

CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam



NEW QUESTION 1

- (Exam Topic 3)

An organization is repairing the damage after an incident. Which of the following controls is being implemented?

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

Answer: C

Explanation:

A corrective control is a type of security control that is designed to mitigate the damage caused by a security incident or to restore the normal operations after an incident. A corrective control can include actions such as restoring from backups, applying patches, isolating infected systems, or implementing new policies and procedures. A corrective control is different from a preventive control, which aims to stop an incident from happening, or a detective control, which aims to identify and record an incident. References:

- > <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/security-controls-3/>
- > <https://www.oreilly.com/library/view/comptia-security-all-in-one/9781260464016/ch31.xhtml>
- > <https://www.professormesser.com/security-plus/sy0-501/security-controls-2/>

NEW QUESTION 2

- (Exam Topic 3)

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
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Answer: A

Explanation:

A compensating control is a type of security control that is implemented in lieu of a recommended security measure that is deemed too difficult or impractical to implement at the present time. A compensating control must provide equivalent or comparable protection for the system or network and meet the intent and rigor of the original security requirement. An example of a compensating control is using a host-based firewall on a legacy Linux system to allow connections from only specific internal IP addresses, as it can provide a similar level of defense as a network firewall that may not be compatible with the system. References:

- > <https://www.techtarget.com/whatis/definition/compensating-control>
- > <https://reciprocity.com/resources/whats-the-difference-between-compensating-controls-and-mitigating-co>

NEW QUESTION 3

- (Exam Topic 2)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

- A. Bollard
- B. Camera
- C. Alarms
- D. Signage
- E. Access control vestibule

Answer: A

Explanation:

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

NEW QUESTION 4

- (Exam Topic 2)

A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

- A. Non-repudiation
- B. Baseline configurations
- C. MFA
- D. DLP

Answer: A

Explanation:

Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.

References:

- * 1. CompTIA Security+ Certification Exam Objectives (SY0-601): <https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf>
- * 2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

NEW QUESTION 5

- (Exam Topic 2)

Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

- A. IP schema
- B. Application baseline configuration
- C. Standard naming convention policy
- D. Wireless LAN and network perimeter diagram

Answer: C

Explanation:

A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P

NEW QUESTION 6

- (Exam Topic 2)

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename="output.txt", level=logging.DEBUG, format="%(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

- A. Logic bomb
- B. Keylogger
- C. Backdoor
- D. Ransomware

Answer: A

Explanation:

A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.

The snippet of Python code shows a logic bomb that executes a function called `delete_all_files()` when the current date is December 25th. The code uses the `datetime` module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the `delete_all_files()` function, which presumably deletes all files on the system.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.kaspersky.com/resource-center/definitions/logic-bomb>

NEW QUESTION 7

- (Exam Topic 2)

A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

- A. Log enrichment
- B. Log queue
- C. Log parser
- D. Log collector

Answer: D

Explanation:

A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://geekflare.com/open-source-centralized-logging/>

NEW QUESTION 8

- (Exam Topic 2)

A security analyst received the following requirements for the deployment of a security camera solution:

- * The cameras must be viewable by the on-site security guards.
- * The cameras must be able to communicate with the video storage server.
- * The cameras must have the time synchronized automatically.
- * The cameras must not be reachable directly via the internet.
- * The servers for the cameras and video storage must be available for remote maintenance via the company VPN.

Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

- A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
- B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
- C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
- D. Implementing a WAF to allow traffic from the local NTP server to the camera server

Answer: B

Explanation:

A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them¹. A jump server can also be used for auditing traffic and user activity for real-time surveillance³. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:

- > A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.
- > C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.
- > D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

References:

1: <https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/> 3: <https://www.ssh.com/academy/iam/jump-server> 2: https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION 9

- (Exam Topic 2)

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

- A. TACACS+
- B. RADIUS
- C. OAuth
- D. OpenID
- E. Kerberos
- F. CHAP

Answer: BE

Explanation:

RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION 10

- (Exam Topic 2)

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal in a secure manner?

- A. Digital signatures
- B. Key exchange
- C. Salting
- D. PPTP

Answer: B

Explanation:

Key exchange Short explanation

Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References:

<https://www.comptia.org/content/guides/what-is-encryption>

NEW QUESTION 11

- (Exam Topic 2)

A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?

- A. Hybrid
- B. private
- C. public
- D. Community

Answer: D

Explanation:

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.ibm.com/cloud/learn/community-cloud>

NEW QUESTION 12

- (Exam Topic 1)

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops. The review yielded the following results.

- The exception process and policy have been correctly followed by the majority of users
- A small number of users did not create tickets for the requests but were granted access
- All access had been approved by supervisors.
- Valid requests for the access sporadically occurred across multiple departments.
- Access, in most cases, had not been removed when it was no longer needed

Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

- A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval
- B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request
- C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team
- D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

Answer: A

Explanation:

According to the CompTIA Security+ SY0-601 documents, the correct answer option is A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval.

This option ensures that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame by requiring supervisors to approve or deny the exceptions on a regular basis. It also reduces the manual workload of the security team and improves the compliance with the company policy.

NEW QUESTION 13

- (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. A VUAN
- D. A screened subnet

Answer: D

Explanation:

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 14

- (Exam Topic 1)

Which of the following controls would provide the BEST protection against tailgating?

- A. Access control vestibule
- B. Closed-circuit television
- C. Proximity card reader
- D. Faraday cage

Answer: A

Explanation:

Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area. They are effective at preventing tailgating, as only one person can pass through each door at a time.

References:

- > <https://www.comptia.org/content/guides/what-is-a-mantrap>
- > CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 222

NEW QUESTION 15

- (Exam Topic 1)

A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

- A. Identity processor
- B. Service requestor
- C. Identity provider
- D. Service provider
- E. Tokenized resource
- F. Notarized referral

Answer: CD

Explanation:

An identity provider (IdP) is responsible for authenticating users and generating security tokens containing user information. A service provider (SP) is responsible for accepting security tokens and granting access to resources based on the user's identity.

NEW QUESTION 16

- (Exam Topic 1)

Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?

- A. Vulnerabilities with a CVSS score greater than 6.9.
- B. Critical infrastructure vulnerabilities on non-IP protocols.
- C. CVEs related to non-Microsoft systems such as printers and switches.
- D. Missing patches for third-party software on Windows workstations and servers.

Answer: D

Explanation:

An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION 17

- (Exam Topic 1)

Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

- A. Production
- B. Test
- C. Staging
- D. Development

Answer: D

Explanation:

A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

NEW QUESTION 18

- (Exam Topic 1)

A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of \$20,000 is credited to the account mentioned in the email. This BEST describes a scenario related to:

- A. whaling.
- B. smishing.
- C. spear phishing
- D. vishing

Answer: C

Explanation:

The scenario of receiving an email stating a database will be encrypted unless a payment is made is an example of spear phishing. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 2: Threats, Attacks, and Vulnerabilities, Social Engineering

NEW QUESTION 19

- (Exam Topic 1)

A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

- A. Implementation of preventive controls
- B. Implementation of detective controls
- C. Implementation of deterrent controls
- D. Implementation of corrective controls

Answer: B

Explanation:

A Security Information and Event Management (SIEM) system is a tool that collects and analyzes security-related data from various sources to detect and respond to security incidents. References: CompTIA Security+ Study Guide 601, Chapter 5

NEW QUESTION 20

- (Exam Topic 3)

Which of the following are common VoIP-associated vulnerabilities? (Select two).

- A. SPIM
- B. Vishing
- C. VLAN hopping
- D. Phishing
- E. DHCP snooping
- F. Tailgating

Answer: AB

Explanation:

SPIM (Spam over Internet Messaging) is a type of VoIP-associated vulnerability that involves sending unsolicited or fraudulent messages over an internet messaging service, such as Skype or WhatsApp. It can trick users into clicking on malicious links, downloading malware, providing personal or financial information, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity. Vishing (Voice Phishing) is a type of VoIP-associated vulnerability that involves making unsolicited or fraudulent phone calls over an internet telephony service, such as Google Voice or Vonage. It can trick users into disclosing personal or financial information, following malicious instructions, transferring money, etc., by using voice spoofing, caller ID spoofing, or interactive voice response systems.

NEW QUESTION 21

- (Exam Topic 3)

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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing 	<ul style="list-style-type: none"> 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

Solution:

Web server Botnet Enable DDoS protection User RAT Implement a host-based IPS Database server Worm Change the default application password Executive Keylogger Disable vulnerable services Application Backdoor Implement 2FA using push notification

A screenshot of a computer program Description automatically generated with low confidence

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	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 22

- (Exam Topic 3)

A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:

- A. decrease the mean time between failures.
- B. remove the single point of failure.
- C. cut down the mean time to repair
- D. reduce the recovery time objective

Answer: B

Explanation:

A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION 23

- (Exam Topic 3)

During a recent security assessment, a vulnerability was found in a common OS. The OS vendor was unaware of the issue and promised to release a patch within the next quarter. Which of the following best describes this type of vulnerability?

- A. Legacy operating system
- B. Weak configuration
- C. Zero day
- D. Supply chain

Answer: C

Explanation:

A zero-day vulnerability is a security flaw that is unknown to the vendor and the public, and therefore has no patch or fix available. A zero-day attack is an exploit that takes advantage of a zero-day vulnerability before the vendor or the security community becomes aware of it. A zero-day attack can cause serious damage to a system or network, as there is no defense against it until a patch is released. References:

- > <https://resources.infosecinstitute.com/certification/security-domain-1-threats-attacks-and-vulnerabilities/>
- > <https://www.professormesser.com/security-plus/sy0-501/zero-day-attacks-4/>

NEW QUESTION 24

- (Exam Topic 3)

Which of the following security concepts should an e-commerce organization apply for protection against erroneous purchases?

- A. Privacy
- B. Availability
- C. Integrity
- D. Confidentiality

Answer: C

Explanation:

Integrity is a security concept that ensures that data is accurate, complete and consistent, and that it has not been tampered with or modified in an unauthorized or unintended way. Integrity is important for e-commerce organizations to protect against erroneous purchases, as it can prevent data corruption, duplication, loss or manipulation that could affect the transactions or the records of the customers. Integrity can be achieved by using methods such as hashing, digital signatures, checksums, encryption and access control. Verified References:

- Security+ (Plus) Certification | CompTIA IT Certifications <https://www.comptia.org/certifications/security> (See What Skills Will You Learn?)
- CompTIA Security+ 601 - Infosec <https://www.infosecinstitute.com/wp-content/uploads/2021/03/CompTIA-Security-eBook.pdf> (See Security+: 5 in-demand cybersecurity skills)
- CompTIA Security+ SY0-601 Certification Study Guide <https://www.comptia.org/training/books/security-sy0-601-study-guide> (See Chapter 1: Threats, Attacks and Vulnerabilities, Section 1.4: Cryptography and PKI)

NEW QUESTION 25

- (Exam Topic 3)

A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?

- A. True positive
- B. True negative
- C. False positive
- D. False negative

Answer: C

Explanation:

A false positive is a type of alert that indicates a security incident when there is none. It can be caused by misconfigured or overly sensitive security tools or systems that generate false or irrelevant alerts. In this case, the alert from the company's SIEM that Mimikatz attempted to run on the remote systems was a false positive because it was triggered by a legitimate vulnerability scanning tool that uses Mimikatz as part of its functionality.

NEW QUESTION 26

- (Exam Topic 4)

The concept of connecting a user account across the systems of multiple enterprises is best known as:

- A. federation
- B. a remote access policy.
- C. multifactor authentication
- D. single sign-on.

Answer: D

Explanation:

The concept of connecting a user account across the systems of multiple enterprises is best known as federation. Federation is a process that allows users to authenticate once and access multiple resources or services across different domains or organizations. For example, a user can use their Google account to sign in to various websites or applications that support federation, without creating separate accounts or passwords for each one. Federation can improve user convenience and security, as well as reduce administrative overhead.

NEW QUESTION 27

- (Exam Topic 4)

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
- C. Red team
- D. Penetration testing

Answer: B

Explanation:

A program that allows individuals to security test the company's internet-facing application and compensates researchers based on the vulnerabilities discovered is best described as a bug bounty program. A bug bounty program is an incentive-based program that rewards ethical hackers for finding and reporting security flaws in software or systems.

NEW QUESTION 28

- (Exam Topic 4)

A vulnerability has been discovered and a known patch to address the vulnerability does not exist. Which of the following controls works best until a proper fix is released?

- A. Detective
- B. Compensating
- C. Deterrent
- D. Corrective

Answer: B

Explanation:

Compensating controls are alternative or additional controls that are implemented when the primary or preferred controls are not feasible or effective. Compensating controls can provide a similar level of protection or reduce the risk to an acceptable level until a proper fix is released. For example, if a vulnerability exists in a web server that allows remote code execution, a compensating control could be to restrict access to the web server by using a firewall or an IPS.

NEW QUESTION 29

- (Exam Topic 4)

Recent changes to a company's BYOD policy require all personal mobile devices to use a two-factor authentication method that is not something you know or have. Which of the following will meet this requirement?

- A. Facial recognition
- B. Six-digit PIN
- C. PKI certificate
- D. Smart card

Answer: A

Explanation:

Facial recognition is a type of biometric authentication that uses the unique features of a person's face to verify their identity. Facial recognition is not something you know or have, but something you are, which is one of the three factors of authentication. Facial recognition can use various methods and technologies, such as 2D or 3D images, infrared sensors, machine learning and more, to capture, analyze and compare facial data. Facial recognition can provide a convenient and secure way to authenticate users on personal mobile devices, as it does not require any additional hardware or input from the user. Facial recognition can also be used in conjunction with other factors, such as passwords or tokens, to provide multi-factor authentication. Verified References:

➤ Biometrics - SY0-601 CompTIA Security+ : 2.4 - Professor Messer IT Certification Training Courses <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/biometrics/> (See Facial Recognition)

➤ Security+ (Plus) Certification | CompTIA IT Certifications <https://www.comptia.org/certifications/security> (See Domain 2: Architecture and Design, Objective 2.4: Given a scenario, implement identity and access management controls.)

➤ Biometric and Facial Recognition - CompTIA Security+ Certification (SY0-501) https://www.oreilly.com/library/view/comptia-security-certification/9781789953091/video9_6.html (See Biometric and Facial Recognition)

NEW QUESTION 30

- (Exam Topic 4)

A security architect at a large, multinational organization is concerned about the complexities and overhead of managing multiple encryption keys securely in a multicloud provider environment. The security architect is looking for a solution with reduced latency to allow the incorporation of the organization's existing keys and to maintain consistent, centralized control and management regardless of the data location. Which of the following would best meet the architect's objectives?

- A. Trusted Platform Module
- B. IaaS
- C. HSMAas
- D. PaaS

Answer: C

Explanation:

HSMAas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption. HSMAas allows the organization to use its own keys or generate new ones, and to control and manage them centrally regardless of where the data is stored or processed. HSMAas also reduces the latency and complexity of managing multiple encryption keys across different cloud providers, as well as the cost and maintenance of deploying physical HSM devices.

* A. Trusted Platform Module. This is not the correct answer, because a Trusted Platform Module (TPM) is a hardware chip that provides secure storage and generation of cryptographic keys on a device, such as a laptop or a server. A TPM does not offer a cloud-based solution for key management and encryption across multiple cloud providers.

* B. IaaS. This is not the correct answer, because IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources, such as servers, storage, and networks, over the internet. IaaS does not provide a specific solution for key management and encryption across multiple cloud providers.

* C. HSMAas. This is the correct answer, because HSMAas stands for Hardware Security Module as a Service, which is a cloud-based service that provides secure and scalable key management and cryptographic operations for data encryption and decryption across multiple cloud providers.

* D. PaaS. This is not the correct answer, because PaaS stands for Platform as a Service, which is a cloud computing model that provides a platform for developing and deploying applications over the internet. PaaS does not provide a specific solution for key management and encryption across multiple cloud providers.

Reference: HSM as a Service (HSMAas) | Encryption Consulting, What Is Hardware Security Module (HSM) | Thales.

NEW QUESTION 31

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)