the installation of a RADIUS server?

- A. CIA
- B. AAA (Most Voted)
- C. ACL
- D. PEM

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [a4e15bd](#) at Aug. 8, 2024, 5:44 p.m.

Comments

✉ [a4e15bd](#) Highly Voted 2 months ago

B

Other being a server, RADIUS is a networking protocol that provides centralized authentication, authorization and accounting for users who connect and use a network service.

upvoted 7 times

✉ [Glacier88](#) Most Recent 1 month, 1 week ago

Selected Answer: B

RADIUS (Remote Authentication Dial-In User Service) is a network access server protocol that provides Authentication, Authorization, and Accounting (AAA) services.

upvoted 1 times

✉ [jafyyy](#) 1 month, 2 weeks ago

B. Remote Authentication Dial-In User Service protocol is used for AAA (Authentication, Authorization & Accounting)
upvoted 1 times

✉ [examreviewer](#) 1 month, 3 weeks ago

Selected Answer: B

RADIUS is a networking protocol that provides centralized authentication, authorization and accounting - AAA
upvoted 3 times

 **examreviewer** 1 month, 3 weeks ago

RADIUS is a networking protocol that provides centralized authentication, authorization and accounting - AAA
upvoted 3 times

 **internslayer** 1 month, 3 weeks ago

Selected Answer: B

B. AAA
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 230 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 230

Topic #: 1

[\[All SY0-701 Questions\]](#)

After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?

- A. Version validation
- B. Version changes
- C. Version updates
- D. Version control Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Dlove](#) at Aug. 12, 2024, 4:04 p.m.

Comments

[Dlove](#) Highly Voted 1 month, 3 weeks ago

Selected Answer: D

D. Version Control

Version control involves maintaining a record of changes made to the document, including details such as who made the changes, when they were made, and what was modified. This process ensures that all revisions are documented, and the most current version of the contract is clearly identified.

upvoted 5 times

[PAWarriors](#) Most Recent 4 weeks ago

Selected Answer: D

Version Control tracks and manages changes in documents, software, and other files and ensures that changes do not create chaos and helps with track of it.

upvoted 1 times

 **jafyyy** 1 month, 2 weeks ago

D. Version Control
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 231 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 231

Topic #: 1

[\[All SY0-701 Questions\]](#)

The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the best option?

A. Hot site

B. Cold site Most Voted

C. Failover site

D. Warm site

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [qacollin](#) at Aug. 9, 2024, 5:10 p.m.

Comments

jafyyy 1 month, 2 weeks ago

B. Cold Site is a facility with minimal infrastructure used as a backup location
upvoted 1 times

qacollin 2 months ago

Selected Answer: B
B. GPT
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 232 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 232

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

- A. Deploy multifactor authentication.
- B. Decrease the level of the web filter settings.
- C. Implement security awareness training.
- D. Update the acceptable use policy.

[Hide Answer](#)

Suggested Answer: C

by qacollin at Aug. 9, 2024, 5:13 p.m.

Comments

jafyyy 1 month, 2 weeks ago

C. Implement security awareness training

This helps employees recognize and avoid phishing & spoofed websites.

upvoted 1 times

qacollin 2 months ago

C. GPT

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 233 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 233

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following teams is best suited to determine whether a company has systems that can be exploited by a potential, identified vulnerability?

- A. Purple team
- B. Blue team
- C. Red team
- D. White team

[Hide Answer](#)

Suggested Answer: C

by [Ina22](#) at Aug. 20, 2024, 8:25 a.m.

Comments

jafyyy 1 month, 2 weeks ago

C. Red Team - simulates attacks to identify and exploit vulnerabilities in a system.
upvoted 1 times

Ina22 1 month, 2 weeks ago

C. RED Team
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 234 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 234

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:

- Allow employees to work remotely or from assigned offices around the world.
- Provide a seamless login experience.
- Limit the amount of equipment required.

Which of the following best meets these conditions?

A. Trusted devices Most Voted

B. Geotagging

C. Smart cards

D. Time-based logins

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [a4e15bd](#) at Aug. 8, 2024, 6:07 p.m.

Comments

✉ [a4e15bd](#) Highly Voted 2 months ago

A

Trusted devices allow users to log in seamlessly from devices that are already recognized and trusted by the system. It supports remote and global access as the device does not need to be in a specific location or equipped with extra hardware. It minimizes the need for additional equipment and provides for a streamlined login experience.

upvoted 5 times

✉ [Glacier88](#) Most Recent 1 month, 1 week ago

Selected Answer: A

Trusted devices.

Remote work: Trusted devices allow employees to work from any location, including remotely or from assigned offices.

Seamless login: Once a device is trusted, users can log in without requiring additional authentication factors, providing a seamless experience.

Limited equipment: Trusted devices typically require minimal additional equipment, such as a mobile app or a hardware token.

Other options don't meet all the conditions:

Geotagging: While it can provide location-based restrictions, it might not be practical for a company with employees working from various locations worldwide.

Smart cards: These require physical cards and readers, which might be inconvenient for remote workers and could increase the amount of equipment required.

Time-based logins: While they can add a layer of security, they might not be ideal for a company with employees working in different time zones.

Trusted devices offer a balance between security and convenience, making them the most suitable solution for the company's requirements.

upvoted 1 times

 **jafyyy** 1 month, 2 weeks ago

A. Trusted Devices - allows users to log in from various location using their own trusted devices without requiring additional hardware.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 235 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 235

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)

- A. Tokenization
- B. CI/CD
- C. Honeypots
- D. Threat modeling
- E. DNS sinkhole
- F. Data obfuscation

[Hide Answer](#)

Suggested Answer: CE

by [a4e15bd](#) at Aug. 8, 2024, 6:14 p.m.

Comments

✉ [a4e15bd](#) 2 months ago

C&E

Honeypot attracts and traps attacker and DNS sinkhole redirects malicious domain name queries to a controlled server to detect and block communication between compromised host and their C2 servers.

upvoted 6 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 236 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 236

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company wants to ensure that the software it develops will not be tampered with after the final version is completed. Which of the following should the company most likely use?

A. Hashing Most Voted

B. Encryption

C. Baselines

D. Tokenization

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [qacollin](#) at Aug. 9, 2024, 6:46 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

A

Hashing ensures integrity of software by detecting any unauthorized changes or tampering after its final version.
upvoted 1 times

✉ **qacollin** 1 month, 4 weeks ago

Selected Answer: A

A. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 237 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 237

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should most likely be configured during the new software deployment?

- A. RADIUS
- B. SAML
- C. EAP
- D. OpenID

[Hide Answer](#)

Suggested Answer: *B*

by  [a4e15bd](#) at Aug. 8, 2024, 6:25 p.m.

Comments

  [a4e15bd](#) Highly Voted  2 months ago

B

SAML is widely used protocol for enabling SSO across different applications and systems, particularly in enterprise environments. It allows users to authentication once and gain access to multiple application, including cloud based services.

RADUIS is typically used for network access authentication and is not generally used for SSO with cloud based applications.

EAP is used for network authentication protocols particularly in wireless networks and does not apply to SSO.

OpenID is an identity layer on top of OAuth 2.0 for authentication but is less commonly used in enterprise environments compared to SAML for SSO.

upvoted 5 times

  [jafyyy](#) Most Recent  1 month, 2 weeks ago

B

SAML

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 238 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 238

Topic #: 1

[\[All SY0-701 Questions\]](#)

A user, who is waiting for a flight at an airport, logs in to the airline website using the public Wi-Fi, ignores a security warning and purchases an upgraded seat. When the flight lands, the user finds unauthorized credit card charges. Which of the following attacks most likely occurred?

- A. Replay attack
- B. Memory leak
- C. Buffer overflow attack
- D. On-path attack Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by Kingamj at Aug. 13, 2024, 10:46 p.m.

Comments

✉️ Glacier88 1 month, 1 week ago

Selected Answer: D

On-path attack.

Public Wi-Fi: Public Wi-Fi networks are often unsecured and can be easily compromised by attackers.

Man-in-the-middle: An on-path attack involves an attacker intercepting communication between the user and the airline website, potentially capturing sensitive information like credit card details.

Security warning: The ignored security warning likely indicated that the connection was not secure, making the user vulnerable to an on-path attack.

Replay attacks, memory leaks, and buffer overflow attacks are less likely in this scenario. Replay attacks involve reusing captured data, but it's not clear how that would have led to unauthorized charges. Memory leaks and buffer overflow attacks are typically associated with software vulnerabilities, not network-based attacks.

upvoted 1 times

✉️ jafyyy 1 month, 2 weeks ago

D

This attack results from an attacker's interception of data sent over public Wi-Fi.

upvoted 1 times

 Kingamj 1 month, 3 weeks ago

Selected Answer: D

ChatGPT

An on-path attack, also known as a man-in-the-middle (MITM) attack, occurs when an attacker intercepts the communication between two parties (in this case, the user and the airline's website). Since the user was on a public Wi-Fi network and ignored security warnings, it's possible that the attacker was able to intercept the credit card information during the transaction, leading to unauthorized charges.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 239 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 239

Topic #: 1

[\[All SY0-701 Questions\]](#)

A network engineer deployed a redundant switch stack to increase system availability. However, the budget can only cover the cost of one ISP connection. Which of the following best describes the potential risk factor?

- A. The equipment MTBF is unknown.
- B. The ISP has no SLA.
- C. An RPO has not been determined.
- D. There is a single point of failure.

[Hide Answer](#)

Suggested Answer: D

by [a4e15bd](#) at Aug. 8, 2024, 6:48 p.m.

Comments

[a4e15bd](#) 2 months ago

D

Since the budget only allows for one ISP connection, this creates a single point of failure for the network connectivity.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 240 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 240

Topic #: 1

[\[All SY0-701 Questions\]](#)

A network team segmented a critical, end-of-life server to a VLAN that can only be reached by specific devices but cannot be reached by the perimeter network. Which of the following best describe the controls the team implemented? (Choose two.)

- A. Managerial
- B. Physical
- C. Corrective
- D. Detective
- E. Compensating Most Voted
- F. Technical Most Voted
- G. Deterrent

[Hide Answer](#)

Suggested Answer: EF

Community vote distribution

EF (100%)

by [a4e15bd](#) at Aug. 8, 2024, 6:54 p.m.

Comments

✉️ **Glacier88** 1 month, 1 week ago

Selected Answer: EF

E. Compensating and F. Technical.

Compensating: The segmentation serves as a compensating control, mitigating the risk associated with using an end-of-life server by isolating it from the perimeter network.

Technical: The VLAN configuration is a technical control, implementing a network-based security measure to restrict access to the critical server. The other options are not applicable in this scenario:

Managerial: Managerial controls are policies, procedures, and guidelines established by management.

Physical: Physical controls are physical barriers or safeguards, such as locks, fences, or security guards.

Corrective: Corrective controls are implemented to address a security incident or vulnerability after it has occurred.

Detective: Detective controls are designed to detect security incidents or vulnerabilities.

Deterrent: Deterrent controls are designed to discourage unauthorized access or malicious activity.

upvoted 2 times

 **b82faaf** 1 month, 3 weeks ago

Selected Answer: EF

- E. Compensating and
- F. Technical (aka technological)

upvoted 3 times

 **a4e15bd** 2 months ago

EF

Technical controls involve the use of technology to manage or mitigate risks. By segmenting the server into VLAN and restricting access to specific devices, the network team has employed a technical control here.

Compensating controls are alternative measures in place to address a risk when the primary control is not feasible which in these case segmenting the server into VLAN and limiting access can be seen as compensating control.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 241 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 241

Topic #: 1

[\[All SY0-701 Questions\]](#)

A threat actor was able to use a username and password to log in to a stolen company mobile device. Which of the following provides the best solution to increase mobile data security on all employees' company mobile devices?

A. Application management

B. Full disk encryption Most Voted

C. Remote wipe Most Voted

D. Containerization

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

B (45%)

C (45%)

10%

by RoRoRoYourBoat at Aug. 9, 2024, 12:34 a.m.

Comments

✉ a4e15bd Highly Voted 1 month, 3 weeks ago

I would go with B. Here is the reasoning, for an immediate response to a compromised device, remote swipe may be the best option. But the question asks "What is the best solution to increase mobile data security on all employee's devices?" Implementing FDE across all company devices raises the baseline security for the entire organization ensuring that data on all devices is protected. With compromised credentials a remote swipe might even be too late, if you don't find out fast enough that the device has been stolen.

upvoted 13 times

✉ EfaChux 1 month, 3 weeks ago

Threat actor already has accessed the device using username and password, encryption is useless at this point.

upvoted 5 times

✉ jafyyy 1 month, 2 weeks ago

The data on the device remains protected by encryption even if the threat actor has gained access to the username/password.

upvoted 3 times

✉ jsmthy 1 week, 2 days ago

This is wrong. Full disk encryption does not protect against malicious access if the attacker has a password. Otherwise, the user would not have access to their own files since they don't have the password.

A remote wipe is the only way out for a stolen device with stolen credentials.

upvoted 1 times

 **b82faaf**  1 month, 3 weeks ago

Selected Answer: B

B. Full disk encryption (FDE).

The question was not asking about the single phone that was stolen (in which case a remote wipe may work after the fact); rather, it asks for "the best solution to increase mobile data security on all employees' company mobile devices".

upvoted 6 times

 **Mich06**  3 days, 9 hours ago

'Data Protection: Full disk encryption (FDE) encrypts all data stored on a mobile device, ensuring that even if the device is lost or stolen, the data remains inaccessible without the proper authentication key (e.g., a password or PIN). This is crucial for protecting sensitive company information from unauthorized access'

The answer is remote wipe because the device has already been accessed using the user name and password'

upvoted 1 times

 **Ty13** 1 week ago

Selected Answer: C

C. Remote Wipe

Anyone who understands MDM would be able to answer this immediately. Phones are already encrypted - whether it's Android or Apple - otherwise your phone would be a disastrously vulnerable computer. If someone steals a phone AND has your credentials, the device has already been pwned and you have no option but to remote wipe it and hopefully stop them from accessing any further info.

upvoted 1 times

 **NONS3c** 2 weeks, 3 days ago

Selected Answer: B

because he talk about the future so B is correct

upvoted 1 times

 **2d97894** 2 weeks, 5 days ago

Selected Answer: B

Key Word: "increase mobile data security"

upvoted 1 times

 **NONS3c** 3 weeks, 4 days ago

Selected Answer: C

Remote wipe allows the company to erase all data from a lost or stolen mobile device remotely. This ensures that even if a threat actor has access to the device and login credentials, the sensitive company data can be deleted, rendering the device essentially useless from a data standpoint.

upvoted 1 times

 **Nehaltarek** 3 weeks, 5 days ago

Selected Answer: B

Answer: B

the question here is a mind playing , the scenario is on a stolen device , however, the question is asking about a security control on the rest of employee devices , not on the stolen device

according to ChatGPT:

Full Disk Encryption (FDE): This ensures that all data stored on the device is encrypted, making it inaccessible without the correct authentication. Even if a threat actor gains physical access to the device, they won't be able to read the data without the decryption key. This helps protect sensitive information from unauthorized access.

Remote Wipe: Allows for the deletion of data on a stolen device, but it needs to be activated quickly after the device is stolen. If the device is not connected to the internet, remote wipe might not be effective.

upvoted 1 times

 **17f9ef0** 1 month ago

Selected Answer: B

Answer is B

upvoted 1 times

 **myazureexams** 1 month, 1 week ago

In that case, containerization would be the best single option. It separates work data from personal data, ensuring that even if a threat actor accesses personal data, they cannot reach the work data. However, it's important to note that this should be complemented with other security measures like strong passwords, two-factor authentication, and regular updates.

Containerization and full disk encryption can help protect data on company mobile devices. Containerization separates work data from personal data, and full disk encryption secures data at rest. Additionally, remote wipe allows for deleting data if a device is lost or stolen.

The question makes it seem like, we screwed up, what can we do moving forward to protect ALL mobile phones. So in that case you would go with any of the other choices.

In the case for this particular phone. Remote wipe makes the most sense. If nothing else is already in place.

upvoted 2 times

✉ **Norbe90** 1 month, 2 weeks ago

Selected Answer: C

Threat actor already has accessed the device using username and password, encryption is useless at this point. C is the correct one
upvoted 3 times

✉ **suleman1000** 1 month, 2 weeks ago

Selected Answer: B

B. Full disk encryption
upvoted 1 times

✉ **nesquick0** 1 month, 2 weeks ago

Selected Answer: C

C. Remote Wipe
in this case B.(Full disk Encryption) is useless, since the attacker already logged-in so it has been decrypted.
upvoted 4 times

✉ **nesquick0** 1 month, 2 weeks ago

sorry i will go with D
since containerization can isolate sensitive data from other apps on the same mobile device.
upvoted 1 times

✉ **EfaChux** 1 month, 3 weeks ago

Selected Answer: D

MDM containerization refers to the process of segregating personal and corporate data on personal devices by creating a logical container to enhance corporate data security.

By using containerization, even if the thief gains access to device they will not able to access the official and confidential information on the device, also with containerization, remote wipe of the official information is possible.
upvoted 3 times

✉ **Gman530** 1 month, 2 weeks ago

I had to look further into this, but I don't think MDM Conatainerization is the answer here as this is a company mobile device, not a BYOD device, so there shouldn't be much personal data on the device that needs to be kept separate from company data.
upvoted 1 times

✉ **Justhereforcomptia** 1 month, 3 weeks ago

Selected Answer: B

Also voting for B, FDE is the best solution. Remote wipe is done after the fact of the infiltration, which might take time to do or even be feasible.
upvoted 2 times

✉ **EfaChux** 1 month, 3 weeks ago

Remote wipe is possible but cannot provide immediate protection of data on the device. You will need to have access to another device and the stolen device needs to be online for you to be able to do remote wipe
upvoted 1 times

✉ **nesquick0** 1 month, 3 weeks ago

Selected Answer: C

C. Remote wipe
since full disk encryption does not protect the data after you sucessfully logged in with user and password
also D. Containerization is not relatable.
upvoted 1 times

✉ **nyyankee718** 1 month, 3 weeks ago

Selected Answer: C

Remote wipe, they already have the password
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for

your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 242 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 242

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best describes the risk present after controls and mitigating factors have been applied?

- A. Residual
- B. Avoided
- C. Inherent
- D. Operational

[Hide Answer](#)

Suggested Answer: A

by [Ina22](#) at Aug. 20, 2024, 7:45 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

A

This is the risk that remains after controls and mitigation efforts have been applied.

upvoted 1 times

✉ **Ina22** 1 month, 2 weeks ago

A. Residual

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 243 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 243

Topic #: 1

[\[All SY0-701 Questions\]](#)

A software development team asked a security administrator to recommend techniques that should be used to reduce the chances of the software being reverse engineered. Which of the following should the security administrator recommend?

- A. Digitally signing the software
- B. Performing code obfuscation
- C. Limiting the use of third-party libraries
- D. Using compile flags

[Hide Answer](#)

Suggested Answer: *B*

by [a4e15bd](#) at Aug. 10, 2024, 3:08 a.m.

Comments

a4e15bd 1 month, 4 weeks ago

B Performing code obfuscation

Code obfuscation deliberately makes the code more difficult to understand. This involves renaming variables, methods etc. Altering the code structure in ways that do not affect functionality but make reverse engineering much harder. Attacker use reverse engineering to find vulnerabilities that can be exploited or remove or bypass security protections such as encryption or anti tamper mechanisms.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 244 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 244

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a possible factor for MFA?

A. Something you exhibit

B. Something you have Most Voted

C. Somewhere you are

D. Someone you know

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [f48446d](#) at Aug. 11, 2024, 9:14 p.m.

Comments

✉ **jafyyy** 1 month, 2 weeks ago

B

something you have like a smartphone or card is a standard factor to verify identity with MFA.

upvoted 1 times

✉ **EfaChux** 1 month, 3 weeks ago

Selected Answer: B

Very tricky with the D option, which says "someone" instead of something you know, which will be the password option.

upvoted 3 times

✉ **mr_reyes** 1 month, 3 weeks ago

This is a very trick question, if this is actually how its worded on the test:

Possible factors for MFA (Multi-Factor Authentication) include:

Something you have: This could be a physical device such as a smart card, a hardware token, or a smartphone app that generates one-time codes.

Incorrect Options:

Something you exhibit: This is not a standard factor in MFA. Authentication factors generally involve items or characteristics, not behavioral traits.

Someone you know: This would be a factor if its worded as "Something you know" (such as a password), but if they actually word it as "Someone you know" its not correct.

Somewhere you are: This would be a factor if its worded as "Something you are" (such as a fingerprint or retina scan), but if they actually word it as "Somewhere you are" its not correct.

upvoted 2 times

 **mr_reyes** 1 month, 3 weeks ago

This would only make sense if they meant to say "Which of the following is not a possible factor for MFA?". Only 1 answer fits that question. Otherwise 3 answers fit the question as its stated.

upvoted 2 times

 **Crucible_Bro** 1 month, 3 weeks ago

Something you have and something you know are both MFA factors...

upvoted 2 times

 **f48446d** 1 month, 3 weeks ago

I don't like the wording to this question. Possible factor? All 3 (know, have, and are) are part of MFA.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 245 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 245

Topic #: 1

[\[All SY0-701 Questions\]](#)

Easy-to-guess passwords led to an account compromise. The current password policy requires at least 12 alphanumeric characters, one uppercase character, one lowercase character, a password history of two passwords, a minimum password age of one day, and a maximum password age of 90 days. Which of the following would reduce the risk of this incident from happening again? (Choose two.)

- A. Increasing the minimum password length to 14 characters. Most Voted
- B. Upgrading the password hashing algorithm from MD5 to SHA-512.
- C. Increasing the maximum password age to 120 days.
- D. Reducing the minimum password length to ten characters.
- E. Reducing the minimum password age to zero days.
- F. Including a requirement for at least one special character. Most Voted

[Hide Answer](#)

Suggested Answer: AF

Community vote distribution

AF (100%)

by [a4e15bd](#) at Aug. 10, 2024, 3:29 a.m.

Comments

[jafyyy](#) 1 month, 2 weeks ago

AF

These options add further complexity.

upvoted 1 times

 **b82faaf** 1 month, 3 weeks ago

Selected Answer: AF

Since the issue is with the passwords being easy to guess, the solution would be one that addresses password complexity (and not password history or age necessarily). Increasing the minimum length of the password and introducing a special character would be the best options for this.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 246 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 246

Topic #: 1

[\[All SY0-701 Questions\]](#)

A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?

- A. The software had a hidden keylogger.
- B. The software was ransomware.
- C. The user's computer had a fileless virus.
- D. The software contained a backdoor.

[Hide Answer](#)

Suggested Answer: D

by [jafyyy](#) at Aug. 21, 2024, 7:21 p.m.

Comments

✉ [jafyyy](#) 1 month, 2 weeks ago

D

The software contained a backdoor bypassing normal authentication method.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 247 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 247

Topic #: 1

[\[All SY0-701 Questions\]](#)

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience

Which of the following best meets all of these requirements?

- A. Connecting dual PDUs to redundant power supplies
- B. Transitioning the platform to an IaaS provider Most Voted
- C. Configuring network load balancing for multiple paths
- D. Deploying multiple large NAS devices for each host

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [jafyyy](#) at Aug. 21, 2024, 7:25 p.m.

Comments

✉ [Glacier88](#) 1 month, 1 week ago

[Selected Answer: B](#)

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience

Which of the following best meets all of these requirements?

- A. Connecting dual PDUs to redundant power supplies
- B. Transitioning the platform to an IaaS provider
- C. Configuring network load balancing for multiple paths
- D. Deploying multiple large NAS devices for each host

upvoted 1 times

 pokii1992 1 month, 2 weeks ago

- B. Transitioning the platform to an IaaS provider

This option addresses the 50% memory utilization baseline, provides scalable storage, and typically includes built-in redundancy to handle single circuit failures. IaaS providers offer flexible resource allocation, easy scalability, and robust infrastructure with multiple layers of redundancy.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 248 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 248

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best describes a use case for a DNS sinkhole?

- A. Attackers can see a DNS sinkhole as a highly valuable resource to identify a company's domain structure.
- B. A DNS sinkhole can be used to draw employees away from known-good websites to malicious ones owned by the attacker.
- C. A DNS sinkhole can be used to capture traffic to known-malicious domains used by attackers.
- D. A DNS sinkhole can be set up to attract potential attackers away from a company's network resources.

[Hide Answer](#)

Suggested Answer: C

by [a4e15bd](#) at Aug. 10, 2024, 1:24 p.m.

Comments

✉ [a4e15bd](#) Highly Voted 1 month, 4 weeks ago

Answer C is correct

DNS sinkhole intercepts attempts to visit harmful websites and redirects them so you don't end up reaching a malicious website and keeps your computer safe.

upvoted 5 times

✉ [scoobysnack209](#) Most Recent 1 month, 3 weeks ago

The Answer is C, and also the same question is in Palo Alto Networks PCNSA certification.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 249 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 249

Topic #: 1

[\[All SY0-701 Questions\]](#)

An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following best describes the type of information the analyst is trying to extract from the image files?

- A. Log data
- B. Metadata**
- C. Encrypted data
- D. Sensitive data

[Hide Answer](#)

Suggested Answer: B

by [Muhammad_Umair](#) at Aug. 14, 2024, 1:10 p.m.

Comments

jafyyy 1 month, 2 weeks ago

B

Image files contain metadata such as geolocation coordinates and other details about the image.

upvoted 1 times

Muhammad_Umair 1 month, 3 weeks ago

(B). Metadata is data about data. So, Geolocation coordinates are definitely about Metadata.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 250 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 250

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following most likely describes why a security engineer would configure all outbound emails to use S/MIME digital signatures?

- A. To meet compliance standards
- B. To increase delivery rates
- C. To block phishing attacks
- D. To ensure non-repudiation

Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [a4e15bd](#) at Aug. 10, 2024, 1:30 p.m.

Comments

a4e15bd Highly Voted 1 month, 4 weeks ago

Answer D is correct.

S/MIME digital signatures provides a way to ensure that the email has not been altered and that it genuinely comes from the sender (Non-repudiation)

upvoted 5 times

TrebleSmith Most Recent 1 month, 2 weeks ago

Selected Answer: D

Digital signatures are going to ensure non-repudiation by confirming that the email came from the user who signed it and has not been tampered with.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 251 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 251

Topic #: 1

[\[All SY0-701 Questions\]](#)

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

- A. Whaling
- B. Credential harvesting
- C. Prepending
- D. Dumpster diving

[Hide Answer](#)

Suggested Answer: D

by [a4e15bd](#) at Aug. 10, 2024, 1:36 p.m.

Comments

[a4e15bd](#) 1 month, 4 weeks ago

D is correct.

In a printing center, sensitive documents that are improperly disposed of could be retrieved from the trash by attackers.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 252 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 252

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following considerations is the most important regarding cryptography used in an IoT device?

- A. Resource constraints Most Voted
- B. Available bandwidth
- C. The use of block ciphers
- D. The compatibility of the TLS version

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (67%)

C (33%)

by [a4e15bd](#) at Aug. 10, 2024, 1:44 p.m.

Comments

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. Resource constraints

Resource constraints are critical in IoT devices because these devices often have limited processing power, memory, and battery life. Cryptographic operations can be resource-intensive, so it's essential to choose algorithms and protocols that are efficient and suitable for the device's capabilities. Failing to consider resource constraints can lead to performance issues or even render the device unable to perform necessary cryptographic operations.

The other options are important but generally secondary to ensuring the cryptography can operate within the device's resource limitations:

- B. Available bandwidth: This is relevant for data transmission but is not a primary concern for the cryptography itself.
- C. The use of block ciphers: Choosing between block ciphers and stream ciphers depends on the specific use case, but resource constraints take precedence.
- D. The compatibility of the TLS version: This is important for secure communications, but resource constraints must first be addressed to ensure that the device can support any chosen protocol.

upvoted 1 times

✉ **Gman530** 1 month, 2 weeks ago

Selected Answer: A

IoT devices typically don't have a ton of resources to dedicate to encrypting/decrypting data.
upvoted 1 times

 **internslayer** 1 month, 3 weeks ago

Selected Answer: A

A: Resource Constraints
upvoted 2 times

 **nesquick0** 1 month, 3 weeks ago

Selected Answer: C

C. The use of block ciphers
upvoted 1 times

 **2fd1029** 3 weeks, 2 days ago

Block cipher is a concept of cryptography, not a consideration for IoT devices with regards to cryptography.
upvoted 1 times

 **nesquick0** 1 month, 3 weeks ago

Selected Answer: C

C. The use of block ciphers
upvoted 1 times

 **a4e15bd** 1 month, 4 weeks ago

A is correct.

IoT devices often have limited processing power, memory and battery life. This makes it crucial to choose cryptographic algorithms that are efficient and can operate within these constraints without degrading device performance.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 253 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 253

Topic #: 1

[\[All SY0-701 Questions\]](#)

A coffee shop owner wants to restrict internet access to only paying customers by prompting them for a receipt number. Which of the following is the best method to use given this requirement?

- A. WPA3
- B. Captive portal Most Voted
- C. PSK
- D. IEEE 802.1X

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [a4e15bd](#) at Aug. 10, 2024, 1:49 p.m.

Comments

 [qacollin](#) 1 month, 3 weeks ago

Selected Answer: B

B. GPT

upvoted 1 times

 [a4e15bd](#) 1 month, 4 weeks ago

B Captive Portal

This will allow the coffee shop to restrict internet access by redirecting users to a web page where they must enter the receipt information to gain access.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 254 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 254

Topic #: 1

[\[All SY0-701 Questions\]](#)

While performing digital forensics, which of the following is considered the most volatile and should have the contents collected first?

- A. Hard drive
- B. RAM** (Most Voted)
- C. SSD
- D. Temporary files

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [a4e15bd](#) at Aug. 10, 2024, 1:57 p.m.

Comments

  **TrebleSmith** 1 month, 2 weeks ago

Selected Answer: B

When the computer powers off, anything in the RAM is going to be lost. Therefore, collecting potential evidence out of the RAM is the first thing that should be done out of these options.

upvoted 3 times

  **a4e15bd** 1 month, 4 weeks ago

B is correct.

You start collecting forensic contents based on the order of volatility which is from the most volatile to the least. You collect CPU, Cache and Registers first and RAM 2nd which contains active processes, open network connections, user sessions and temp data which are lost when the system is powered off. Temporary files and hard drive/SSD comes last in the order respectively.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 255 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 255

Topic #: 1

[\[All SY0-701 Questions\]](#)

A hosting provider needs to prove that its security controls have been in place over the last six months and have sufficiently protected customer data. Which of the following would provide the best proof that the hosting provider has met the requirements?

- A. NIST CSF
- B. SOC 2 Type 2 report Most Voted
- C. CIS Top 20 compliance reports
- D. Vulnerability report

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [a4e15bd](#) at Aug. 10, 2024, 2:42 p.m.

Comments

✉ **siheom** 3 weeks, 3 days ago

Selected Answer: B

VOTE B

upvoted 1 times

✉ **a4e15bd** 1 month, 4 weeks ago

This report provides an audit of the service organization controls over a specified period of time like six months or more and assess how well those controls protect customers data according to predefined criteria.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 256 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 256

Topic #: 1

[\[All SY0-701 Questions\]](#)

A city municipality lost its primary data center when a tornado hit the facility. Which of the following should the city staff use immediately after the disaster to handle essential public services?

- A. BCP Most Voted
- B. Communication plan
- C. DRP Most Voted
- D. IRP

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

A (50%) C (50%)

by Muhammad_Umair at Aug. 18, 2024, 12:57 p.m.

Comments

✉️ User92 1 day, 4 hours ago

Selected Answer: C

Given answer is correct. An DRP, is a subset of the BCP, but DRP focuses on faster recovery after disasters
upvoted 1 times

✉️ BluezClues 3 days, 4 hours ago

Selected Answer: A

A. BCP
Not DRP because...
A Disaster Recovery Plan (DRP) focuses on restoring IT infrastructure and data after a disaster. In this case, the city needs to continue running public services immediately, not just restore IT functions. A DRP will be important later in the recovery phase, but the BCP addresses the immediate need for continuing essential operations.
upvoted 1 times

✉️ Gbemi 4 days ago

The correct ans is A,BCP. It is mainly activated after disaster has happened to ensure critical services still run uninterrupted
upvoted 1 times

 **Ty13** 1 week ago

Selected Answer: C

C. Disaster Recovery Plan

Business continuity focuses on keeping business operational during a disaster, while disaster recovery focuses on restoring data access and IT infrastructure after a disaster.

upvoted 1 times

 **W3g4N0S** 2 weeks, 2 days ago

Selected Answer: A

The correct answer is A

The Business Continuity Plan (BCP) focuses on ensuring that essential public services continue running immediately after a disaster. While a Disaster Recovery Plan (DRP) (option C) is critical for restoring systems and assets after a disaster, the BCP is what enables the city to continue critical operations without interruption, addressing the immediate response to keep services running.

The DRP is more about the technical recovery of systems, whereas the BCP is about maintaining operations in the short term while systems are being restored.

upvoted 4 times

 **c7af7af** 1 week, 5 days ago

I see what you're saying, however, that DRP may include a hot / warm site to continue services. The key in this question is "which of the following should the city use IMMEDIATELY AFTER the disaster" I'm going with DRP on this one

upvoted 2 times

 **BluezClues** 3 days, 4 hours ago

A. BCP

Not DRP because...

A Disaster Recovery Plan (DRP) focuses on restoring IT infrastructure and data after a disaster. In this case, the city needs to continue running public services immediately, not just restore IT functions. A DRP will be important later in the recovery phase, but the BCP addresses the immediate need for continuing essential operations.

upvoted 1 times

 **TrebleSmith** 1 month, 2 weeks ago

Selected Answer: C

A Disaster Recovery Plan is going to do exactly what the name states, put in place a plan to restore functions of assets after a disaster.

upvoted 3 times

 **Muhammad_Umair** 1 month, 2 weeks ago

C. Data Recovery Plan

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 257 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 257

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is considered a preventive control?

- A. Configuration auditing
- B. Log correlation
- C. Incident alerts
- D. Segregation of duties Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Muhammad_Umair](#) at Aug. 18, 2024, 12:59 p.m.

Comments

✉️ **TrebleSmith** 1 month, 2 weeks ago

Selected Answer: D

Segregation of duties is going to PREVENT users from having the ability to potentially manipulate processes within the business by splitting duties amongst others. Somewhat of a "checks and balances" kind of system.

upvoted 3 times

✉️ **Muhammad_Umair** 1 month, 3 weeks ago

D. Segregation of duties.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 258 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 258

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator notices that a testing system is down. While investigating, the systems administrator finds that the servers are online and accessible from any device on the server network. The administrator reviews the following information from the monitoring system:

Server name	IP	Traffic sent	Traffic received	Status
File01	10.12.14.13	2654812	23185	Up
DC01	10.12.15.2	168741	65481	Up
Test01	10.25.1.3	14872	654123168	Down
Test02	10.25.1.4	16941	651321685	Down
DC02	10.12.15.3	32145	32158	Up
Finance01	10.18.1.14	12374	6548	Up

Which of the following is the most likely cause of the outage?

- A. Denial of service Most Voted
- B. ARP poisoning
- C. Jamming
- D. Kerberoasting

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [TrebleSmith](#) at Aug. 8, 2024, 6:10 p.m.

Comments

 **a4e15bd** Highly Voted 1 month, 4 weeks ago

A Denial of Service.

This is clearly indicative of DoS attack where the two Test hosts are being overwhelmed with excessive traffic received causing them to become unresponsive and crash.

upvoted 7 times

 **Muhammad_Umair** Most Recent 1 month, 3 weeks ago

A). DDOS attack.

upvoted 1 times

 **Justhereforcomptia** 1 month, 3 weeks ago

Selected Answer: A

DDOS attack, check the traffic received on the servers

upvoted 2 times

 **TrebleSmith** 2 months ago

Selected Answer: A

I do not see Kerberoasting anywhere in the exam objectives, leading me to believe the answer is A: DoS

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 259 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 259

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security team has been alerted to a flood of incoming emails that have various subject lines and are addressed to multiple email inboxes. Each email contains a URL shortener link that is redirecting to a dead domain. Which of the following is the best step for the security team to take?

- A. Create a blocklist for all subject lines.
- B. Send the dead domain to a DNS sinkhole.
- C. Quarantine all emails received and notify all employees.
- D. Block the URL shortener domain in the web proxy. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (73%) B (18%) 9%

by RoRoYourBoat at Aug. 9, 2024, 12:47 a.m.

Comments

✉ **RoRoYourBoat** Highly Voted 1 month, 4 weeks ago

Selected Answer: D

D. Block the URL shortener domain in the web proxy: By blocking the URL shortener domain, the security team can prevent users from accessing potentially malicious links, even if the domain is currently dead. This proactive measure helps mitigate the risk of future attacks using the same URL shortener.

upvoted 8 times

✉ **jsmthy** Most Recent 1 week, 3 days ago

Selected Answer: C

Quarantine is correct. The dead domain may not do anything, but there can be several layers of redirects. You can place the dead domain on the DNS sinkhole, but that won't prevent users from clicking the links. If you block the URL shortener, you could block legitimate traffic to that shortener.

upvoted 1 times

✉ **dhewa** 1 week, 3 days ago

Selected Answer: B

Well D is an option but it might not address the root cause if the attacker switches to a different URL shortener.
upvoted 1 times

 **nyyankee718** 1 week, 6 days ago

Selected Answer: B

URL shortener will not block everything
upvoted 1 times

 **Hayder81** 1 month ago

D. Block the URL shortener domain in the web proxy:
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 260 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 260

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is working to secure company data on corporate laptops in case the laptops are stolen. Which of the following solutions should the administrator consider?

- A. Disk encryption Most Voted
- B. Data loss prevention
- C. Operating system hardening
- D. Boot security

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [qacollin](#) at Aug. 12, 2024, 4:33 p.m.

Comments

✉ **Hayder81** 1 month ago

- A. Disk encryption
upvoted 1 times

✉ **qacollin** 1 month, 3 weeks ago

- Selected Answer: A**
- A. GPT
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 261 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 261

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company needs to keep the fewest records possible, meet compliance needs, and ensure destruction of records that are no longer needed. Which of the following best describes the policy that meets these requirements?

- A. Security policy
- B. Classification policy
- C. Retention policy Most Voted
- D. Access control policy

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [jafyyy](#) at Aug. 21, 2024, 8 p.m.

Comments

✉ **Glacier88** 1 month, 1 week ago

Selected Answer: C

C. Retention policy.

Reasoning:

Security policy: While a security policy is important for protecting sensitive information, it doesn't specifically address the retention and destruction of records.

Classification policy: A classification policy helps categorize information based on its sensitivity and value, but it doesn't provide guidelines for how long records should be retained or when they should be destroyed.

Retention policy: A retention policy establishes rules for how long different types of records should be kept and when they can be destroyed. This is exactly what the company needs to meet compliance requirements and minimize the number of records it needs to store.

Access control policy: An access control policy governs who can access different types of information. While it's important for data protection, it doesn't directly address the retention and destruction of records.

Therefore, a retention policy is the best option for the company to meet its requirements of keeping the fewest records possible, meeting compliance needs, and ensuring destruction of records that are no longer needed.

upvoted 2 times

 **jafyyy** 1 month, 2 weeks ago

C

Retention policy specifies how long a record should be kept & when it should be disposed.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 262 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 262

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

- A. Code repositories
- B. Dark web
- C. Threat feeds
- D. State actors
- E. Vulnerability databases

[Hide Answer](#)

Suggested Answer: A

by [a4e15bd](#) at Aug. 12, 2024, 2:24 a.m.

Comments

✉ [pokii1992](#) 1 month, 2 weeks ago

A. Code repositories

Code repositories often contain hardcoded credentials, API keys, or other sensitive information that developers may accidentally commit without proper security measures. This can expose these credentials when the code is shared or made public, leading to unintentional leakage of corporate credentials in cloud environments.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 263 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 263

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?

- A. End users will be required to consider the classification of data that can be used in documents.
- B. The policy will result in the creation of access levels for each level of classification.
- C. The organization will have the ability to create security requirements based on classification levels.
- D. Security analysts will be able to see the classification of data within a document before opening it.

[Hide Answer](#)

Suggested Answer: C

by [pokii1992](#) at Aug. 24, 2024, 8:39 p.m.

Comments

✉ [pokii1992](#) 1 month, 2 weeks ago

The answer C is the best reason because it directly addresses the core benefit of data classification policies:

Creating security requirements based on classification levels allows organizations to implement tailored, appropriate security measures for different types of data. This approach ensures that the most sensitive information receives the highest level of protection, while less critical data may have less stringent controls. This targeted approach optimizes security efforts and resource allocation, providing a more effective and efficient way to protect an organization's information assets.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 264 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 264

Topic #: 1

[\[All SY0-701 Questions\]](#)

An analyst is performing a vulnerability scan against the web servers exposed to the internet without a system account. Which of the following is most likely being performed?

- A. Non-credentialed scan Most Voted
- B. Packet capture
- C. Privilege escalation
- D. System enumeration
- E. Passive scan

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [jafyyy](#) at Aug. 21, 2024, 8:05 p.m.

Comments

  [FrozenCarrot](#) 3 weeks, 4 days ago

Selected Answer: A

Without system account.

upvoted 1 times

  [jafyyy](#) 1 month, 2 weeks ago

A

Type of scan conducted without logging into the system

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 265 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 265

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is hardening corporate systems and applying appropriate mitigations by consulting a real-world knowledge base for adversary behavior. Which of the following would be best for the administrator to reference?

- A. MITRE ATT&CK
- B. CSIRT
- C. CVSS
- D. SOAR

[Hide Answer](#)

Suggested Answer: A

by [a4e15bd](#) at Aug. 12, 2024, 2:56 a.m.

Comments

a4e15bd 1 month, 3 weeks ago

MITRE ATT&CK is a comprehensive and widely used framework that categorizes and describes the various tactics, techniques and procedures (TTPs) employed by adversaries, it is used for threat intelligence, defensive strategy etc.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 266 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 266

Topic #: 1

[\[All SY0-701 Questions\]](#)

An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will most likely meet the requirements?

- A. A website-hosted solution
- B. Cloud shared storage
- C. A secure email solution
- D. Microservices using API

[Hide Answer](#)

Suggested Answer: D

by [a4e15bd](#) at Aug. 12, 2024, 3:03 a.m.

Comments

[a4e15bd](#) 1 month, 3 weeks ago

D. Microservices Using API

By using APIs will allow for increased speed of data transfer compared to file based transfer methods like SFTP.

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 267 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 267

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following addresses individual rights such as the right to be informed, the right of access, and the right to be forgotten?

A. GDPR Most Voted

B. PCI DSS

C. NIST

D. ISO

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [b82faaf](#) at Aug. 13, 2024, 10:31 a.m.

Comments

  [Syl0](#) 2 months, 2 weeks ago

GDPR - General Data Protection Regulation
NIST - Network institute of standards and technology, so doesn't have that.
PCI DSS - Payment Card Industry Data security standards
ISO - International standard for Standardisation
upvoted 2 times

  [jafyyy](#) 2 months, 4 weeks ago

A
- Addressed individual rights to be informed, access or to be forgotten among other rights.
upvoted 1 times

  [b82faaf](#) 3 months, 1 week ago

Selected Answer: A
A. GDPR
upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

[View all questions & answers for the SY0-701 exam](#)

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 268 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 268

Topic #: 1

[\[All SY0-701 Questions\]](#)

An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?

- A. The administrator should allow SAN certificates in the browser configuration.
- B. The administrator needs to install the server certificate into the local truststore.
- C. The administrator should request that the secure LDAP port be opened to the server.
- D. The administrator needs to increase the TLS version on the organization's RA.

[Hide Answer](#)

Suggested Answer: B

by [a4e15bd](#) at Aug. 12, 2024, 3:12 a.m.

Comments

✉ [a4e15bd](#) 1 month, 3 weeks ago

B is correct

The administrator needs to the server's certificate in the local trust store of the machine where LDAP browser tool is being used. This will allow the client to trust the server's certificate and establish a secure connection.

upvoted 6 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 269 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 269

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the most important security concern when using legacy systems to provide production service?

- A. Instability
- B. Lack of vendor support Most Voted
- C. Loss of availability
- D. Use of insecure protocols Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

B (50%)

D (50%)

by [jafyyy](#) at Aug. 21, 2024, 8:15 p.m.

Comments

✉️ **User92** 1 day, 4 hours ago

Selected Answer: D

Given answer is correct - because legacy systems often rely on outdated and insecure protocols that can be easily exploited.
upvoted 1 times

✉️ **cyoncon** 1 day, 18 hours ago

Selected Answer: B

Primary concern is vendor support.
upvoted 1 times

✉️ **BluezClues** 3 days, 3 hours ago

Selected Answer: B

B.
Lack of Vendor Support
Why it isn't D. Use of Protocols: Many legacy systems use outdated and insecure protocols, which is certainly a concern, but insecure protocols can

often be mitigated by wrapping them in secure communication channels (e.g., VPNs, encryption). The lack of vendor support to address these insecure protocols is actually a greater problem than their presence because there's no way to patch or upgrade them without vendor assistance.
upvoted 1 times

BluezClues 3 days, 3 hours ago

B.

Lack of Vendor Support

Why it isn't D. Use of Protocols: Many legacy systems use outdated and insecure protocols, which is certainly a concern, but insecure protocols can often be mitigated by wrapping them in secure communication channels (e.g., VPNs, encryption). The lack of vendor support to address these insecure protocols is actually a greater problem than their presence because there's no way to patch or upgrade them without vendor assistance.

upvoted 1 times

a0bfa81 5 days, 22 hours ago

Selected Answer: B

The most important security concern when using legacy systems is the lack of vendor support. Without vendor support, legacy systems may not receive essential security updates, patches, or technical assistance, leaving them vulnerable to known exploits and threats. This can significantly increase the risk of security breaches.

upvoted 1 times

nyyankee718 6 days, 9 hours ago

Selected Answer: B

insecure protocol is an issue but would be greater without vendor support

upvoted 1 times

Examplary 6 days, 21 hours ago

Selected Answer: D

Legacy Systems - Outdated computing software, hardware, or other technologies that have been largely superseded by newer and more efficient alternatives.

Unsupported Systems - Hardware or software products that no longer receive official technical support, security updates, or patches from their respective vendors or developers.

Just because something is legacy does not mean that it's no longer supported by the vendor. However, it does mean that it is likely using outdated technologies/protocols. I vote D.

upvoted 1 times

2fef490 2 weeks, 6 days ago

Selected Answer: B

The most important security concern with legacy systems is the lack of vendor support. Without vendor support, there are no updates, security patches, or fixes for newly discovered vulnerabilities. This leaves the system exposed to potential attacks that cannot be easily mitigated, increasing the risk of security breaches.

upvoted 3 times

NONS3c 3 weeks, 4 days ago

Selected Answer: D

it is correct

upvoted 1 times

17f9ef0 4 weeks, 1 day ago

Selected Answer: D

Answer is D

upvoted 1 times

Syl0 1 month ago

hmmm, if it's security concern, shouldn't it be D use of insecure protocol?

upvoted 1 times

Cee007 1 month, 1 week ago

Selected Answer: D

The answer is D. Legacy systems rely on outdated protocols which often contain vulnerabilities that attackers can exploit. They may also lack the security features to protect against modern threats.

upvoted 3 times

Ina22 1 month, 2 weeks ago

D. Use of insecure protocols.

Legacy systems often rely on outdated protocols that may not have the necessary security features to protect against modern threats. This can lead to vulnerabilities that attackers can exploit, compromising the integrity, confidentiality, and availability of the system and its data.

upvoted 1 times

jafyyy 1 month, 2 weeks ago

D

Legacy systems rely on outdated and insecure protocols with known vulnerabilities.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 270 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 270

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

- A. A spraying attack was used to determine which credentials to use.
- B. A packet capture tool was used to steal the password. Most Voted
- C. A remote-access Trojan was used to install the malware.
- D. A dictionary attack was used to log in as the server administrator.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [baronvon](#) at Aug. 24, 2024, 5:08 p.m.

Comments

✉ **FrozenCarrot** 3 weeks, 4 days ago

Telnet no encryption
upvoted 1 times

✉ **pokii1992** 1 month, 2 weeks ago

B. A packet capture tool was used to steal the password.

This is the most likely scenario given that the administrator regularly used Telnet, which transmits data in plain text. An attacker could easily capture the login credentials using a packet sniffing tool, then use those stolen credentials to install the malicious software on the server.
upvoted 1 times

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: B

B. A packet capture tool was used to steal the password.

Telnet transmits data, including credentials, in plaintext, making it vulnerable to interception. A packet capture tool could easily capture the login credentials being transmitted, allowing an attacker to gain unauthorized access to the server.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 271 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 271

Topic #: 1

[\[All SY0-701 Questions\]](#)

A user is requesting Telnet access to manage a remote development web server. Insecure protocols are not allowed for use within any environment. Which of the following should be configured to allow remote access to this server?

- A. HTTPS
- B. SNMPv3
- C. SSH Most Voted
- D. RDP
- E. SMTP

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [baronvon](#) at Aug. 24, 2024, 5:09 p.m.

Comments

✉ [pokii1992](#) 1 month, 2 weeks ago

SSH is recommended because:
It provides strong encryption for all data transmitted
It's a secure protocol, meeting the requirement of avoiding insecure options
It allows secure remote access to servers, which is what you're looking for
It's widely used and supported for development environments
It can be used to set up secure tunnels for accessing web servers remotely
upvoted 1 times

✉ [baronvon](#) 1 month, 2 weeks ago

Selected Answer: C

C. SSH

SSH (Secure Shell) provides encrypted remote access to servers, making it a secure alternative to Telnet, which transmits data in plaintext. SSH is commonly used for secure management of remote systems and would be the appropriate choice given the restriction on insecure protocols.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 272 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 272

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is working to find a cost-effective solution to implement certificates for a large number of domains and subdomains owned by the company. Which of the following types of certificates should the administrator implement?

- A. Wildcard Most Voted
- B. Client certificate
- C. Self-signed
- D. Code signing

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [a4e15bd](#) at Aug. 12, 2024, 3:17 p.m.

Comments

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. Wildcard

Wildcard certificates allow you to secure a domain and all of its subdomains with a single certificate. This can be a cost-effective solution for managing certificates for a large number of domains and subdomains.

upvoted 1 times

✉ **scholi** 1 month, 2 weeks ago

Wildcards are used to search for files or directories that match a certain pattern.

* (Asterisk): Represents zero or more characters.

Example: *.txt matches all files with a .txt extension.

? (Question Mark): Represents exactly one character.

Example: file?.doc matches file1.doc, fileA.doc, etc.

upvoted 1 times

 **scholi** 1 month, 2 weeks ago

A wildcard is a character or symbol used in computing to represent one or more characters in a string, allowing for flexible searching, matching, and filtering. Wildcards are commonly used in various contexts such as file searching, pattern matching, and access control.

Wildcards are used to search for files or directories that match a certain pattern.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 273 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 273

Topic #: 1

[\[All SY0-701 Questions\]](#)

An auditor discovered multiple insecure ports on some servers. Other servers were found to have legacy protocols enabled. Which of the following tools did the auditor use to discover these issues?

A. Nessus Most Voted

B. curl

C. Wireshark

D. netcat

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qacollin](#) at Aug. 12, 2024, 5:07 p.m.

Comments

  [baronvon](#) 1 month, 2 weeks ago

Selected Answer: A

A. Nessus

Nessus is a vulnerability scanner that can identify insecure ports, legacy protocols, and other security issues on servers. It is designed to detect vulnerabilities and misconfigurations in systems.

upvoted 1 times

  [qacollin](#) 1 month, 3 weeks ago

Selected Answer: A

A. GPT

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 274 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 274

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst received a tip that sensitive proprietary information was leaked to the public. The analyst is reviewing the PCAP and notices traffic between an internal server and an external host that includes the following:

...

12:47:22.327233 PPPoE [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 331) 10.5.1.1 > 52.165.16.154: IP6 (hlim E3, next-header TCP (6) payload length: 271) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:dddd:a601:24fa.13788: Flags [P], cksum 0xd7ee (correct), seq 97:348, ack 102, win 16444, length 251

...

Which of the following was most likely used to exfiltrate the data?

- A. Encapsulation Most Voted
- B. MAC address spoofing
- C. Steganography
- D. Broken encryption
- E. Sniffing via on-path position

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by qacollin at Aug. 12, 2024, 5:09 p.m.

Comments

✉ pokii1992 1 month, 2 weeks ago

A. Encapsulation

The PCAP shows traffic using IPv6 encapsulated within IPv4 (proto IPv6 (41)), which could be used to hide sensitive data within seemingly normal network traffic. This encapsulation technique can potentially bypass certain security controls and filters, making it an effective method for data exfiltration.

upvoted 2 times

 **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. Encapsulation

The traffic described involves IPv6 encapsulated within IPv4, which can indicate that data is being transmitted through encapsulation to obscure the content or bypass filters. This technique could be used to exfiltrate sensitive data by embedding it within legitimate traffic patterns.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 275 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 275

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

- A. Serverless architecture Most Voted
- B. Thin clients
- C. Private cloud
- D. Virtual machines

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [qacollin](#) at Aug. 12, 2024, 5:21 p.m.

Comments

✉ **pokii1992** 1 month, 2 weeks ago

Serverless architecture is recommended because it:

- Eliminates server management tasks
- Reduces deployment time significantly
- Lowers costs by only charging for actual code execution
- Automatically scales based on demand
- Allows developers to focus solely on writing code
- Handles infrastructure and scaling automatically

upvoted 1 times

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. Serverless architecture

Serverless architecture allows the company to reduce the time and expense associated with code deployment by handling the underlying

infrastructure management automatically. This means the company only needs to focus on the code itself, without worrying about provisioning or managing servers. This approach can also scale automatically with demand, further reducing operational overhead and costs.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 276 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 276

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator is performing an audit on a stand-alone UNIX server, and the following message is immediately displayed:

(Error 13): /etc/shadow: Permission denied.

Which of the following best describes the type of tool that is being used?

A. Pass-the-hash monitor

B. File integrity monitor

C. Forensic analysis

D. Password cracker Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (64%)

B (36%)

by AZZ99 at Aug. 12, 2024, 6:58 p.m.

Comments

✉ **Cyberity** Highly Voted 1 month, 2 weeks ago

Selected Answer: D

Password crackers often attempt to access this file to obtain hashed passwords for cracking.

upvoted 5 times

✉ **User92** Most Recent 1 day, 3 hours ago

Selected Answer: D

Password crackers often attempt to access the /etc/shadow file to retrieve hashed passwords for cracking.

upvoted 1 times

✉ **Ty13** 1 week ago

Selected Answer: B

B. File Integrity Monitoring

The /etc/shadow file stores encrypted user passwords, and you can only access it as root. If you're checking file integrity, you're checking the permissions are still properly set and haven't been changed. You WANT to see 'Permission Denied' if you're auditing the system.

upvoted 1 times

 **FrozenCarrot** 3 weeks, 1 day ago

Selected Answer: B

The /etc/shadow is a text-based password file.

upvoted 1 times

 **850bc48** 1 month ago

D. password cracking

upvoted 1 times

 **Gman530** 1 month, 1 week ago

Selected Answer: B

A file integrity monitor would attempt to read the contents of etc/shadow while doing integrity checks, this may fail due to insufficient permissions.

- File Integrity monitor matches the activity of an administrator performing an audit.

- Password Cracking is more aligned with pentesting than auditing.

upvoted 2 times

 **AZZ99** 1 month, 3 weeks ago

Selected Answer: D

Copy pasted to ChatGPT and the answer is D. Make sense to me.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 277 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 277

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323, and SRTP. Which of the following does this rule set support?

A. RTOS

B. VoIP Most Voted

C. SoC

D. HVAC

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [scoobysnack209](#) at Aug. 14, 2024, 9:19 p.m.

Comments

✉ **Syl0** 1 month ago

RTOS - Real-Time Operating system
VoIP - Voice over Internet Protocol
SoC - System on Chip
HVAC - Heat, Ventilation, Air condition

RTP - Real-Time Transport Protocol
SIP - Session initiation Protocol
SRTP - Secure Real-time Transport Protocol
upvoted 1 times

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: B
B. VoIP

The protocols RTP (Real-time Transport Protocol), SIP (Session Initiation Protocol), H.323, and SRTP (Secure Real-time Transport Protocol) are commonly used in Voice over IP (VoIP) communications. RTP handles the transport of media streams, SIP manages call setup and control, H.323 is a standard for multimedia communication, and SRTP provides encryption for RTP. Therefore, the firewall rules for these protocols support VoIP.

upvoted 3 times

 **scoobysnack209** 1 month, 3 weeks ago

RTP Real-time Transport Protocol

SRTP Secure Real-time Transport Protocol

SIP Session Initiation Protocol

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 278 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 278

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following best describes a social engineering attack that uses a targeted electronic messaging campaign aimed at a Chief Executive Officer?

- A. Whaling Most Voted
- B. Spear phishing
- C. Impersonation
- D. Identity fraud

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [baronvon](#) at Aug. 24, 2024, 5:58 p.m.

Comments

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. Whaling

Whaling is a type of social engineering attack specifically targeting high-profile individuals such as CEOs or other executives. It is a form of spear phishing that focuses on these high-value targets with highly personalized and convincing messages.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 279 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 279

Topic #: 1

[\[All SY0-701 Questions\]](#)

During a penetration test, a flaw in the internal PKI was exploited to gain domain administrator rights using specially crafted certificates. Which of the following remediation tasks should be completed as part of the cleanup phase?

A. Updating the CRL Most Voted

B. Patching the CA Most Voted

C. Changing passwords

D. Implementing SOAR

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (54%)

A (46%)

by [a4e15bd](#) at Aug. 13, 2024, 2:38 a.m.

Comments

baronvon Highly Voted 1 month, 1 week ago

Selected Answer: B

B. Patching the CA

Here's why:

Patching the Certificate Authorities: This involves updating the CA software to address the specific vulnerability that was exploited. Since the attack exploited a flaw in the PKI, patching the CA is crucial to fixing the vulnerability and preventing similar attacks in the future.

While the other options are also important in a broader security context, they may not directly address the specific issue with the PKI flaw:

-Updating the Certificate Revocation Lists (CRLs): This is important for managing revoked certificates but may not address the root cause of the PKI vulnerability.

-Changing passwords: This is a good security practice but would not resolve the underlying issue with the PKI vulnerability.

-Implementing SOAR (Security Orchestration, Automation, and Response): SOAR can help with automating responses and managing security operations but does not directly address the specific PKI vulnerability.

-Therefore, patching the Certificate Authorities is the most effective and direct remediation task for this situation.
upvoted 5 times

 **User92** (Most Recent) 1 day, 3 hours ago

Selected Answer: B

Updating the CRL is also important, but it primarily deals with revoking compromised certificates rather than fixing the underlying vulnerability.
upvoted 1 times

 **Ty13** 1 week ago

Selected Answer: A

A. Updating the CRL

It's a really bad question because you would do BOTH A and B.

The only reason I'm saying A is because the question specifically says "cleanup phase". Patching the CA would TECHNICALLY fall under the Eradication Phase - we're eradicating a threat (patching a vulnerable CA server) - and then cleanup would be updating the CRL.
upvoted 3 times

 **tamdod** 1 month, 1 week ago

This occurred during a penetration test. We should patch the CA first to prevent further exploitation, that ensures no new certificates can be issued using the same flaw. Then we would update the CRL.
upvoted 2 times

 **TrebleSmith** 1 month, 2 weeks ago

Selected Answer: A

While patching the Certificate Authority is important to prevent a similar attack in the future, I believe that updating the Certificate Revocation List will apply more directly to the clean-up phase.
upvoted 3 times

 **suleman1000** 1 month, 2 weeks ago

Selected Answer: B

B: Patching the CA
upvoted 1 times

 **salahsami2002** 1 month, 2 weeks ago

B. Patching the CA (Certificate Authority)

Since the flaw in the internal Public Key Infrastructure (PKI) was exploited to gain domain administrator rights, the primary remediation task should be to patch the Certificate Authority (CA). This will address the vulnerability that allowed the exploitation of the PKI system. Other tasks like updating the Certificate Revocation List (CRL) may be necessary, but patching the CA will directly resolve the issue that led to the compromise.
upvoted 1 times

 **a4e15bd** 1 month, 3 weeks ago

A. Update the CRL is correct

The first priority is to revoke any compromised certificates. This ensures that those certificates can no longer be used for unauthorized access.
upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 280 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 280

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company wants to implement MFA. Which of the following enables the additional factor while using a smart card?

A. PIN Most Voted

B. Hardware token

C. User ID

D. SMS

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [a4e15bd](#) at Aug. 13, 2024, 2:42 a.m.

Comments

✉ **baronvon** 1 month, 2 weeks ago

Selected Answer: A

A. PIN

Here's why:

PIN (Personal Identification Number): When using a smart card, the smart card itself serves as one factor (something you have), and the PIN entered to access the smart card provides the second factor (something you know). This combination of something you have (the smart card) and something you know (the PIN) constitutes MFA.

The other options are not directly related to the authentication factor provided by the smart card:

-Hardware token: This could be another factor for MFA but is not used in conjunction with a smart card; instead, it's a standalone factor.

-User ID: This is usually a username and not a factor in MFA.

-SMS: This can be used as an additional factor in some MFA setups but is not directly related to smart cards. It represents a different method of delivering a second factor, such as a one-time passcode sent via text message.

upvoted 1 times

 **a4e15bd** 1 month, 3 weeks ago

When using a smart card as part of MFA, the additional factor is typically a PIN. The smart card provides something you have and the PIN provides something you know, which together constitutes two factors of authentication.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 281 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 281

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company hired an external consultant to assist with required system upgrades to a critical business application. A systems administrator needs to secure the consultant's access without sharing passwords to critical systems. Which of the following solutions should most likely be utilized?

- A. TACACS+
- B. SAML
- C. An SSO platform
- D. Role-based access control
- E. PAM software

[Hide Answer](#)

Suggested Answer: E

by [a4e15bd](#) at Aug. 13, 2024, 2:50 a.m.

Comments

[a4e15bd](#) Highly Voted 3 months, 1 week ago

E. PAM Software

PAM software helps manage and secure privileged accounts and access credentials. It allows admins to grant temporary, controlled access to critical systems without sharing passwords directly. PAM software can track, monitor and log all activities performed by the consultant.

upvoted 6 times

[scoobysnack209](#) Most Recent 3 months ago

PAM Privileged Access Management

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 282 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 282

Topic #: 1

[\[All SY0-701 Questions\]](#)

A newly implemented wireless network is designed so that visitors can connect to the wireless network for business activities. The legal department is concerned that visitors might connect to the network and perform illicit activities. Which of the following should the security team implement to address this concern?

- A. Configure a RADIUS server to manage device authentication.
- B. Use 802.1X on all devices connecting to wireless.
- C. Add a guest captive portal requiring visitors to accept terms and conditions.
- D. Allow for new devices to be connected via WPS.

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  [a4e15bd](#) at Aug. 13, 2024, 2:57 a.m.

Comments

  [Ty13](#) 1 week, 1 day ago

[Selected Answer: C](#)

C. Captive Portal

A, B, and D don't account for people performing illicit activities.

upvoted 1 times

  [a4e15bd](#) 1 month, 3 weeks ago

C

Users logging into captive portal and accepting the terms and conditions before gaining access should address the concern raised by legal department.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 283 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 283

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following data roles is responsible for identifying risks and appropriate access to data?

- A. Owner
- B. Custodian
- C. Steward Most Voted
- D. Controller

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (57%)

A (43%)

by [qacollin](#) at Aug. 12, 2024, 5:39 p.m.

Comments

✉ [a4e15bd](#) Highly Voted 1 month, 3 weeks ago

A. Owner

The data owner is indeed responsible for identifying risks and determining the appropriate access to data.
upvoted 12 times

✉ [User92](#) Most Recent 1 day, 2 hours ago

Selected Answer: C

The data owner is typically responsible for the overall management of the data. A Data Steward is tasked with managing data quality, ensuring data governance policies are followed, and identifying risks related to data handling and access.
upvoted 1 times

✉ [Ty13](#) 1 week ago

Selected Answer: A

A. Owner

The Data Owner is chiefly responsible for identifying risks related to the data and determining who should have access to it.

upvoted 1 times

 **Chrissyy6111** 1 week, 2 days ago

A. Owner, data steward is just another name for data custodian that Comptia uses.

upvoted 1 times

 **opeyemi777** 2 weeks, 3 days ago

Selected Answer: A

Ensuring that adequate and timely risk identification and access to appropriate data is performed is the responsibility of the owner

upvoted 2 times

 **Hayder81** 1 month ago

C. Steward

Data Steward: Oversees data governance policies, ensures data quality, manages access control, and helps in identifying risks to ensure proper use of data.

upvoted 4 times

 **apant** 1 month, 1 week ago

Selected Answer: C

C. Steward

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 284 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 284

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following physical controls can be used to both detect and deter? (Choose two.)

A. Lighting Most Voted

B. Fencing

C. Signage

D. Sensor Most Voted

E. Bollard

F. Lock

[Hide Answer](#)

Suggested Answer: AD

Community vote distribution

AD (88%)

13%

by [nesquick0](#) at Aug. 13, 2024, 3:13 p.m.

Comments

✉ [TrebleSmith](#) Highly Voted 1 month, 2 weeks ago

Selected Answer: AD

Lighting will illuminate the area, detect people attempting to be under the cover of night, and deter them from committing unwanted acts. Furthermore, a sensor will detect movement in an area, and sensors that are visible can ward off any potential bad actors.

upvoted 5 times

✉ [Gman530](#) Most Recent 1 month, 2 weeks ago

Selected Answer: AD

These are the only 2 that can both detect and deter
upvoted 2 times

✉ [nesquick0](#) 1 month, 3 weeks ago

Selected Answer: CD

C , D zzzz

upvoted 1 times

  **TrebleSmith** 1 month, 2 weeks ago

In the nicest way, do you mind explaining how a sign detects or helps to detect unwanted activity?

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 285 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 285

Topic #: 1

[\[All SY0-701 Questions\]](#)

A multinational bank hosts several servers in its data center. These servers run a business-critical application used by customers to access their account information. Which of the following should the bank use to ensure accessibility during peak usage times?

- A. Load balancer
- B. Cloud backups
- C. Geographic dispersal
- D. Disk multipathing

[Hide Answer](#)

Suggested Answer: A

by [pokii1992](#) at Aug. 24, 2024, 9:28 p.m.

Comments

✉ [pokii1992](#) 1 month, 2 weeks ago

A. Load balancer

A load balancer is the most appropriate solution to ensure accessibility of a business-critical application during peak usage times. It distributes incoming network traffic across multiple servers, optimizing resource utilization, maximizing throughput, minimizing response time, and avoiding overload on any single server. This is particularly crucial for a multinational bank's customer-facing application during high-traffic periods.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 286 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 286

Topic #: 1

[\[All SY0-701 Questions\]](#)

The author of a software package is concerned about bad actors repackaging and inserting malware into the software. The software download is hosted on a website, and the author exclusively controls the website's contents. Which of the following techniques would best ensure the software's integrity?

- A. Input validation
- B. Code signing
- C. Secure cookies
- D. Fuzzing

[Hide Answer](#)

Suggested Answer: B

by pokii1992 at Aug. 24, 2024, 9:30 p.m.

Comments

✉ **pokii1992** 1 month, 2 weeks ago

B. Code Signing

Code signing helps ensure the integrity and authenticity of your software package. It prevents bad actors from successfully repackaging your software with malware, as the digital signature would no longer match. Users can verify that the software comes from you and hasn't been tampered with since you signed it, increasing trust and security.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 287 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 287

Topic #: 1

[\[All SY0-701 Questions\]](#)

A third-party vendor is moving a particular application to the end-of-life stage at the end of the current year. Which of the following is the most critical risk if the company chooses to continue running the application?

A. Lack of security updates Most Voted

B. Lack of new features

C. Lack of support

D. Lack of source code access

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [qacollin](#) at Aug. 12, 2024, 5:54 p.m.

Comments

a4e15bd 1 month, 3 weeks ago

A. Lack of security updates is correct.
upvoted 2 times

qacollin 1 month, 3 weeks ago

Selected Answer: A
A. GPT
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 288 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 288

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst recently read a report about a flaw in several of the organization's printer models that causes credentials to be sent over the network in cleartext, regardless of the encryption settings. Which of the following would be best to use to validate this finding?

- A. Wireshark
- B. netcat
- C. Nessus
- D. Nmap

[Hide Answer](#)

Suggested Answer: A

by [a4e15bd](#) at Aug. 13, 2024, 3:16 a.m.

Comments

Muhammad_Umair 1 month, 3 weeks ago

- A. As Wireshark is used to capture a data packet.
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 289 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 289

Topic #: 1

[\[All SY0-701 Questions\]](#)

A development team is launching a new public-facing web product. The Chief Information Security Officer has asked that the product be protected from attackers who use malformed or invalid inputs to destabilize the system. Which of the following practices should the development team implement?

A. Fuzzing Most Voted

B. Continuous deployment

C. Static code analysis

D. Manual peer review

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (75%)

C (25%)

by qacollin at Aug. 12, 2024, 6:04 p.m.

Comments

✉ dhewa 1 week, 6 days ago

Selected Answer: A

Fuzzing, or fuzz testing, is an automated software testing technique that involves inputting random, unexpected, or invalid data into a program to identify vulnerabilities. The goal is to discover bugs, crashes, or security issues by monitoring how the program responds to these inputs. Fuzzing is particularly effective for testing software that processes structured data, such as file formats or network protocols.

upvoted 1 times

✉ TrebleSmith 1 month, 1 week ago

Selected Answer: A

Fuzzing is "... involves feeding a system with invalid, unexpected, or random inputs, also known as fuzz, to try to crash it or trigger errors.". This is going to be the best answer for this question.

upvoted 1 times

✉ Gman530 1 month, 2 weeks ago

Selected Answer: C

- Static Code Analysis (SAST)
 - A method of debugging an application by reviewing and examining its source code before running the program
 - Identifies issues like buffer overflows, SQL injection, and XSS
 - Important for proper input validation in both front-end and back-end code
- upvoted 1 times

 **a4e15bd** 1 month, 3 weeks ago

Answer A, Fuzzing is correct.

upvoted 2 times

 **qacollin** 1 month, 3 weeks ago

Selected Answer: A

- A. GPT

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 290 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 290

Topic #: 1

[\[All SY0-701 Questions\]](#)

During an annual review of the system design, an engineer identified a few issues with the currently released design. Which of the following should be performed next according to best practices?

- A. Risk management process
- B. Product design process
- C. Design review process
- D. Change control process

[Most Voted](#)

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (75%)

C (25%)

by RoRoYourBoat at Aug. 12, 2024, 10:15 p.m.

Comments

✉ PAWarriors 6 days, 20 hours ago

Correct answer is C. Design review process.

The next step that should be performed according to best practices after identifying issues with the currently released design is the C. Design review process.

> In this question the keyword is "Next".
upvoted 1 times

✉ Ty13 1 week, 1 day ago

[Selected Answer: C](#)

C. Design Review

You still need to evaluate issues and determine if revisions are necessary. If they don't, then that's the end of it.

You only need Change Control when you're actually making changes.

upvoted 1 times

 **dhewa** 1 week, 6 days ago

Selected Answer: C

"Next" is the key word here.

upvoted 1 times

 **EfaChux** 1 month, 3 weeks ago

Selected Answer: D

D. should be the answer since the designed is already release, hence its a change control that will be required.

upvoted 3 times

 **a4e15bd** 1 month, 3 weeks ago

The design review process allows stakeholders to assess the identified issues and discuss potential solutions and make necessary adjustments.

upvoted 1 times

 **nesquick0** 1 month, 3 weeks ago

what is it then?

upvoted 1 times

 **a4e15bd** 1 month, 3 weeks ago

I am going to revise my answer. It should be D. Change Control process, because a design review process has already taken place and the next step really should be Change control process and not another design review process.

upvoted 1 times

 **RoRoRoYourBoat** 1 month, 3 weeks ago

Selected Answer: D

According to best practices, after identifying issues with the currently released design during an annual review, the next step should be:

D. Change control process: The change control process ensures that any modifications to the design are systematically evaluated, approved, and documented. This helps in maintaining the integrity of the system and ensures that changes are implemented in a controlled and coordinated manner.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 291 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 291

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is best to use when determining the severity of a vulnerability?

- A. CVE
- B. OSINT
- C. SOAR
- D. CVSS Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [dhewa](#) at Aug. 22, 2024, 6:52 a.m.

Comments

[dhewa](#) 1 month, 2 weeks ago

Selected Answer: D

Common Vulnerability Scoring System
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

EXAM SY0-701 TOPIC 1 QUESTION 292 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 292

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization experienced a security breach that allowed an attacker to send fraudulent wire transfers from a hardened PC exclusively to the attacker's bank through remote connections. A security analyst is creating a timeline of events and has found a different PC on the network containing malware. Upon reviewing the command history, the analyst finds the following:

PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-domain.com /ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327

Which of the following best describes how the attacker gained access to the hardened PC?

- A. The attacker created fileless malware that was hosted by the banking platform.
- B. The attacker performed a pass-the-hash attack using a shared support account. Most Voted
- C. The attacker utilized living-off-the-land binaries to evade endpoint detection and response software.
- D. The attacker socially engineered the accountant into performing bad transfers.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [Muhammad_Umair](#) at Aug. 18, 2024, 10:32 a.m.

Comments

[a4e15bd](#) 1 month, 2 weeks ago

Selected Answer: B

B. is the correct answer.

upvoted 1 times

[Muhammad_Umair](#) 1 month, 3 weeks ago

Mimikatz is an open-source tool that allows users to view and extract credentials stored on a Windows system. It can extract plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory. Answer (B)

upvoted 4 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 293 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 293

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is the best resource to consult for information on the most common application exploitation methods?

- A. OWASP Most Voted
- B. STIX
- C. OVAL
- D. Threat intelligence feed
- E. Common Vulnerabilities and Exposures

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [qacollin](#) at Aug. 12, 2024, 6:14 p.m.

Comments

  **FrozenCarrot** 3 weeks, 3 days ago

OWASP (Open Web Application Security Project). OWASP provides extensive resources, guidelines, and tools related to web application security, including the OWASP Top 10, which lists the most critical security risks to web applications.

upvoted 1 times

  **Muhammad_Umair** 1 month, 2 weeks ago

A).OWASP

upvoted 1 times

  **qacollin** 1 month, 3 weeks ago

Selected Answer: A

A. GPT

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

[View all questions & answers for the SY0-701 exam](#)

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 294 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 294

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst is reviewing the logs on an organization's DNS server and notices the following unusual snippet:

```
Log from named: post-processed 20230102 0045L
...
qry_source: 124.22.158.37 TCP/53
qry_dest: 52.165.16.154 TCP/53
qry_dest: 10.100.50.5 TCP/53
qry_type: AXFR
| zone int.comptia.org
-----| www A 10.100.50.21
-----| dns A 10.100.5.5
-----| adds A 10.101.10.10
-----| fshare A 10.101.10.20
-----| sip A 10.100.5.11
...
```

Which of the following attack techniques was most likely used?

- A. Determining the organization's ISP-assigned address space
- B. Bypassing the organization's DNS sinkholing
- C. Footprinting the internal network Most Voted
- D. Attempting to achieve initial access to the DNS server
- E. Exfiltrating data from fshare.int.complia.org

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by  cri88 at Aug. 19, 2024, 12:45 a.m.

Comments

 **a4e15bd** 1 month, 2 weeks ago

Selected Answer: C

AXFR can be used for footprinting during the reconnaissance phase.

upvoted 1 times

 **cri88** 1 month, 2 weeks ago

Selected Answer: C

C. Footprinting the internal network

Explanation: The AXFR request is typically used by attackers to obtain a complete list of DNS records, which can reveal internal IP addresses and hostnames, thereby providing a detailed map of the internal network. This information can then be used for further attacks, such as identifying critical systems or planning network intrusions.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 295 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 295

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst at an organization observed several user logins from outside the organization's network. The analyst determined that these logins were not performed by individuals within the organization. Which of the following recommendations would reduce the likelihood of future attacks? (Choose two.)

- A. Disciplinary actions for users
- B. Conditional access policies Most Voted
- C. More regular account audits
- D. Implementation of additional authentication factors Most Voted
- E. Enforcement of content filtering policies
- F. A review of user account permissions

[Hide Answer](#)

Suggested Answer: BD

Community vote distribution

BD (100%)

by [a4e15bd](#) at Aug. 13, 2024, 6:03 p.m.

Comments

✉ [cri88](#) 1 month, 2 weeks ago

Selected Answer: BD

B. Conditional access policies

D. Implementation of additional authentication factors

Explanation:

B. Conditional access policies: Implementing conditional access policies can restrict access based on certain conditions, such as geographical location, device compliance, or risk level. This would help prevent unauthorized logins from outside the organization's network.

D. Implementation of additional authentication factors: Adding multi-factor authentication (MFA) provides an extra layer of security, making it much harder for unauthorized individuals to gain access even if they have the correct credentials.

upvoted 1 times

 **a4e15bd** 1 month, 3 weeks ago

B&D

Conditional access policies restrict access based on certain conditions such as location, device type or risk level and if anything suspicious is detected, conditional access can block those attempts.

MFAL on the other hand is a strong security measure that adds an extra layer of verification.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 296 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 296

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security team is addressing a risk associated with the attack surface of the organization's web application over port 443. Currently, no advanced network security capabilities are in place. Which of the following would be best to set up? (Choose two.)

A. NIDS Most Voted

B. Honeypot

C. Certificate revocation list

D. HIPS

E. WAF Most Voted

F. SIEM

[Hide Answer](#)

Suggested Answer: AE

Community vote distribution

AE (75%)	13%	13%
----------	-----	-----

by [a4e15bd](#) at Aug. 14, 2024, 2:24 a.m.

Comments

Ty13 1 week, 1 day ago

Selected Answer: AE

A. NIDS

E. WAF

They're asking for setting things up. So set up a WAF and then a NIDS - anomalies would alert admins to take action.

SIEM is good because it's still collecting data, but it's more about overall data security whereas NIDS is specifically for the network.
upvoted 1 times

Szajba123 3 weeks, 4 days ago

Selected Answer: EF

Why:

E. WAF (Web Application Firewall):

A WAF is specifically designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It can help prevent attacks such as SQL injection, cross-site scripting (XSS), and other common web-based threats. Setting up a WAF on port 443 (which is used for HTTPS traffic) would directly address risks associated with web application vulnerabilities.

F. SIEM (Security Information and Event Management):

A SIEM system collects and analyzes security data from across the network, including logs and events from the web application. It provides real-time analysis, helps in detecting anomalies, and assists in responding to potential threats. This would complement the WAF by providing a broader view of security incidents and facilitating incident response.

upvoted 1 times

 **ef5549f** 1 month, 1 week ago

GPT: A & E

upvoted 1 times

 **a4e15bd** 1 month, 2 weeks ago

Selected Answer: DE

Changing my previous answer. I got with D & E. Together these two tools should provide a comprehensive defense securing both the application and the underlying server.

upvoted 1 times

 **suleman1000** 1 month, 2 weeks ago

Selected Answer: AE

NIDS and WAF

upvoted 1 times

 **cri88** 1 month, 2 weeks ago

Selected Answer: AE

E. WAF (Web Application Firewall)

A. NIDS (Network Intrusion Detection System)

Explanation:

E. WAF (Web Application Firewall): A WAF specifically protects web applications by filtering and monitoring HTTP/HTTPS traffic between a web application and the internet. It can help detect and block attacks targeting the web application, such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities.

A. NIDS (Network Intrusion Detection System): NIDS monitors network traffic for suspicious activity and potential threats. Deploying NIDS can help detect malicious activity at the network level, including attempts to exploit vulnerabilities over port 443.

These two options would significantly enhance the security of the web application by providing both application-level protection (WAF) and network-level monitoring (NIDS).

upvoted 1 times

 **nnyankee718** 1 month, 3 weeks ago

Selected Answer: AE

Could be A and F also?

NIDS (Network Intrusion Detection System):

This system monitors network traffic for potential malicious activity, including attempts to exploit vulnerabilities in the web application. While it primarily detects rather than prevents, it provides valuable insights into potential threats and alerts the security team

upvoted 3 times

 **mr_reyes** 1 month, 3 weeks ago

Doesn't SIEM only monitor and report, not actually prevent? Wouldn't HIPS be more appropriate?

upvoted 3 times

 **a4e15bd** 1 month, 3 weeks ago

WAF and SIEM are correct answers.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 297 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 297

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator would like to create a point-in-time backup of a virtual machine. Which of the following should the administrator use?

- A. Replication
- B. Simulation
- C. Snapshot
- D. Containerization

[Hide Answer](#)

Suggested Answer: C

by [Muhammad_Umair](#) at Aug. 18, 2024, 11:14 a.m.

Comments

✉ **Muhammad_Umair** 1 month, 3 weeks ago

C) As We can take screenshot of current state of a VM.
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for

your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 298 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 298

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security administrator notices numerous unused, non-compliant desktops are connected to the network. Which of the following actions would the administrator most likely recommend to the management team?

- A. Monitoring
- B. Decommissioning Most Voted
- C. Patching
- D. Isolating

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [qacollin](#) at Aug. 6, 2024, 3:06 p.m.

Comments

✉ [qacollin](#) 2 months ago

Selected Answer: B

Decommissioning unused and non-compliant desktops will reduce security risks by removing potential points of vulnerability from the network. This action helps to ensure that only compliant and necessary devices are connected, maintaining the integrity and security of the network.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 299 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 299

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?

- A. Sanitization
- B. Formatting
- C. Degaussing
- D. Defragmentation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by  [a4e15bd](#) at Aug. 14, 2024, 2:35 a.m.

Comments

  [a4e15bd](#)  3 months, 1 week ago

Sanitization is the process of removing sensitive data from a storage device in a manner that ensures the data cannot be recovered while allowing the device to be reused. This involves methods like overwriting the data with zeros or other patterns multiple times.

upvoted 6 times

  [01a4c2e](#)  1 month ago

 **Selected Answer: A**

A. Sanitization - Sanitization refers to the process of removing data from a storage device in such a way that the data cannot be recovered. This can include methods like overwriting the data multiple times, which ensures that the drives can be reused safely.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 300 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 300

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization wants to improve the company's security authentication method for remote employees. Given the following requirements:

- Must work across SaaS and internal network applications
- Must be device manufacturer agnostic
- Must have offline capabilities

Which of the following would be the most appropriate authentication method?

- A. Username and password
- B. Biometrics
- C. SMS verification
- D. Time-based tokens Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [a4e15bd](#) at Aug. 14, 2024, 2:41 a.m.

Comments

[a4e15bd](#) Highly Voted 1 month, 3 weeks ago

D. Time-based tokens

These tokens generate a unique code that changes every 30 or 60 seconds. They work across various platforms including SaaS and internal applications, are device manufacturer agnostic and can be used offline.

upvoted 5 times

[Cee007](#) Most Recent 1 month, 1 week ago

Selected Answer: D

D. Time-based tokens.

Time-based tokens work across various platforms including SaaS and internal applications, are device manufacturer agnostic and can be used offline.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 301 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 301

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security officer is implementing a security awareness program and has placed security-themed posters around the building and assigned online user training. Which of the following will the security officer most likely implement?

- A. Password policy
- B. Access badges
- C. Phishing campaign
- D. Risk assessment

[Hide Answer](#)

Suggested Answer: C

by [a4e15bd](#) at Aug. 14, 2024, 2:45 a.m.

Comments

[a4e15bd](#) 1 month, 3 weeks ago

C. Phishing campaign

This is simulating phishing attacks to educate employees about recognizing and handling of phishing attempts.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 302 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 302

Topic #: 1

[\[All SY0-701 Questions\]](#)

A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?

- A. DDoS attack
- B. Rogue employee
- C. Insider threat
- D. Supply chain Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by  [qacollin](#) at Aug. 12, 2024, 6:40 p.m.

Comments

 [dhewa](#) 1 week, 6 days ago

Selected Answer: D

This type of vulnerability occurs when a malicious update affects a software platform that many organizations rely on, highlighting risks associated with third-party software and dependencies.

upvoted 2 times

 [qacollin](#) 1 month, 3 weeks ago

Selected Answer: D

D. GPT

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 303 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 303

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company web server is initiating outbound traffic to a low-reputation, public IP on non-standard port. The web server is used to present an unauthenticated page to clients who upload images to the company. An analyst notices a suspicious process running on the server that was not created by the company development team. Which of the following is the most likely explanation for this security incident?

- A. A web shell has been deployed to the server through the page.
- B. A vulnerability has been exploited to deploy a worm to the server.
- C. Malicious insiders are using the server to mine cryptocurrency.
- D. Attackers have deployed a rootkit Trojan to the server over an exposed RDP port.

[Hide Answer](#)

Suggested Answer: A

by [a4e15bd](#) at Aug. 14, 2024, 2:53 a.m.

Comments

✉ **a4e15bd** 1 month, 3 weeks ago

A. A web shell has been deployed to the server through the page.
The shell would allow the attacker to gain unauthorized access and control over the server.
upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 304 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 304

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization requests a third-party full-spectrum analysis of its supply chain. Which of the following would the analysis team use to meet this requirement?

- A. Vulnerability scanner
- B. Penetration test
- C. SCAP Most Voted
- D. Illumination tool Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (50%)	C (36%)	14%
---------	---------	-----

by RoRoYourBoat at Aug. 10, 2024, 10:15 p.m.

Comments

✉ a4e15bd Highly Voted 1 month, 3 weeks ago

Answer is C, SCAP.

SCAP offers framework for automating security compliance and vulnerability assessments which is crucial for a comprehensive analysis of security and compliance aspects across the supply chain.

upvoted 6 times

✉ User92 Most Recent 5 hours, 9 minutes ago

Selected Answer: D

An illumination tool is specifically designed to provide a comprehensive, full-spectrum analysis of a supply chain. SCAP, are more focused on cybersecurity aspects rather than providing a holistic view of the supply chain.

upvoted 1 times

✉ Ty13 1 week ago

Selected Answer: D

D. Illumination Tool

It's for the Supply Chain. SCAP is for software/security flaws.

upvoted 2 times

✉ **nap61** 1 week, 2 days ago

Selected Answer: D
Vulnerability feeds make use of common identifiers to facilitate sharing of intelligence data across different platforms. Many vulnerability scanners use the Security Content Automation Protocol (SCAP) to obtain feed or plug-in updates (scap.nist.gov).

upvoted 1 times

✉ **weusubu** 1 week, 4 days ago

In the SY0701 Student guide I was provided, there is no mention of SCAP standing for Supply Chain Assessment Process. It doesn't even refer to that process anywhere in the book. It does show a SCAP acronym for Security Content Automation Protocol. For those of us who are already struggling to memorize acronyms, can someone please advise on which definition for SCAP is correct?

upvoted 3 times

✉ **myazureexams** 2 weeks, 5 days ago

Selected Answer: C

Answer is C

The analysis team would typically use a Supply Chain Assessment Process (SCAP) to meet the requirement of a full-spectrum analysis of the organization's supply chain. An Illumination Tool is not a standard term used in this context, and SCAP is specifically designed for supply chain evaluations.

upvoted 2 times

✉ **Exemplary** 6 days, 5 hours ago

Supply Chain Assessment Process is not a thing. SCAP stands for Security Content Automation Protocol.

upvoted 1 times

✉ **cri88** 2 weeks, 6 days ago

Selected Answer: D

An illumination tool is designed to provide visibility and analysis across various stages of the supply chain, helping organizations identify risks, dependencies, and inefficiencies. It covers the full spectrum of supply chain analysis, which is what the organization is requesting.

SCAP (C), while useful for automating security assessments and compliance, is focused on system vulnerabilities and security baselines, not the broader supply chain visibility and operational analysis required for full-spectrum supply chain evaluation.

upvoted 2 times

✉ **17f9ef0** 4 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

✉ **17f9ef0** 4 weeks ago

Correction, answer is actually D

upvoted 1 times

✉ **dhewa** 1 month, 2 weeks ago

Selected Answer: D

An illumination tool is designed to map out and visualize complex supply chain networks. It provides end-to-end visibility, identifies risks, ensures compliance, and optimizes performance, making it ideal for a full-spectrum analysis of a supply chain.

upvoted 1 times

✉ **cri88** 1 month, 2 weeks ago

Selected Answer: D

The correct answer is D. Illumination tool.

An illumination tool is designed to provide a comprehensive overview and analysis of a supply chain, identifying risks, vulnerabilities, and potential points of failure across the entire spectrum.

The other options are typically more focused on cybersecurity:

- A. Vulnerability scanner is used to identify security vulnerabilities within a network or system.
- B. Penetration test simulates an attack on a system to identify weaknesses.
- C. SCAP (Security Content Automation Protocol) is used to automate vulnerability management, policy compliance, and security measurement. For a full-spectrum analysis of a supply chain, an illumination tool would be more appropriate.

upvoted 4 times

✉ **Kingamj** 1 month, 3 weeks ago

Selected Answer: C

ChatGPT

upvoted 2 times

 **qacollin** 1 month, 3 weeks ago

Selected Answer: C

C. GPT

upvoted 2 times

 **RoRoRoYourBoat** 1 month, 3 weeks ago

Selected Answer: B

B. Penetration test: A penetration test (or pen test) involves simulating cyberattacks to identify vulnerabilities and weaknesses in the supply chain. This comprehensive approach helps in understanding the security posture and potential risks across the entire supply chain.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 305 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 305

Topic #: 1

[\[All SY0-701 Questions\]](#)

A systems administrator deployed a monitoring solution that does not require installation on the endpoints that the solution is monitoring. Which of the following is described in this scenario?

A. Agentless solution Most Voted

B. Client-based soon

C. Open port

D. File-based solution

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by [abbey0922](#) at Aug. 28, 2024, 6:55 a.m.

Comments

✉ [abbey0922](#) 1 month, 1 week ago

Selected Answer: A

Agentless monitoring does not require the installation of software on the target device. It uses standard protocols to collect information, making it less intrusive and less resource intensive.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 306 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 306

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst is reviewing the source code of an application in order to identify misconfigurations and vulnerabilities. Which of the following kinds of analysis best describes this review?

- A. Dynamic
- B. Static Most Voted
- C. Gap
- D. Impact

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by  [Sigepneo01](#) at Aug. 25, 2024, 2:45 p.m.

Comments

 [cri88](#) 3 weeks ago

Selected Answer: B

Static analysis refers to reviewing the source code of an application without executing it, in order to identify misconfigurations, vulnerabilities, and potential security flaws. This is the type of analysis the security analyst is performing by examining the code directly.

Dynamic analysis (A) involves analyzing the application while it is running, to detect vulnerabilities that only appear during execution. Gap analysis (C) identifies discrepancies between current security measures and desired standards, but is not focused on source code review. Impact analysis (D) assesses the potential consequences of identified vulnerabilities but is not the process of reviewing source code directly.
upvoted 1 times

 [Sigepneo01](#) 1 month, 1 week ago

Static code analysis entails the review of source code and it is static because it is not running on a computer. This is the opposite of dynamic code analysis which is done while the code is actually executing on the computer system.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 307 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 307

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following agreement types is used to limit external discussions?

- A. BPA
- B. NDA Most Voted
- C. SLA
- D. MSA

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by [TrebleSmith](#) at Sept. 4, 2024, 1:29 p.m.

Comments

✉ [TrebleSmith](#) 1 month ago

Selected Answer: B

A Non-Disclosure Agreement is a legal document prohibiting the disclosure of details that are agreed upon under the NDA. This will include limiting external discussions.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 308 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 308

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

- A. Internal audit
- B. Penetration testing
- C. Attestation
- D. Due diligence Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by Cee007 at Sept. 5, 2024, 5:45 p.m.

Comments

✉️ cri88 3 weeks ago

Selected Answer: D

D. Due diligence

In this context, due diligence refers to the process of evaluating the security, compliance, and risk associated with a third-party vendor or service, such as a SaaS application. Requesting a SOC 2 report is a common part of the due diligence process to assess the vendor's controls related to security, availability, processing integrity, confidentiality, and privacy.

Internal audit (A) refers to an organization's internal review of its own processes, not an external vendor.

Penetration testing (B) involves actively testing for vulnerabilities by simulating attacks, which is not applicable here.

Attestation (C) refers to a third-party audit or certification, such as the SOC 2 report itself, but the analyst is conducting due diligence by requesting the report.

upvoted 2 times

✉️ PAWarriors 3 weeks, 4 days ago

Selected Answer: D

Security challenges with Software-as-a-Service (SaaS) providers --> Vendor selection should consider due diligence, historical performance and commitment to security

upvoted 1 times

 **Cee007** 1 month ago

Selected Answer: D

D. Due diligence

Due diligence in this context involves evaluating the security, availability, processing integrity, confidentiality, and privacy of the SaaS application by reviewing the SOC 2 report provided by the vendor. This process helps ensure that the vendor meets the required security and operational standards before the SaaS application is implemented.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 309 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 309

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is used to conceal credit card information in a database log file?

A. Tokenization

B. Masking Most Voted

C. Hashing

D. Obfuscation

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (100%)

by Cee007 at Sept. 5, 2024, 5:46 p.m.

Comments

✉️ cri88 3 weeks ago

Selected Answer: B

B. Masking

Masking is used to conceal sensitive information, such as credit card numbers, by replacing or hiding parts of the data. In the context of database log files, masking ensures that sensitive information is not exposed while maintaining the usability of the data for other purposes.

Tokenization (A) replaces sensitive data with a token that can only be mapped back to the original data using a secure system, but it is not typically used for log file entries.

Hashing (C) converts data into a fixed-length hash, but it's a one-way function, making it unsuitable if the original data needs to be retrieved. Obfuscation (D) refers to making data less understandable but is less structured and secure than masking for specific data like credit card numbers.

upvoted 4 times

✉️ Cee007 1 month ago

Selected Answer: B

B. Masking

Masking involves altering the credit card information in such a way that it is not easily readable or identifiable while still retaining some format or structure for processing or display purposes. This is particularly useful for ensuring sensitive data is protected in log files or other records.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 310 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 310

Topic #: 1

[\[All SY0-701 Questions\]](#)

SIMULATION

-

A systems administrator is configuring a site-to-site VPN between two branch offices. Some of the settings have already been configured correctly. The systems administrator has been provided the following requirements as part of completing the configuration:

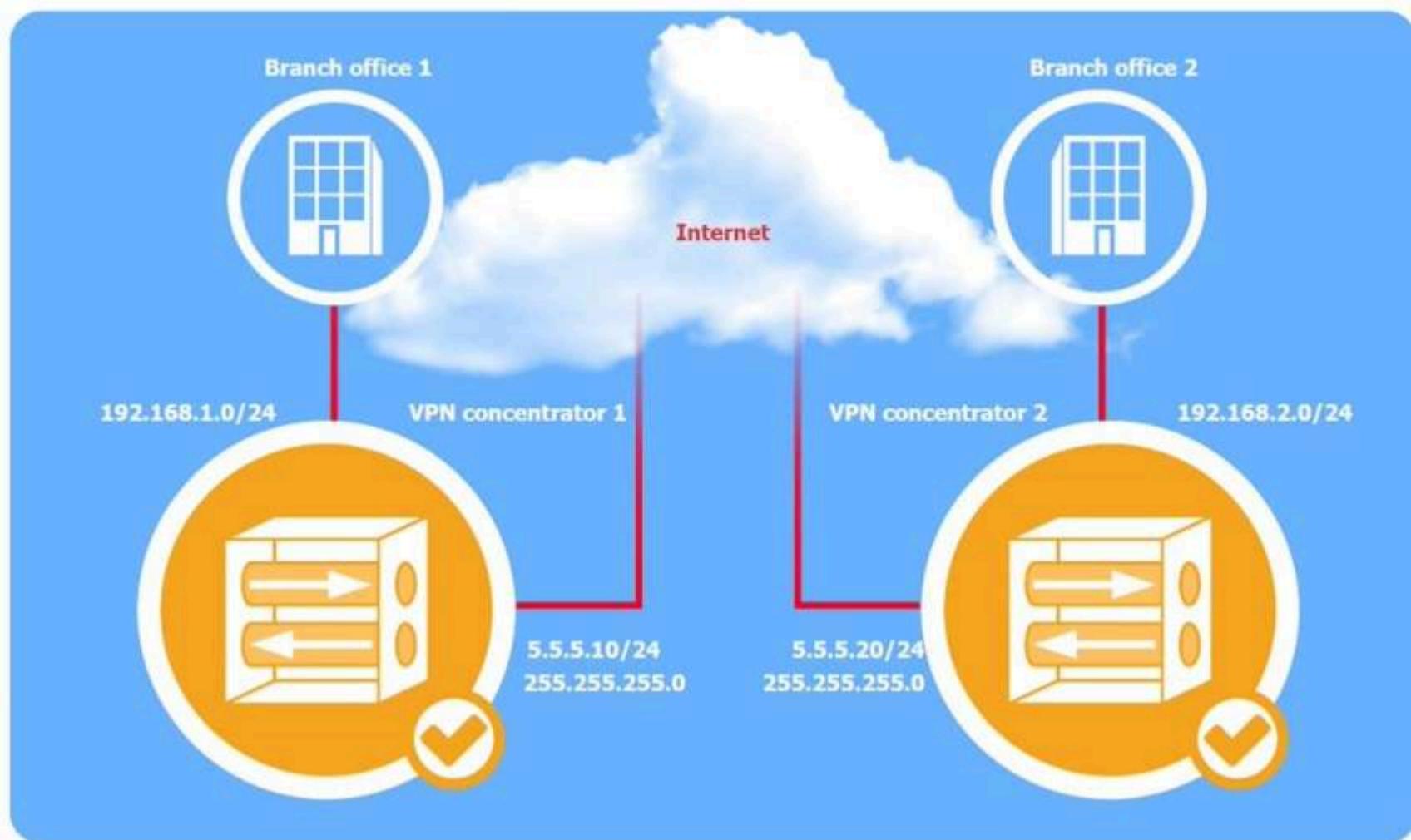
- Most secure algorithms should be selected
- All traffic should be encrypted over the VPN
- A secret password will be used to authenticate the two VPN concentrators

INSTRUCTIONS

-

Click on the two VPN Concentrators to configure the appropriate settings.

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



VPN Concentrator 1

Phase 1 Phase 2

Peer IP address:

Auth method:
PKI
PSK
RADIUS

Negotiation mode: MAIN

Encryption algorithm:
AES256
ECC secp160r1
3DES

Hash algorithm:
SHA256
MD5
SHA1

DH key group: 14

VPN Concentrator 1

Phase 1 Phase 2

Mode: Tunnel

Protocol:

- Select
- ESP
- AH

Encryption algorithm:

- Select
- 3DES
- AES256
- BLOWFISH

Hash algorithm:

- Select
- SHA256
- MD5
- SHA1

Local network/mask:

Remote network/mask:

Reset to Default **Save** **Close**

VPN Concentrator 2

Phase 1 Phase 2

Peer IP address:

Auth method:

- Select
- PKI
- RADIUS
- PSK

Negotiation mode: MAIN

Encryption algorithm:

- Select
- 3DES
- AES256
- ECC secp160r1

Hash algorithm:

- Select
- SHA256
- SHA1
- MD5

DH key group: 14

Reset to Default **Save** **Close**

VPN Concentrator 2

Phase 1 **Phase 2**

Mode: Tunnel

Protocol:

- Select
- ESP
- AH

Encryption algorithm:

- Select
- BLOWFISH
- 3DES
- AES256

Hash algorithm:

- Select
- SHA256
- SHA1
- MD5

Local network/mask:

Remote network/mask:

Reset to Default **Save** **Close**

The dialog box is titled "VPN Concentrator 2". It has two tabs: "Phase 1" and "Phase 2", with "Phase 2" currently selected. Under "Phase 2", there are four main configuration sections: "Protocol", "Encryption algorithm", "Hash algorithm", and two network-related fields ("Local network/mask" and "Remote network/mask"). Each section contains a dropdown menu with specific options. The "Protocol" dropdown shows "Select", "ESP", and "AH". The "Encryption algorithm" dropdown shows "Select", "BLOWFISH", "3DES", and "AES256". The "Hash algorithm" dropdown shows "Select", "SHA256", "SHA1", and "MD5". At the bottom of the dialog are three buttons: "Reset to Default", "Save" (highlighted in green), and "Close".

Hide Answer

VPN Concentrator 1

Phase 1 **Phase 2**

Peer IP address: **5.5.5.20**

Auth method: Select
PKI
PSK
RADIUS

Negotiation mode: MAIN

Encryption algorithm: Select
AES256
ECC secp160r1
3DES

Hash algorithm: Select
SHA256
MD5
SHA1

DH key group: 14

Reset to Default **Save** **Close**

VPN Concentrator 1

Phase 1 **Phase 2**

Mode: Tunnel

Protocol: Select
ESP
AH

Encryption algorithm: Select
3DES
AES256
BLOWFISH

Hash algorithm: Select
SHA256
MD5
SHA1

Local network/mask: **255.255.255.0**

Remote network/mask: **255.255.255.0**

Reset to Default **Save** **Close**

Suggested Answer:

VPN Concentrator 2

Phase 1 **Phase 2**

Peer IP address: **5.5.5.10**

Auth method: Select
PKI
PSK
RADIUS

Negotiation mode: MAIN

Encryption algorithm: Select
AES256
ECC secp160r1
3DES

Hash algorithm: Select
SHA256
MD5
SHA1

DH key group: 14

Reset to Default **Save** **Close**

VPN Concentrator 2

Phase 1 **Phase 2**

The screenshot shows a configuration dialog for a VPN tunnel. The 'Mode' is set to 'Tunnel'. Under 'Protocol', 'ESP' is selected. In the 'Encryption algorithm' dropdown, 'AES256' is highlighted. The 'Hash algorithm' dropdown shows 'SHA256' as the selected option. The 'Local network/mask' field contains '255.255.255.0' and the 'Remote network/mask' field contains '255.255.255.0'. At the bottom are three buttons: 'Reset to Default', 'Save' (which is green), and 'Close'.

by TrebleSmith at Sept. 4, 2024, 4:44 p.m.

Comments

TrebleSmith Highly Voted 1 month ago
VPN Concentrator 1 (Branch Office 1) Configuration:

Phase 1:
Peer IP address: 5.5.5.20 (IP of VPN Concentrator 2)
Auth method: PSK (Pre-Shared Key)
Negotiation mode: MAIN
Encryption algorithm: AES256
Hash algorithm: SHA256
DH key group: 14

Phase 2:
Mode: Tunnel
Protocol: ESP (Encapsulating Security Payload)
Encryption algorithm: AES256
Hash algorithm: SHA256
Local network/mask: 192.168.1.0/24
Remote network/mask: 192.168.2.0/24

VPN Concentrator 2 (Branch Office 2) Configuration:

Phase 1:
Peer IP address: 5.5.5.10 (IP of VPN Concentrator 1)
Auth method: PSK (Pre-Shared Key)
Negotiation mode: MAIN
Encryption algorithm: AES256
Hash algorithm: SHA256
DH key group: 14

Phase 2:
Mode: Tunnel
Protocol: ESP (Encapsulating Security Payload)
Encryption algorithm: AES256
Hash algorithm: SHA256
Local network/mask: 192.168.2.0/24
Remote network/mask: 192.168.1.0/24
upvoted 10 times

Ty13 1 week ago
Auth should be PKI, not PSK. PKI is more secure than PSK.
upvoted 1 times

Ty13 1 week ago
Nevermind, I just realized the question asked for PSK specifically.
upvoted 1 times

koala_lay 3 weeks, 2 days ago
Special thanks to your valuable discussion.
upvoted 2 times

TrebleSmith 1 month ago

I supplied ChatGPT with all of the images included in this PBQ and these are the results. I am putting this out here as a discussion starter in case there are any issues with the answer supplied to me, as there are no comments at the time of me posting this.

upvoted 5 times

 **bobernb** Most Recent 4 days, 6 hours ago

I agree with TrebleSmith's answers, but I'm not sure about local network/mask and remote network/mask for both concentrators. I suppose that these ask for subnet masks which are
VPN Concentrator 1, Phase 2:
Local network/mask: 255.255.255.0
Remote network/mask: 255.255.255.0

VPN Concentrator 2, Phase 2:
Local network/mask: 255.255.255.0
Remote network/mask: 255.255.255.0

Please, tell me what you think

upvoted 1 times

 **RobJob** 1 day, 2 hours ago

/24 is the same as 255.255.255.0

upvoted 1 times

 **bobernb** 3 days, 13 hours ago

Nevermind, I've just learned what is CIDR notation, and I agree with all of TrebleSmith's answers.

upvoted 1 times

 **Deathstrangler** 3 weeks, 2 days ago

@PAWarriors How did you get the local area network and the remote mask

upvoted 2 times

 **PAWarriors** 3 weeks, 3 days ago

Correct information:

VPN Concentrator 1 (Branch Office 1) Configuration:

Phase 1:

Peer IP address: 5.5.5.20 (IP of VPN Concentrator 2)
Auth method: PSK (Pre-Shared Key)
Negotiation mode: MAIN
Encryption algorithm: AES256
Hash algorithm: SHA256
DH key group: 14

Phase 2:

Mode: Tunnel
Protocol: ESP (Encapsulating Security Payload)
Encryption algorithm: AES256
Hash algorithm: SHA256
Local network/mask: 192.168.1.0/24
Remote network/mask: 192.168.2.0/24

VPN Concentrator 2 (Branch Office 2) Configuration:

Phase 1:

Peer IP address: 5.5.5.10 (IP of VPN Concentrator 1)
Auth method: PSK (Pre-Shared Key)
Negotiation mode: MAIN
Encryption algorithm: AES256
Hash algorithm: SHA256
DH key group: 14

Phase 2:

Mode: Tunnel
Protocol: ESP (Encapsulating Security Payload)
Encryption algorithm: AES256
Hash algorithm: SHA256
Local network/mask: 192.168.2.0/24
Remote network/mask: 192.168.1.0/24

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 311 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 311

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service. Which of the following is the engineer most likely to deploy?

- A. Layer 4 firewall
- B. NGFW
- C. WAF Most Voted
- D. UTM

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Cee007](#) at Sept. 5, 2024, 6:02 p.m.

Comments

✉ [cri88](#) 3 weeks ago

Selected Answer: C

C. WAF (Web Application Firewall)

A Web Application Firewall (WAF) is specifically designed to protect web applications by filtering, monitoring, and blocking HTTP/S traffic to and from a web service. Since the organization is hosting a new service through a web portal, a WAF would be the most appropriate solution to protect against common web-based attacks like SQL injection, cross-site scripting (XSS), and other OWASP Top 10 threats.

Layer 4 firewall (A) provides protection at the transport layer, which is too low-level to specifically protect web applications. NGFW (Next-Generation Firewall) (B) adds application-level filtering and protection, but is generally broader in scope, not specifically tailored to web applications.

UTM (Unified Threat Management) (D) is a multi-functional security device but doesn't provide the specialized web application protection that a WAF offers.

Thus, WAF is the most suitable solution for protecting a web service accessed via a portal.

upvoted 1 times

 **FrozenCarrot** 3 weeks, 2 days ago

Portal -> WAF
upvoted 1 times

 **Cee007** 1 month ago

Selected Answer: C
C. WAF (Web Application Firewall)

A WAF is specifically designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. It can help prevent attacks such as SQL injection, cross-site scripting (XSS), and other web-based threats that could target the new service accessed through the web portal.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 312 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 312

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following topics would most likely be included within an organization's SDLC?

- A. Service-level agreements
- B. Information security policy
- C. Penetration testing methodology
- D. Branch protection requirements Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (50%)

C (30%)

B (20%)

by [Ayokunle01](#) at Sept. 4, 2024, 4:30 p.m.

Comments

✉️ **User92** 2 hours, 21 minutes ago

Selected Answer: D

Branch protection requirements are directly related to the software development process, particularly in version control and code management. These requirements help ensure that only reviewed and approved code is merged into the main branch, maintaining the integrity and quality of the software throughout its development lifecycle.

Why not B: Information security policy is a broader organizational policy that governs overall security practices.

Why not C: Penetration testing methodology is part of security testing but not specifically tied to the SDLC phases.

upvoted 1 times

✉️ **khank14** 4 days, 16 hours ago

so many different answers

upvoted 1 times

✉️ **dhewa** 1 week, 5 days ago

Selected Answer: B

This is because an information security policy outlines the guidelines and practices for protecting sensitive data throughout the development process.

upvoted 1 times

Lavette 2 weeks, 4 days ago

C. Penetration testing methodology is often part of the SDLC, especially in the testing phase, to identify vulnerabilities in the software before it goes live. While the other options are important in the broader organizational policies and security management, they are not typically a direct part of the SDLC process.

upvoted 1 times

cri88 2 weeks, 6 days ago

Selected Answer: B

B. Information security policy

An Information security policy is often included within an organization's Software Development Life Cycle (SDLC) because security considerations are critical during the design, development, and deployment phases of software development. The SDLC aims to integrate security measures throughout the process to protect against vulnerabilities and ensure compliance with security standards.

Service-level agreements (A) are more related to contracts and service performance rather than the SDLC.

Penetration testing methodology (C) is typically used for post-development testing, not a core part of the SDLC.

Branch protection requirements (D) relate to source code management and version control, but they are not commonly included as a core topic of the SDLC.

Thus, Information security policy aligns most closely with the SDLC's focus on incorporating security best practices throughout the software development process.

upvoted 1 times

17f9ef0 4 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

a4e15bd 4 weeks, 1 day ago

Selected Answer: C

The correct answer is C in this context. Pen Testing methodology could be part of the SDLC and directly relevant to the testing and security assurance phases of software development.

D is incorrect because Branch Protection Requirements is more related to security measures around the physical or network infrastructure not software development.

upvoted 1 times

Cee007 1 month ago

Selected Answer: D

D. Branch protection requirements

Branch protection requirements are related to the version control and development process within the SDLC, ensuring that code changes are reviewed, tested, and approved before being merged into main branches. This helps maintain code quality and security throughout the development process.

Penetration testing is usually conducted as part of the testing phase or after deployment to identify vulnerabilities and security weaknesses. It is a separate process from the core stages of the SDLC but is an important aspect of ensuring the security and robustness of the application once development is completed.

upvoted 4 times

koala_lay 3 weeks, 2 days ago

Agree to answer D.

upvoted 1 times

Ayokunle01 1 month ago

B. Information security policy

An organization's Software Development Life Cycle (SDLC) typically includes information security policy to ensure that software development aligns with the organization's overall security posture. This policy outlines security requirements, standards, and guidelines for software development.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 313 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 313

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following control types is AUP an example of?

- A. Physical
- B. Managerial
- C. Technical
- D. Operational Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (67%)

B (33%)

by [Syl0](#) at Sept. 4, 2024, 3:02 p.m.

Comments

✉️ **User92** 4 hours, 54 minutes ago

Selected Answer: D

In fact, Comptia asks the same practical question and uses AUP as the example of operational controls.
upvoted 1 times

✉️ **Exemplary** 6 days, 4 hours ago

Selected Answer: B

Direct from Dion Training's Udemy course:
Managerial Controls - Aka administrative controls. Involve the strategic planning and governance side of security. Ensures that the org's security strategies align with its business goals and its risk tolerance.
Risk assessments
Security policies
Training programs
Incident response strategies

Operational Controls - Procedures and measures designed to protect data on a day-to-day basis and are mainly governed by internal processes and human actions.

Backup procedures
Account reviews
User awareness training programs

AUP = Acceptable Use Policy. Security policies = Managerial Controls.

upvoted 1 times

 **Chrissyy6111** 1 week, 2 days ago

Selected Answer: D

D. Operational. Comptia gives this same practice question and uses AUP as an specific example of operational controls.
upvoted 3 times

 **RIDA_007** 1 week, 5 days ago

Managerial controls are tend to be directive such as policies, hence I am gowing with B.
Remember that operational controls are driven by people like security guards, more physical in nature.
upvoted 2 times

 **myazureexams** 2 weeks, 5 days ago

Selected Answer: B

Many of you are quoting GPT responses. However, you have to offer the correct prompt. As follows: Operational control or managerial control? The choices are managerial or operational. I understand it is a type of administrative control, but that is not one of the choices. Please explain the best answer:

GPT Answer: Based on the given choices, an Acceptable Use Policy (AUP) would be considered a managerial control. This is because it establishes guidelines and policies that guide the organization's operations, which aligns more with the concept of managerial control.

I am definitely going with Managerial, which was my first answer before consulting GPT. I've also studied for over a year in-depth.
upvoted 2 times

 **PAWarriors** 3 weeks, 3 days ago

Selected Answer: D

D. Operational: Operational controls are procedures and policies that dictate how users should behave and how processes are carried out to ensure security. The AUP falls under this category as it defines acceptable and unacceptable behavior for users, making it an operational control.
upvoted 3 times

 **Hayder81** 3 weeks, 6 days ago

B. Managerial control.

upvoted 1 times

 **Zobo411** 4 weeks ago

Selected Answer: D

GPTTTTTTTTTTTTTTTTT

upvoted 1 times

 **850bc48** 4 weeks, 1 day ago

Chat GPT:

The correct answer is D. Operational.

An Acceptable Use Policy (AUP) is an example of an operational control. It defines the appropriate use of resources, such as networks, systems, and data, by users within an organization. AUPs are administrative in nature and help to manage behavior and actions within an organization's environment, making them part of operational controls.

- A. Physical controls are designed to protect the physical infrastructure, like locks, badges, or surveillance cameras.
 - B. Managerial controls focus on the oversight and management of security policies, such as risk assessments and audits.
 - C. Technical controls (also known as logical controls) include things like firewalls, encryption, and access control systems, which rely on technology to enforce security.
- upvoted 3 times

 **Cee007** 1 month ago

Selected Answer: B

B. Managerial

An AUP is a set of guidelines or rules established by management to dictate acceptable and unacceptable use of organizational resources, such as computers and networks. It is a managerial control designed to ensure that users adhere to security policies and practices.

upvoted 1 times

 **Syl0** 1 month ago

AUP - Acceptable Use Policies

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 314 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 314

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in, so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

- A. Enable SAML.
- B. Create OAuth tokens.
- C. Use password vaulting.
- D. Select an IdP. Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [Syl0](#) at Sept. 4, 2024, 3:03 p.m.

Comments

✉ [850bc48](#) 1 month ago

Chat GPT:

The correct answer is D. Select an IdP (Identity Provider).

The first step in reducing the number of credentials employees must maintain is to select an Identity Provider (IdP). An IdP centralizes authentication and allows users to log in once and gain access to multiple applications, usually through a single sign-on (SSO) mechanism. Once an IdP is in place, other technologies like SAML (Security Assertion Markup Language) or OAuth can be configured to manage authentication with the SaaS applications.

- A. Enable SAML is a protocol used for authentication, but it requires an IdP to manage authentication.
- B. Create OAuth tokens is a way to grant limited access to resources but also requires an IdP or similar system to manage identities.
- C. Use password vaulting is a temporary solution that stores passwords, but it doesn't reduce the need for multiple log-ins, nor does it provide the benefits of centralized identity management.

upvoted 1 times

 **Cee007** 1 month ago

Selected Answer: D

D. Select an IdP (Identity Provider)

Selecting an IdP is the initial step in implementing Single Sign-On (SSO) or federated identity management, which will allow employees to use a single set of credentials to access multiple SaaS applications. After selecting an IdP, the security team can then enable SAML or other SSO protocols to integrate with the applications and manage authentication.

upvoted 2 times

 **Syl0** 1 month ago

IdP - Identity Provider

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 315 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 315

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company's online shopping website became unusable shortly after midnight on January 30, 2023. When a security analyst reviewed the database server, the analyst noticed the following code used for backing up data:

```
IF DATE() = "01/30/2023" THEN BEGIN  
    DROP DATABASE WebShopOnline;  
END
```

Which of the following should the analyst do next?

- A. Check for recently terminated DBAs.
- B. Review WAF logs for evidence of command injection. Most Voted
- C. Scan the database server for malware.
- D. Search the web server for ransomware notes.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

B (75%)

A (25%)

by Cee007 at Sept. 5, 2024, 6:11 p.m.

Comments

myazureexams 2 weeks, 6 days ago

Selected Answer: B

The answer is B.

Based on the provided scenario, the security analyst should prioritize reviewing Web Application Firewall (WAF) logs for evidence of command injection. The unusual database command suggests an unauthorized change, possibly through an injection attack. Checking for recently terminated DBAs is less relevant in this situation.

upvoted 2 times

 PAWarriors 3 weeks, 4 days ago

Selected Answer: B

B. Review WAF logs for evidence of command injection.

The code provided (DROP DATABASE WebShopOnline) suggests that the database was deliberately dropped on a specific date (January 30, 2023). This could potentially be the result of a command injection attack, where an attacker inserts malicious code to manipulate or destroy the database.

upvoted 2 times

 17f9ef0 1 month ago

Selected Answer: B

Answer is B

upvoted 1 times

 a4e15bd 1 month ago

Selected Answer: B

While insider threats are always a possibility, the structure of the code suggest an automated or external trigger, rather than an action by a disgruntled employee. A terminate DBA would likely have direct access to drop the database rather than making such as time specific command. Attackers use SQL injection to execute commands like DROP Database remotely through vulnerable interfaces. So B. Reviewing the WAF logs for evidence of command injection makes the correct answer.

upvoted 1 times

 Cee007 1 month ago

Selected Answer: A

A. Check for recently terminated DBAs.

The code indicates that the database was intentionally dropped based on a specific date, which suggests that someone with access and knowledge of the database setup (such as a database administrator) may have executed or scheduled this command. Checking for recently terminated DBAs could help identify if an insider threat or an ex-employee had a role in this incident.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 316 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 316

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be the best way to test resiliency in the event of a primary power failure?

- A. Parallel processing
- B. Tabletop exercise
- C. Simulation testing
- D. Production failover Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (67%)

C (33%)

by Cee007 at Sept. 5, 2024, 6:12 p.m.

Comments

✉ 17f9ef0 1 month ago

Selected Answer: C

Answer is C
upvoted 1 times

✉ 850bc48 1 month ago

Chat GPT:
The correct answer is D. Production failover.

A production failover is the best way to test resiliency in the event of a primary power failure because it involves switching from the primary system to a backup system in a real-world environment. This tests the actual failover processes and infrastructure under real conditions, ensuring that systems can continue to operate if the primary power source fails.

- A. Parallel processing is related to computing performance and efficiency, not specifically to power resiliency.
- B. Tabletop exercise is a discussion-based exercise to simulate scenarios, but it doesn't provide practical validation of systems under actual failover conditions.

C. Simulation testing is a hypothetical or virtual test that can assess various failure scenarios, but it doesn't fully replicate the impact of a real production failover.

upvoted 2 times

 **Cee007** 1 month ago

Selected Answer: D

D. Production failover

Production failover involves switching to a backup power source or system to ensure that operations continue seamlessly in the event of a primary power failure. This type of testing verifies that the failover mechanisms work as intended under real-world conditions and ensures that the system can handle the transition smoothly.

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 317 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 317

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be the most appropriate way to protect data in transit?

- A. SHA-256
- B. SSL3.0
- C. TLS 1.3 Most Voted
- D. AES-256

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (100%)

by [Syl0](#) at Sept. 5, 2024, 2:04 p.m.

Comments

✉ [a4e15bd](#) 4 weeks ago

Selected Answer: C

TLS for sure. Easy one.
upvoted 2 times

✉ [850bc48](#) 1 month ago

Chat GPT:The correct answer is C. TLS 1.3.

TLS (Transport Layer Security) 1.3 is the most appropriate protocol for protecting data in transit, as it provides encryption, integrity, and secure authentication between two communicating parties. It is an updated, secure version of SSL/TLS and is widely recommended for secure communication over networks.

- A. SHA-256 is a hashing algorithm, primarily used for ensuring data integrity, not for encrypting data in transit.
- B. SSL 3.0 is an outdated and vulnerable protocol that should no longer be used for securing data.
- C. TLS 1.3 is the most appropriate protocol for protecting data in transit, as it provides encryption, integrity, and secure authentication between two communicating parties.
- D. AES-256 is an encryption algorithm, but it is typically used for data at rest or as part of protocols like TLS for data in transit; by itself, it is not a protocol for securing data in transit.

upvoted 2 times

 **Cee007** 1 month ago

Selected Answer: C

C. TLS 1.3

Transport Layer Security (TLS) 1.3 is the latest version of the TLS protocol and provides strong encryption for securing data in transit between clients and servers. It offers improved security and performance compared to previous versions like SSL 3.0 and earlier TLS versions.

upvoted 1 times

 **Syl0** 1 month ago

TLS sounds right...

SHA256 is a hash

SSL 3.0 is fused for HTTPS

TLS is for data in transit

AES256 is for data at rest

upvoted 2 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 318 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 318

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a common, passive reconnaissance technique employed by penetration testers in the early phases of an engagement?

- A. Open-source intelligence Most Voted
- B. Port scanning
- C. Pivoting
- D. Exploit validation

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

A (100%)

by Cee007 at Sept. 5, 2024, 6:15 p.m.

Comments

✉️ **a4e15bd** 4 weeks ago

Selected Answer: A

correct answer if A. OSINT
upvoted 1 times

✉️ **850bc48** 1 month ago

Chat GPT:
The correct answer is A. Open-source intelligence (OSINT).

OSINT is a common passive reconnaissance technique where penetration testers gather information from publicly available sources, such as websites, social media, and databases, without directly interacting with the target systems. This helps them learn more about the target while minimizing the chances of detection.

Options B, C, and D involve more active techniques, which usually come later in the penetration testing process:

B. Port scanning is an active technique to identify open ports and services on a target.

- C. Pivoting refers to using a compromised system to gain access to other systems within a network.
- D. Exploit validation involves testing vulnerabilities to confirm whether they can be successfully exploited.

upvoted 1 times

 abbey0922 1 month ago

Selected Answer: A

Passive reconnaissance gathers information about the target system without contacting it directly. An open source intelligence (OSINT) investigation can discover publicly available information about the target system. The utility of such information depends on the type of penetration test

upvoted 1 times

 Cee007 1 month ago

Selected Answer: A

A. Open-source intelligence (OSINT)

OSINT involves gathering information from publicly available sources, such as social media, websites, and online databases, without actively interacting with the target system. This technique helps in identifying potential vulnerabilities and understanding the target's environment before more intrusive methods are used.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 319 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 319

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following threat actors is the most likely to seek financial gain through the use of ransomware attacks?

- A. Organized crime
- B. Insider threat
- C. Nation-state
- D. Hacktivists

[Hide Answer](#)

Suggested Answer: A

by [88d4601](#) at Nov. 17, 2024, 9:20 p.m.

Comments

✉ [88d4601](#) 1 day, 9 hours ago

The answer is A
upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for

your success. Start learning today with ExamTopics!

Start Learning for free



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 333 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 333

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following is a risk of conducting a vulnerability assessment?

- A. A disruption of business operations
- B. Unauthorized access to the system
- C. Reports of false positives Most Voted
- D. Finding security gaps in the system

[Hide Answer](#)

Suggested Answer: A

Community vote distribution

C (100%)

by  [jacobtriestech](#) at Nov. 16, 2024, 9:32 a.m.

Comments

  [9ef4a35](#) 1 day, 23 hours ago

A. A disruption of business operations.

Conducting a vulnerability assessment involves actively scanning and probing systems for weaknesses. This process can sometimes result in unintended consequences, such as:

System instability.

Network performance degradation.

Disruption of critical business operations due to overly aggressive scanning.

This makes disruption of business operations a key risk associated with vulnerability assessments.

upvoted 1 times

  [jacobtriestech](#) 2 days, 22 hours ago

Selected Answer: C

A vulnerability assessment is a process of identifying, classifying, and prioritizing vulnerabilities in a system. While it's a valuable security practice, it can sometimes lead to false positives, which are security alerts that incorrectly identify a threat.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

↳ Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 336 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 336

Topic #: 1

[\[All SY0-701 Questions\]](#)

An organization plans to expand its operations internationally and needs to keep data at the new location secure. The organization wants to use the most secure architecture model possible. Which of the following models offers the highest level of security?

- A. Cloud-based
- B. Peer-to-peer
- C. On-premises
- D. Hybrid Most Voted

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

D (100%)

by [Emmyrajj](#) at Nov. 16, 2024, 4:32 a.m.

Comments

✉️ [Emmyrajj](#) 3 days, 3 hours ago

Selected Answer: D

A hybrid architecture combines both on-premises and cloud-based solutions, offering flexibility and enhanced security. It allows the organization to keep sensitive data on-premises where it can implement strict controls, while leveraging the cloud for scalability and other less sensitive operations. This model provides the highest level of security by enabling organizations to apply tailored security measures for different types of data and workloads, ensuring compliance with regional regulations.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 341 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 341

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company installed cameras and added signs to alert visitors that they are being recorded. Which of the following controls did the company implement? (Choose two.)

A. Directive

B. Deterrent Most Voted

C. Preventive

D. Detective Most Voted

E. Corrective

F. Technical

[Hide Answer](#)

Suggested Answer: BD

Community vote distribution

BD (100%)

by fab34 at Nov. 15, 2024, 3:59 p.m.

Comments

✉ dC_Furious 20 hours, 21 minutes ago

B - Deterrent - Signs
D - Detective - Cameras

i don't understand why it would be A, defo false
upvoted 2 times

✉ 9ef4a35 3 days ago

The answer is BD. Deterrent and Detective
upvoted 2 times

✉ 74cd09c 3 days, 8 hours ago

detect and deter - BD

upvoted 3 times

 **fab34** 3 days, 15 hours ago

Selected Answer: BD

Deterrent = Signs

Detecitve = Cameras

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 379 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 379

Topic #: 1

[\[All SY0-701 Questions\]](#)

A company processes and stores sensitive data on its own systems. Which of the following steps should the company take first to ensure compliance with privacy regulations?

- A. Implement access controls and encryption.
- B. Develop and provide training on data protection policies.
- C. Create incident response and disaster recovery plans.
- D. Purchase and install security software.

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

A (100%)

by  [Emmyrajj](#) at Nov. 16, 2024, 6:30 a.m.

Comments

  [9ef4a35](#) 2 days, 2 hours ago

B. Develop and provide training on data protection policies.
upvoted 1 times

  [Emmyrajj](#) 3 days, 2 hours ago

Selected Answer: A

The first step in ensuring compliance with privacy regulations is to protect sensitive data by implementing access controls and encryption. Privacy regulations often mandate that organizations safeguard sensitive data to prevent unauthorized access or disclosure. Implementing these technical controls ensures that sensitive data is accessible only to authorized individuals and is protected if it is intercepted or stolen.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 385 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 385

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following allows an exploit to go undetected by the operating system?

A. Firmware vulnerabilities Most Voted

B. Side loading

C. Memory injection

D. Encrypted payloads

[Hide Answer](#)

Suggested Answer: C

Community vote distribution

C (50%)

A (50%)

by  [jacobtriestech](#) at Nov. 16, 2024, 10:35 a.m.

Comments

  [Emmyrajj](#) 2 days, 20 hours ago

Selected Answer: C

Memory injection is a technique where malicious code is injected directly into the memory space of a running process, allowing the exploit to execute without being written to disk. This makes it difficult for the operating system and traditional antivirus software to detect, as there are no files or persistent artifacts for security tools to analyze.

upvoted 1 times

  [jacobtriestech](#) 2 days, 22 hours ago

Selected Answer: A

Firmware vulnerabilities are often overlooked and can provide attackers with persistent access to a device, even after a full operating system reinstallation. This is because firmware is deeply embedded in the hardware and can be difficult to update or patch.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, Free.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 391 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 391

Topic #: 1

[\[All SY0-701 Questions\]](#)

A security analyst attempts to start a company's database server. When the server starts, the analyst receives an error message indicating the database server did not pass authentication. After reviewing and testing the system, the analyst receives confirmation that the server has been compromised and that attackers have redirected all outgoing database traffic to a server under their control. Which of the following MITRE ATT&CK techniques did the attacker most likely use to redirect database traffic?

- A. Browser extension
- B. Process injection
- C. Valid accounts
- D. Escape to host Most Voted

[Hide Answer](#)

Suggested Answer: D

Community vote distribution

D (100%)

by [jacobtriestech](#) at Nov. 16, 2024, 10:39 a.m.

Comments

✉ [jacobtriestech](#) 2 days, 21 hours ago

Selected Answer: D

Escape to host is a technique where an attacker gains unauthorized access to a system and then pivots to other systems within the network. In this case, the attacker gained access to the database server and then redirected its traffic to a controlled server. This indicates a successful escape to host.

upvoted 3 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)



- Expert Verified, Online, **Free**.

← Comptia Discussions



Exam SY0-701 All Questions

View all questions & answers for the SY0-701 exam

[Go to Exam](#)

📄 EXAM SY0-701 TOPIC 1 QUESTION 428 DISCUSSION

Actual exam question from CompTIA's SY0-701

Question #: 428

Topic #: 1

[\[All SY0-701 Questions\]](#)

Which of the following would be the best solution to deploy a low-cost standby site that includes hardware and internet access?

- A. Recovery site
- B. Cold site
- C. Hot site
- D. Warm site Most Voted

[Hide Answer](#)

Suggested Answer: B

Community vote distribution

D (100%)

by [jacobtriestech](#) at Nov. 17, 2024, 9:15 a.m.

Comments

✉ [jacobtriestech](#) 2 days ago

Selected Answer: D

A warm site is a cost-effective solution that provides a partially configured IT environment. It includes hardware, software, and network connections, but it may require some additional setup and configuration to become fully operational. This makes it ideal for organizations that need a quick recovery time but don't require immediate failover capabilities.

upvoted 1 times

Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)