



CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

NEW QUESTION 1

A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

- A. Use an entropy-as-a-service vendor to leverage larger entropy pools.
- B. Loop multiple pseudo-random number generators in a series to produce larger numbers.
- C. Increase key length by two orders of magnitude to detect brute forcing.
- D. Shift key generation algorithms to ECC algorithm

Answer: A

NEW QUESTION 2

A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

- A. Making employees rotate through jobs ensures succession plans can be implemented and prevents single point of failure.
- B. Forcing different people to perform the same job minimizes the amount of time malicious actions go undetected by forcing malicious actors to attempt collusion between two or more people.
- C. Administrators and engineers who perform multiple job functions throughout the day benefit from being cross-trained in new job areas.
- D. It eliminates the need to share administrative account passwords because employees gain administrative rights as they rotate into a new job area.

Answer: B

NEW QUESTION 3

A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

- A. Summarize the most recently disclosed vulnerabilities.
- B. Research industry best practices and latest RFCs.
- C. Undertake an external vulnerability scan and penetration test.
- D. Conduct a threat modeling exercise

Answer: D

NEW QUESTION 4

An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:

1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location

The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

- A. Develop a security exemption, as it does not meet the security policies
- B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
- C. Require the solution owner to accept the identified risks and consequences
- D. Review the entire procurement process to determine the lessons learned

Answer: C

NEW QUESTION 5

Given the following output from a local PC:

```
C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
Link-local IPv6 Address . . . . . : fe80::4551:67ba:77a6:62e1%11
IPv4 Address. . . . . : 172.30.0.28
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

- A. Allow 172.30.0.28:80 -> ANY
- B. Allow 172.30.0.28:80 -> 172.30.0.0/16
- C. Allow 172.30.0.28:80 -> 172.30.0.28:443
- D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Answer: B

NEW QUESTION 6

A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

- A. Set up a VDI environment that prevents copying and pasting to the local workstations of outsourced staff members
- B. Install a client-side VPN on the staff laptops and limit access to the development network
- C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff
- D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Answer: D

NEW QUESTION 7

A systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

- A. These devices can communicate over networks older than HSPA+ and LTE standards, exposing device communications to poor encryption routines
- B. The organization will be unable to restrict the use of NFC, electromagnetic induction, and Bluetooth technologies
- C. The associated firmware is more likely to remain out of date and potentially vulnerable
- D. The manufacturers of the baseband radios are unable to enforce mandatory access controls within their driver set

Answer: B

NEW QUESTION 8

An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

- A. Threat modeling
- B. Risk assessment
- C. Vulnerability data
- D. Threat intelligence
- E. Risk metrics
- F. Exploit frameworks

Answer: F

NEW QUESTION 9

An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.

Data Type	Confidentiality	Integrity	Availability
PII	High	Medium	Low
Proprietary	High	High	Medium
Competitive	High	Medium	Medium
Industrial	Low	Low	High
Financial	Medium	High	Low

Based on the data classification table above, which of the following BEST describes the overall classification?

- A. High confidentiality, high availability
- B. High confidentiality, medium availability
- C. Low availability, low confidentiality
- D. High integrity, low availability

Answer: B

NEW QUESTION 10

A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

- A. OTA updates
- B. Remote wiping
- C. Side loading
- D. Sandboxing
- E. Containerization
- F. Signed applications

Answer: EF

NEW QUESTION 10

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:

Duplicate IP addresses
Rogue network devices

Infected systems probing the company's network

Which of the following should be implemented to remediate the above issues? (Choose two.)

- A. Port security
- B. Route protection
- C. NAC
- D. HIPS
- E. NIDS

Answer: BC

NEW QUESTION 11

After investigating virus outbreaks that have cost the company \$1,000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

	Solution Cost	Year 1 Support	Year 2 Support	Estimated Yearly Incidents
Product A	\$10,000	\$3,000	\$1,000	1
Product B	\$14,250	\$1,000	\$1,000	0
Product C	\$9,500	\$2,000	\$2,000	1
Product D	\$7,000	\$1,000	\$2,000	2
Product E	\$7,000	\$4,000	\$4,000	0

Using the table above, which of the following would be the BEST business-driven choice among five possible solutions?

- A. Product A
- B. Product B
- C. Product C
- D. Product D
- E. Product E

Answer: E

NEW QUESTION 15

A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

- A. Install a HIPS on the web servers
- B. Disable inbound traffic from offending sources
- C. Disable SNMP on the web servers
- D. Install anti-DDoS protection in the DMZ

Answer: A

NEW QUESTION 18

An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

- A. Magic link sent to an email address
- B. Customer ID sent via push notification
- C. SMS with OTP sent to a mobile number
- D. Third-party social login
- E. Certificate sent to be installed on a device
- F. Hardware tokens sent to customers

Answer: CE

NEW QUESTION 20

A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

```
^32^[34fda19(fd^43gfd/home/user/lib/module.so.343jk^rfw(342fds43g
```

Which of the following did the analyst use to determine the location of the malicious payload?

- A. Code deduplicators

- B. Binary reverse-engineering
- C. Fuzz testing
- D. Security containers

Answer: B

NEW QUESTION 24

An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

- A. Black box testing
- B. Gray box testing
- C. Code review
- D. Social engineering
- E. Vulnerability assessment
- F. Pivoting
- G. Self-assessment
- H. White teaming
- I. External auditing

Answer: AEF

NEW QUESTION 29

A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

Which of the following tools is the security engineer using to produce the above output?

- A. Vulnerability scanner
- B. SIEM
- C. Port scanner
- D. SCAP scanner

Answer: B

NEW QUESTION 33

A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

- A. The OS version is not compatible
- B. The OEM is prohibited
- C. The device does not support FDE
- D. The device is rooted

Answer: D

NEW QUESTION 36

A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

- A. Inform the customer that the service provider does not have any control over third-party blacklist entries
- B. The customer should reach out to the blacklist operator directly
- C. Perform a takedown of any customer accounts that have entries on email blacklists because this is a strong indicator of hostile behavior
- D. Work with the legal department and threaten legal action against the blacklist operator if the netblocks are not removed because this is affecting legitimate traffic
- E. Establish relationship with a blacklist operators so broad entries can be replaced with more granular entries and incorrect entries can be quickly pruned

Answer: D

NEW QUESTION 40

A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day exploit and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

- A. File size

- B. Digital signature
- C. Checksums
- D. Anti-malware software
- E. Sandboxing

Answer: B

NEW QUESTION 45

Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

- A. Business partnership agreement
- B. Memorandum of understanding
- C. Service-level agreement
- D. Interconnection security agreement

Answer: D

NEW QUESTION 47

A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: “<object object_ref=... />” and “<state state_ref=... />”. Which of the following tools BEST supports the use of these definitions?

- A. HTTP interceptor
- B. Static code analyzer
- C. SCAP scanner
- D. XML fuzzer

Answer: D

NEW QUESTION 50

A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization: `localStorage.setItem("session-cookie", document.cookie);` Which of the following should the security engineer recommend?

- A. SessionStorage should be used so authorized cookies expire after the session ends
- B. Cookies should be marked as “secure” and “HttpOnly”
- C. Cookies should be scoped to a relevant domain/path
- D. Client-side cookies should be replaced by server-side mechanisms

Answer: C

NEW QUESTION 54

During a security event investigation, a junior analyst fails to create an image of a server’s hard drive before removing the drive and sending it to the forensics analyst. Later, the evidence from the analysis is not usable in the prosecution of the attackers due to the uncertainty of tampering. Which of the following should the junior analyst have followed?

- A. Continuity of operations
- B. Chain of custody
- C. Order of volatility
- D. Data recovery

Answer: C

NEW QUESTION 59

An architect was recently hired by a power utility to increase the security posture of the company’s power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources.

Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

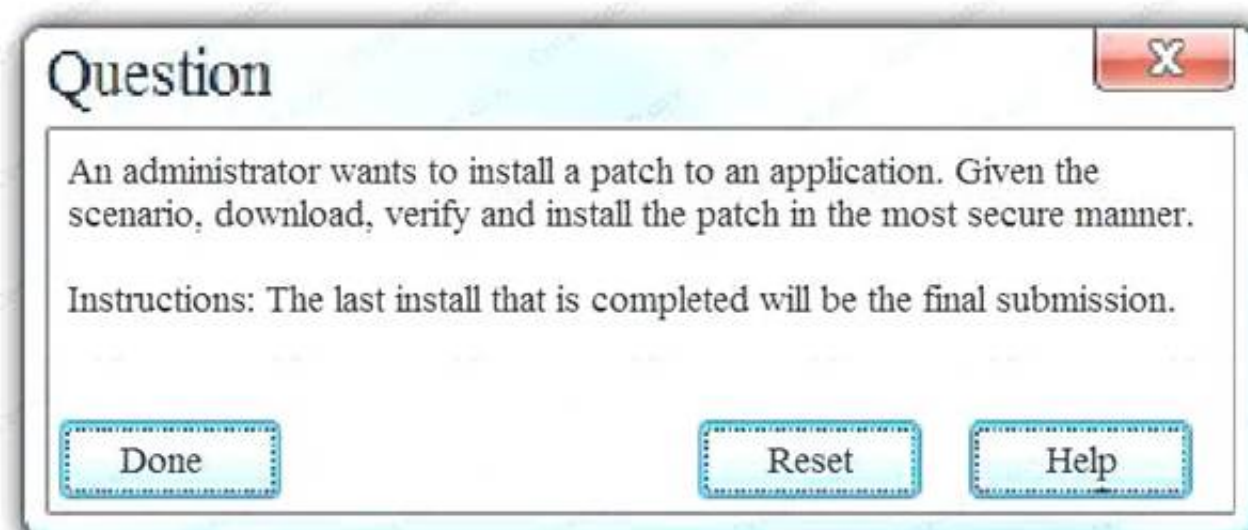
- A. Isolate the systems on their own network
- B. Install a firewall and IDS between systems and the LAN
- C. Employ own stratum-0 and stratum-1 NTP servers
- D. Upgrade the software on critical systems
- E. Configure the systems to use government-hosted NTP servers

Answer: BE

NEW QUESTION 64

Exhibit:

Home>Download Center>Application Patch		
The links in this section correspond to separate files available in this download center. Download the most appropriate file.		
File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download
HASH: 1759adb5g34700aae19bc4578fc19cc2		



- Step 1: Verify that the certificate is valid or no
- In case of any warning message, cancel the download. Step 2: If certificate issue is not there then, download the file in your system. Step 3: Match the hash value of the downloaded file with the one which you selected on the website
- Step 4: Install the file if the hash value matches.
- Step 1: Verify that the certificate is valid or no
- In case of any warning message, cancel the download. Step 2: If certificate issue is not there then, download the file in your system
- Step 3: Calculate the hash value of the downloaded file. Step 4: Match the hash value of the downloaded file with the one which you selected on the website
- Step 5: Install the file if the hash value matches.

Answer: B

NEW QUESTION 69

Given the code snippet below:

```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

    char username[8];

    printf("Enter your username: ");

    gets(username)

    printf("\n");

    if (username == NULL) {

        printf("you did not enter a username\n");

    }

    if strcmp(username, "admin") {

        printf("%s", "Admin user, enter your physical token value: ");

        // rest of conditional logic here has been snipped for brevity

    } else {

        printf("Standard user, enter your password: ");

        // rest of conditional logic here has been snipped for brevity

    }

}
```

Which of the following vulnerability types is the MOST concerning?

- A. Only short usernames are supported, which could result in brute forcing of credentials.
- B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
- C. Hardcoded usernames with different code paths taken depend on which user is entered.
- D. Format string vulnerability is present for admin users but not for standard user

Answer: B

NEW QUESTION 74

Security policies that are in place at an organization prohibit USB drives from being utilized across the entire enterprise, with adequate technical controls in place to block them. As a way to still be able to work from various locations on different computing resources, several sales staff members have signed up for a web-based storage solution without the consent of the IT department. However, the operations department is required to use the same service to transmit certain business partner documents.

Which of the following would BEST allow the IT department to monitor and control this behavior?

- A. Enabling AAA
- B. Deploying a CASB
- C. Configuring an NGFW
- D. Installing a WAF
- E. Utilizing a vTPM

Answer: B

NEW QUESTION 79

A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources. Which of the following should the analyst use to remediate the vulnerabilities?

- A. Protocol analyzer
- B. Root cause analyzer
- C. Behavioral analytics
- D. Data leak prevention

Answer: D

NEW QUESTION 82

An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

Active full-device encryption Enabled remote-device wipe Blocking unsigned applications

Containerization of email, calendar, and contacts

Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements?

- A. Require frequent password changes and disable NFC.
- B. Enforce device encryption and activate MAM.
- C. Install a mobile antivirus application.
- D. Configure and monitor devices with an MD

Answer: B

NEW QUESTION 87

Given the following information about a company's internal network:

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

A security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do?

- A. Use a protocol analyzer on 192.168.1.0/24
- B. Use a port scanner on 192.168.1.0/24
- C. Use an HTTP interceptor on 192.168.1.0/24
- D. Use a port scanner on 192.168.192.0/25
- E. Use a protocol analyzer on 192.168.192.0/25
- F. Use an HTTP interceptor on 192.168.192.0/25

Answer: B

NEW QUESTION 90

The Chief Information Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and twofactor authentication is not provided natively. Which of the following would BEST address the CIO's concerns?

- A. Procure a password manager for the employees to use with the cloud applications.
- B. Create a VPN tunnel between the on-premises environment and the cloud providers.
- C. Deploy applications internally and migrate away from SaaS applications.
- D. Implement an IdP that supports SAML and time-based, one-time password

Answer: B

NEW QUESTION 94

A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?

- A. Check for any relevant or required overlays.
- B. Review enhancements within the current control set.
- C. Modify to a high-baseline set of controls.
- D. Perform continuous monitorin

Answer: C

NEW QUESTION 95

A security analyst is inspecting pseudocode of the following multithreaded application:

1. perform daily ETL of data
 - 1.1 validate that yesterday's data model file exists
 - 1.2 validate that today's data model file does not exist
 - 1.2 extract yesterday's data model
 - 1.3 transform the format
 - 1.4 load the transformed data into today's data model file
 - 1.5 exit

Which of the following security concerns is evident in the above pseudocode?

- A. Time of check/time of use
- B. Resource exhaustion
- C. Improper storage of sensitive data
- D. Privilege escalation

Answer: A

NEW QUESTION 97

A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

1. Information should be sourced from the trusted master data source.
2. There must be future requirements for identity proofing of devices and users.
3. A generic identity connector that can be reused must be developed.
4. The current project scope is for internally hosted applications only.

Which of the following solution building blocks should the security architect use to BEST meet the requirements?

- A. LDAP, multifactor authentication, oAuth, XACML
- B. AD, certificate-based authentication, Kerberos, SPML
- C. SAML, context-aware authentication, oAuth, WAYF
- D. NAC, radius, 802.1x, centralized active directory

Answer: A

NEW QUESTION 102

The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code. Which of the following is an SDLC best practice that should have been followed?

- A. Versioning
- B. Regression testing
- C. Continuous integration
- D. Integration testing

Answer: B

NEW QUESTION 103

A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.

Which of the following security controls would address the user's privacy concerns and provide the BEST level of security for the home network?

- A. Ensure all IoT devices are configured in a geofencing mode so the devices do not work when removed from the home network
- B. Disable the home assistant unless actively using it, and segment the network so each IoT device has its own segment.
- C. Install a firewall capable of cryptographically separating network traffic require strong authentication to access all IoT devices, and restrict network access for the home assistant based on time-of-day restrictions.
- D. Segment the home network to separate network traffic from users and the IoT devices, ensure security settings on the home assistant support no or limited recording capability, and install firewall rules on the router to restrict traffic to the home assistant as much as possible.
- E. Change all default passwords on the IoT devices, disable Internet access for the IoT devices and the home assistant, obtain routable IP addresses for all devices, and implement IPv6 and IPSec protections on all network traffic.

Answer: B

NEW QUESTION 106

An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES- 256-GCM on VPNs between sites. Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

- A. Add a second-layer VPN from a different vendor between sites.
- B. Upgrade the cipher suite to use an authenticated AES mode of operation.
- C. Use a stronger elliptic curve cryptography algorithm.
- D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
- E. Ensure cryptography modules are kept up to date from vendor supplying the

Answer: C

NEW QUESTION 111

Which of the following is a feature of virtualization that can potentially create a single point of failure?

- A. Server consolidation
- B. Load balancing hypervisors
- C. Faster server provisioning
- D. Running multiple OS instances

Answer: A

NEW QUESTION 113

A technician receives the following security alert from the firewall's automated system: Match_Time: 10/10/16 16:20:43

Serial: 002301028176

Device_name: COMPSEC1 Type: CORRELATION

Scrusex: domain\samjones Scr: 10.50.50.150

Object_name: beacon detection Object_id: 6005

Category: compromised-host Severity: medium

Evidence: host repeatedly visited a dynamic DNS domain (17 time) After reviewing the alert, which of the following is the BEST analysis?

- A. the alert is a false positive because DNS is a normal network function.
- B. this alert indicates a user was attempting to bypass security measures using dynamic DNS.
- C. this alert was generated by the SIEM because the user attempted too many invalid login attempts.
- D. this alert indicates an endpoint may be infected and is potentially contacting a suspect hos

Answer: B

NEW QUESTION 118

Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

- A. Integer overflow
- B. Click-jacking
- C. Race condition
- D. SQL injection
- E. Use after free
- F. Input validation

Answer: E

Explanation:

Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.

Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.

According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."

Incorrect Answers:

A: Integer overflow is the result of an attempt by a CPU to arithmetically generate a number larger than what can fit in the devoted memory storage space.

Arithmetic operations always have the potential of returning unexpected values, which may cause an error that forces the whole program to shut down. This is not what is described in this question.

B: Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information

or taking control of their computer while clicking on seemingly innocuous web pages. This is not what is described in this question.

C: A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence to be done correctly. This is not what is described in this question.

D: SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to dat

A. This is not

what is described in this question.

F: Input validation is used to ensure that the correct data is entered into a field. For example, input validation would prevent letters typed into a field that expects number from being accepted. This is not what is described in this question.

References:

<http://www.webopedia.com/TERM/U/use-after-free.HYPERLINK> "http://www.webopedia.com/TERM/U/use-after-free.html"html

htHYPERLINK "https://en.wikipedia.org/wiki/Clickjacking"tps://en.wikipedia.org/wiki/Clickjacking <http://searchstorage.tHYPERLINK>

"http://searchstorage.techtarget.com/definition/racecondition" echtarget.com/definition/race-condiHYPERLINK "http://searchstorage.techtarget.com/definition/race-condition"tion

NEW QUESTION 120

A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

- A. Client side input validation
- B. Stored procedure
- C. Encrypting credit card details
- D. Regular expression matching

Answer: D

Explanation:

Regular expression matching is a technique for reading and validating input, particularly in web software. This question is asking about securing input fields where customers enter their credit card details. In this case, the expected input into the credit card number field would be a sequence of numbers of a certain length. We can use regular expression matching to verify that the input is indeed a sequence of numbers. Anything that is not a sequence of numbers could be malicious code. Incorrect Answers:

A: Client side input validation could be used to validate the input into input fields. Client side input validation is where the validation is performed by the web browser. However this question is asking for the BEST answer. A user with malicious intent could bypass the client side input validation whereas it would be much more difficult to bypass regular expression matching implemented in the application code.

B: A stored procedure is SQL code saved as a script. A SQL user can run the stored procedure rather than typing all the SQL code contained in the stored procedure. A stored procedure is not used for validating input.

C: Any stored credit card details should be encrypted for security purposes. Also a secure method of transmission such as SSL or TLS should be used to encrypt the data when transmitting the credit card number over a network such as the Internet. However, encrypting credit card details is not a way of securing the input fields in an application.

NEW QUESTION 122

An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

- A. Replicate NAS changes to the tape backups at the other datacenter.
- B. Ensure each server has two HBAs connected through two routes to the NAS.
- C. Establish deduplication across diverse storage paths.
- D. Establish a SAN that replicates between datacenters.

Answer: D

Explanation:

A SAN is a Storage Area Network. It is an alternative to NAS storage. SAN replication is a technology that replicates the data on one SAN to another SAN; in this case, it would replicate the data to a SAN in the backup datacenter. In the event of a disaster, the SAN in the backup datacenter would contain all the data on the original SAN.

Array-based replication is an approach to data backup in which compatible storage arrays use built-in software to automatically copy data from one storage array to another. Array-based replication software runs on one or more storage controllers resident in disk storage systems, synchronously or asynchronously replicating data between similar storage array models at the logical unit number (LUN) or volume block level. The term can refer to the creation of local copies of data within

the same array as the source data, as well as the creation of remote copies in an array situated off site. Incorrect Answers:

A: Replicating NAS changes to the tape backups at the other datacenter would result in a copy of the NAS data in the backup datacenter. However, the data will be stored on tape. In the event of a disaster, you would need another NAS to restore the data to.

B: Ensuring that each server has two routes to the NAS is not a viable solution. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

C: Deduplication is the process of eliminating multiple copies of the same data to save storage space. The NAS is still a single point of failure. In the event of a disaster, you could lose the NAS and all the data on it.

References:

<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication> chdisasterrecovery.tHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>" echtarget.com/definition/HYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-based-replication>"Array-basedrepliHYPERLINK

"<http://searchdisasterrecovery.techtarget.com/definition/Array-basedreplication>"

cation

NEW QUESTION 125

select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson

Which of the following types of attacks is the user attempting?

- A. XML injection
- B. Command injection
- C. Cross-site scripting
- D. SQL injection

Answer: D

Explanation:

The code in the question is SQL code. The attack is a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: The code in the question is not XML code. Therefore this is not an XML injection attack so this answer is incorrect.

B: Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. The code in the question is not the type of code you would use in a command injection attack.

C: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The code in the question is not the type of code you would use in an XSS attack.

References: http://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 130

A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

- A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
- B. A DLP gateway should be installed at the company border.
- C. Strong authentication should be implemented via external biometric devices.
- D. Full-tunnel VPN should be required for all network communication.
- E. Full-drive file hashing should be implemented with hashes stored on separate storage.
- F. Split-tunnel VPN should be enforced when transferring sensitive dat

Answer: BD

Explanation:

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Full-tunnel VPN should be required for all network communication. This will ensure that all data transmitted over the network is encrypted which would prevent a malicious user accessing the data by using packet sniffing.

Incorrect Answers:

A: This question is asking which of the following additional controls MUST be implemented to minimize the risk of data leakage. Implementing a full system backup does not minimize the risk of data leakage.

C: Strong authentication implemented via external biometric devices will ensure that only authorized people can access the network. However, it does not minimize the risk of data leakage.

E: Full-drive file hashing is not required because we already have full drive encryption.

F: Split-tunnel VPN is used when a user is remotely accessing the network. Communications with company servers go over a VPN whereas private communications such as web browsing does not use a VPN. A more secure solution is a full tunnel VPN.

References:

<http://whatis.techtarget.com/defHYPERLINK> "<http://whatis.techtarget.com/definition/data-lossprevention-DLP>"inition/data-loss-prevention-DLP

NEW QUESTION 134

Which of the following describes a risk and mitigation associated with cloud data storage?

- A. Risk: Shared hardware caused data leakage Mitigation: Strong encryption at rest
- B. Risk: Offsite replication Mitigation: Multi-site backups
- C. Risk: Data loss from de-duplication Mitigation: Dynamic host bus addressing

D. Risk: Combined data archivingMitigation: Two-factor administrator authentication

Answer: A

Explanation:

With cloud data storage, the storage provider will have large enterprise SANs providing large pools of storage capacity. Portions of the storage pools are assigned to customers. The risk is that multiple customers are storing their data on the same physical hardware storage devices. This presents a risk (usually a very small risk, but a risk all the same) of other customers using the same cloud storage hardware being able to view your data.

The mitigation of the risk is to encrypt your data stored on the SAN. Then the data would be unreadable even if another customer was able to access it.

Incorrect Answers:

B: Offsite replication is used for disaster recovery purposes. It is not considered to be a risk as long as the data is secure in the other site. Multi-site backups are not a risk mitigation.

C: Data loss from de-duplication is not considered to be a risk. De-duplication removes duplicate copies of data to reduce the storage space required for the data.

A. Dynamic host bus addressing is not a risk mitigation.

D: Combined data archiving is not considered to be a risk. The archived data would be less accessible to other customers than the live data on the shared storage.

NEW QUESTION 138

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

- A. Require each Company XYZ employee to use an IPSec connection to the required systems
- B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
- C. Require Company ABC employees to use two-factor authentication on the required systems
- D. Require a site-to-site VPN for intercompany communications

Answer: B

Explanation:

VDI stands for Virtual Desktop Infrastructure. Virtual desktop infrastructure is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Company ABC can configure virtual desktops with the required restrictions and required access to systems that the users in company XYZ require. The users in company XYZ can then log in to the virtual desktops over a secure encrypted connection and then access authorized systems only. Incorrect Answers:

A: Requiring IPSec connections to the required systems would secure the connections to the required systems. However, it does not prevent access to unauthorized systems.

C: The question states that the representatives reside at Company XYZ's headquarters. Therefore, they will be access Company ABC's systems remotely. Two factor authentication requires that the user be present at the location of the system to present a smart card or for biometric authentication; two factor authentication cannot be performed remotely.

D: A site-to-site VPN will just create a secure connection between the two sites. It does not restrict access to unauthorized systems.

References:

<http://searchvirtualdesktop.techtarget.com/definition/virtualdesktop> irtualdesktop.techtarget.com/definition/virtual-desktop

NEW QUESTION 143

A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

- A. A separate physical interface placed on a private VLAN should be configured for live host operations.
- B. Database record encryption should be used when storing sensitive information on virtual servers.
- C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
- D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network

Answer: A

Explanation:

VDI virtual machines can be migrated across physical hosts while the virtual machines are still powered on. In VMware, this is called vMotion. In Microsoft Hyper-V, this is called Live Migration. When a virtual machine is migrated between hosts, the data is unencrypted as it travels across the network. To prevent access to the data as it travels across the network, a dedicated network should be created for virtual machine migrations. The dedicated migration network should only be accessible by the virtual machine hosts to maximize security.

Incorrect Answers:

B: Database record encryption is used for encrypting database records only. This question does not state that the only sensitive data is database records. The data is at risk as it travels across the network when virtual machines are migrated between hosts. Data is unencrypted when it is transmitted over the network.

C: Full disk encryption is a good idea to secure data stored on disk. However, the data is unencrypted when it is transmitted over the network.

D: The sensitive data is on the VDI virtual machines. Storing the sensitive information on an isolated fiber channel network would make the information inaccessible from the virtual machines.

NEW QUESTION 147

Ann is testing the robustness of a marketing website through an intercepting proxy. She has intercepted the following HTTP request:

POST /login.aspx HTTP/1.1 Host: comptia.org

Content-type: text/html txtUsername=ann&txtPassword=ann&alreadyLoggedIn=false&submit=true

Which of the following should Ann perform to test whether the website is susceptible to a simple authentication bypass?

- A. Remove all of the post data and change the request to /login.aspx from POST to GET
- B. Attempt to brute force all usernames and passwords using a password cracker
- C. Remove the txtPassword post data and change alreadyLoggedIn from false to true
- D. Remove the txtUsername and txtPassword post data and toggle submit from true to false

Answer: C

Explanation:

The text "txtUsername=ann&txtPassword=ann" is an attempted login using a username of 'ann' and also a password of 'ann'.

The text "alreadyLoggedIn=false" is saying that Ann is not already logged in.

To test whether we can bypass the authentication, we can attempt the login without the password

and we can see if we can bypass the 'alreadyloggedin' check by changing alreadyLoggedIn from false to true. If we are able to log in, then we have bypassed the authentication check.

Incorrect Answers:

A: GET /login.aspx would just return the login form. This does not test whether the website is susceptible to a simple authentication bypass.

B: We do not want to guess the usernames and passwords. We want to see if we can get into the site without authentication.

D: We need to submit the data so we cannot toggle submit from true to false.

NEW QUESTION 151

ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).

- A. Establish a list of users that must work with each regulation
- B. Establish a list of devices that must meet each regulation
- C. Centralize management of all devices on the network
- D. Compartmentalize the network
- E. Establish a company framework
- F. Apply technical controls to meet compliance with the regulation

Answer: BDF

Explanation:

Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

There are six main requirements for PCI compliance. The vendor must: Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program Implement strong access control measures Regularly monitor and test networks Maintain an information security policy

To achieve PCI and SOX compliance you should:

Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.

Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.

Apply technical controls to meet compliance with the regulation. Secure the data as required. Incorrect Answers:

A: It is not necessary to establish a list of users that must work with each regulation. All users should be trained to manage sensitive data.

A: However, PCI and SOX compliance is more about the security of the data on the computers that contain the data.

C: Central management of all devices on the network makes device management easier for administrators. However, it is not a requirement for PCI and SOX compliance.

E: A company framework is typically related to the structure of employee roles and departments. It is not a requirement for PCI and SOX compliance.

References:

<http://searchcompliance.techtarget.com/definition/PCI-compliance>HYPERLINK "http://searchcompliance.techtarget.com/definition/PCI-compliance"nce

NEW QUESTION 154

A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?

- A. Online password testing
- B. Rainbow tables attack
- C. Dictionary attack
- D. Brute force attack

Answer: B

Explanation:

The passwords in a Windows (Active Directory) domain are encrypted.

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are prematched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse

the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

Incorrect Answers:

A: Online password testing cannot be used to crack passwords on a windows domain.

C: The question states that the domain enforces strong complex passwords. Strong complex passwords must include upper and lowercase letters, numbers and punctuation marks. A word in the dictionary would not meet the strong complex passwords requirement so a dictionary attack would be ineffective at cracking the passwords in this case.

D: Brute force attacks against complex passwords take much longer than a rainbow tables attack. References:

<http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm>ty.about.com/od/hackertoHYPERLINK

"http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"ols/a/Rainbow-TableHYPERLINK "http://netsecurity.about.com/od/hackertools/a/Rainbow-Tables.htm"s.htm

NEW QUESTION 157

ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC

counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

- A. TOTP
- B. PAP
- C. CHAP
- D. HOTP

Answer: D

Explanation:

The question states that the HMAC counter-based codes and are valid until they are used. These are “one-time” use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm.

HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server. Both hardware and software tokens are available from various vendors. Hardware tokens implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP. Software tokens are available for (nearly) all major mobile/smartphone platforms.

Incorrect Answers:

A: TOTP is Time-based One-time Password. This is similar to the one-time password system used in this question. However, TOTPs expire after a period of time. In this question, the passwords (codes) expire after first use regardless of the timing of the first use.

B: PAP (Password Authentication Protocol) is a simple authentication protocol in which the user name and password is sent to a remote access server in a plaintext (unencrypted) form. PAP is not what is described in this question.

C: CHAP (Challenge-Handshake Authentication Protocol) is an authentication protocol that provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. CHAP is not what is described in this question.

References:

https://en.wikipedia.org/wiki/HMAC-based_One-time_HYPERLINK "https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_Algorithm"Password_Algorithm

NEW QUESTION 159

A small company is developing a new Internet-facing web application. The security requirements are: Users of the web application must be uniquely identified and authenticated.

Users of the web application will not be added to the company’s directory services. Passwords must not be stored in the code.

Which of the following meets these requirements?

- A. Use OpenID and allow a third party to authenticate users.
- B. Use TLS with a shared client certificate for all users.
- C. Use SAML with federated directory services.
- D. Use Kerberos and browsers that support SAM

Answer: A

Explanation:

Users create accounts by selecting an OpenID identity provider, and then use those accounts to sign onto any website which accepts OpenID authentication.

OpenID is an open standard and decentralized protocol by the non-profit OpenID Foundation that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. This eliminates the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. In other words, users can log into multiple unrelated websites without having to register with their information over and over again.

Several large organizations either issue or accept OpenIDs on their websites according to the OpenID Foundation: AOL, Blogger, Flickr, France Telecom, Google, Hyves, LiveJournal, Microsoft (provider name Microsoft account), Mixi, Myspace, Novell, Orange, Sears, Sun, Telecom Italia, Universal Music Group, VeriSign, WordPress, and Yahoo!. Other providers include BBC, IBM, PayPal, and Steam. Incorrect Answers:

B: The question states that users of the web application must be uniquely identified and authenticated. A shared client certificate for all users does not meet this requirement.

C: The question states that users of the web application will not be added to the company’s directory services. SAML with federated directory services would require that the users are added to the directory services.

D: The question states that users of the web application must be uniquely identified and authenticated. Kerberos and browsers that support SAML provides no authentication mechanism. References:

<https://en.wikipedia.org/wiki/OpenID>

NEW QUESTION 161

Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

- A. Establish a cloud-based authentication service that supports SAML.
- B. Implement a new Diameter authentication server with read-only attestation.
- C. Install a read-only Active Directory server in the corporate DMZ for federation.
- D. Allow external connections to the existing corporate RADIUS serve

Answer: A

Explanation:

There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments.

By eliminating all passwords and instead using digital signatures for authentication and authorization

of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise

environments, are more secure and help simplify identity management across large and diverse user communities.

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by

SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision – in other words it can decide whether to perform some service for the connected principal. Incorrect Answers:

B: Diameter authentication server with read-only attestation is not a solution that has wide compatibility among SaaS vendors.

C: The question states that password replication is not acceptable. A read-only Active Directory server in the corporate DMZ would involve password replication.

D: Allowing external connections to the existing corporate RADIUS server is not a secure solution. It is also not a solution that has wide compatibility among SaaS vendors.

References:

<https://www.onelogin.com/company/press/press-releases/97-percent-of-saas-vendors-backingsaml-based-single-sign-on>

https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

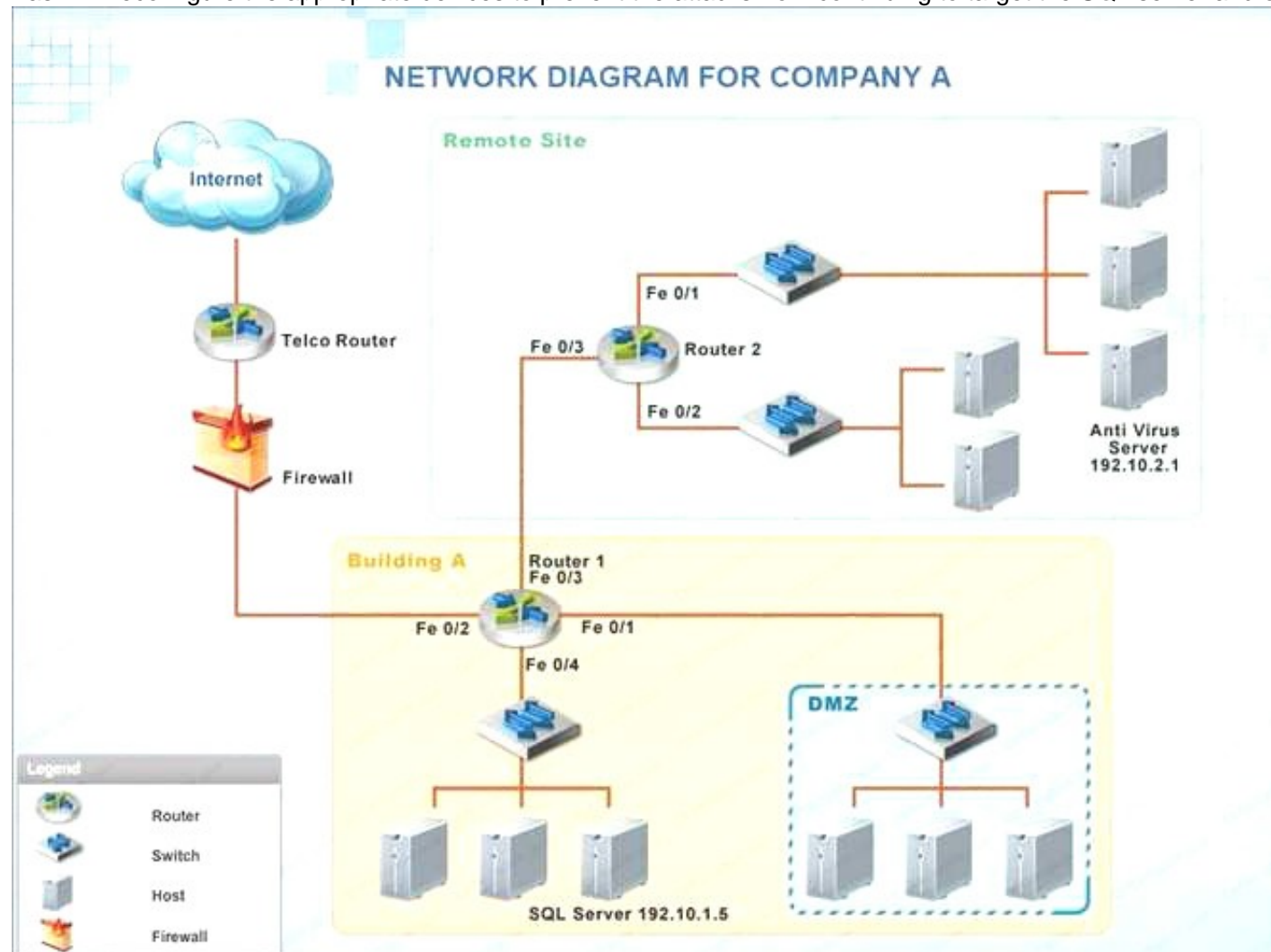
NEW QUESTION 163

Company A has noticed abnormal behavior targeting their SQL server on the network from a rogue IP address. The company uses the following internal IP address ranges: 192.10.1.0/24 for the corporate site and 192.10.2.0/24 for the remote site. The Telco router interface uses the 192.10.5.0/30 IP range.

Instructions: Click on the simulation button to refer to the Network Diagram for Company A. Click on Router 1, Router 2, and the Firewall to evaluate and configure each device.

Task 1: Display and examine the logs and status of Router 1, Router 2, and Firewall interfaces.

Task 2: Reconfigure the appropriate devices to prevent the attacks from continuing to target the SQL server and other servers on the corporate network.




```

Router1
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.775:%Router1: ICMP Echo Request - from 192.10.3.204 to 192.10.1.5
*Jul 15 14:47:29.776:%Router1: list 101 permitted icmp 192.10.3.204 (FastEthernet 0/3) ->
192.10.1.5, 6 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet
0/3) -> 192.10.1.5 (80), 3 packets.

```

```

Router2
*Jul 15 10:47:27: %FW-6-INIT: Firewall inspection startup completed;
beginning operation.
*Jul 15 14:47:29.777:%Router2: ICMP Echo Request - from 192.10.3.254 to 192.10.2.1
*Jul 15 14:47:29.778:%Router2: list 101 permitted icmp 192.10.3.254 (FastEthernet 0/2) ->
192.10.2.1, 5 packets.
*Jul 15 09:47:32: %SYS-6-CLOCKUPDATE: System clock has been updated from
14:47:32 UTC Sun Jul 15 2007 to 09:47:32 EST Sun Jul 15 2007, configured
from console by console.
*Jul 15 14:47:29.779:%Router2: list 101 permitted tcp 192.10.3.254(35650) (FastEthernet
0/2) -> 192.10.2.1 (80), 2 packets.

```

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			

A. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.3.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>

B. Check the answer below

FIREWALL ACCESS CONTROL LIST (ACL)			
Source Address	Destination Address	Deny	Allow
0.0.0.0	192.10.0.0/30	<input checked="" type="checkbox"/>	<input type="checkbox"/>
0.0.0.0	192.10.0.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.3.0/24	192.10.1.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.4.0/24	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.10.4.0/29	<input type="checkbox"/>	<input checked="" type="checkbox"/>
0.0.0.0	192.100.3.0/24	<input checked="" type="checkbox"/>	<input type="checkbox"/>
192.10.5.0/30	192.10.0.0/16	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.1.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
192.10.5.0/30	192.10.2.0/24	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IP Any	IP Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Reset ACL"/> <input type="button" value="Save"/> <input type="button" value="Exit"/>			

We have traffic coming from two rogue IP addresses: 192.10.3.204 and 192.10.3.254 (both in the 192.10.3.0/24 subnet) going to IPs in the corporate site subnet (192.10.1.0/24) and the remote site subnet (192.10.2.0/24). We need to Deny (block) this traffic at the firewall by ticking the following two checkboxes:

192.10.3.0/24	192.10.1.0/24	<input type="checkbox"/>	<input type="checkbox"/>
192.10.3.0/24	192.10.2.0/24	<input type="checkbox"/>	<input type="checkbox"/>

Answer: A

NEW QUESTION 168

Compliance with company policy requires a quarterly review of firewall rules. A new administrator is asked to conduct this review on the internal firewall sitting between several internal networks. The intent of this firewall is to make traffic more restrictive. Given the following information answer the questions below:
 User Subnet: 192.168.1.0/24 Server Subnet: 192.168.2.0/24 Finance Subnet: 192.168.3.0/24 Instructions: To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns. Firewall ACLs are read from the top down
 Task 1) An administrator added a rule to allow their machine terminal server access to the server subnet. This rule is not working. Identify the rule and correct this issue.

Task 2) All web servers have been changed to communicate solely over SSL. Modify the appropriate rule to allow communications.

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network. This rule is not working. Identify and correct this issue.

Task 4) Other than allowing all hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.

Firewall Interface

Instructions:

To perform the necessary tasks, please modify the DST port, Protocol, Action, and/or Rule Order columns.

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆️ ⬇️
any	any	any	any	any	Permit	⬆️ ⬇️
any	any	192.168.2.11	1433	UDP	Deny	⬆️ ⬇️
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⬆️ ⬇️
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⬆️ ⬇️
any	any	192.168.2.33	80	TCP	Permit	⬆️ ⬇️



A. Check the answer below

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	⬆️ ⬇️
any	any	192.168.2.33	443	TCP	Permit	⬆️ ⬇️
any	any	192.168.2.11	1433	TCP	Deny	⬆️ ⬇️
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	⬆️ ⬇️
192.168.1.5	any	192.168.2.0/24	any	any	Deny	⬆️ ⬇️
any	any	any	any	any	Deny	⬆️ ⬇️

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne

B. This rule is not workin

C. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio

D. It is not working because the action is set to Den

E. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	⬆️ ⬇️
--------------	-----	----------------	------	-----	------	-------

Task 2)

All web servers have been changed to communicate solely over SS

F. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo

G. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).

any	any	192.168.2.33	80	TCP	Permit	⬆️ ⬇️
-----	-----	--------------	----	-----	--------	-------

Task 3) An administrator added a rule to block access to the SQL server from anywhere on the network

H. This rule is not workin

I. Identify and correct this issue.The SQL Server rule is shown in the image belo

J. It is not working because the protocol is wron

K. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny	⬆️ ⬇️
-----	-----	--------------	------	-----	------	-------

Task 4) Other than allowing all

hosts to do network time and SSL, modify a rule to ensure that no other traffic is allowed.The network time rule is shown in the image below.

However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rule
L. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit	↑	↓
-----	-----	-----	-----	-----	--------	---	---

M. Check the answer below

SRC	SRC Port	DST	DST Port	Protocol	Action	Rule Order	
192.168.1.10	any	192.168.2.0/24	3389	any	Permit	↑	↓
any	any	192.168.2.33	443	TCP	Permit	↑	↓
any	any	192.168.2.11	1433	TCP	Deny	↑	↓
192.168.1.0/24	any	192.168.2.0/24	123	UDP	Permit	↑	↓
192.168.1.5	any	192.168.2.0/24	any	any	Deny	↑	↓
any	any	any	any	any	Deny	↑	↓

Task 1) An administrator added a rule to allow their machine terminal server access to the server subne

N. This rule is not workin

O. Identify the rule and correct this issue.The rule shown in the image below is the rule in questio

P. It is not working because the action is set to Den

Q. This needs to be set to Permit.

192.168.1.10	any	192.168.2.0/24	3389	any	Deny	↑	↓
--------------	-----	----------------	------	-----	------	---	---

Task 2)

All web servers have been changed to communicate solely over SS

R. Modify the appropriate rule to allow communications.The web servers rule is shown in the image belo

S. Port 80 (HTTP) needs to be changed to port 443 for HTTPS (HTTP over SSL).Task 3) An administrator added a rule to block access to the SQL server from anywhere on the networ

T. This rule is not workin

. Identify and correct this issue.The SQL Server rule is shown in the image belo

. It is not working because the protocol is wron

. It should be TCP, not UDP.

any	any	192.168.2.11	1433	UDP	Deny	↑	↓
-----	-----	--------------	------	-----	------	---	---

Task 4)

Other than allowing all hosts to do network time and SSL, modify a rule to ensure that noother traffic is allowed.The network time rule is shown in the image below.However, this rule is not being used because the ‘any’ rule shown below allows all traffic and the rule is placed above the network time rul

. To block all other traffic, the ‘any’ rule needs to be set to Deny, not Permit and the rule needs to be placed below all the other rules (it needs to be placed atthe bottom of the list to the rule is enumerated last).

any	any	any	any	any	Permit	↑	↓
-----	-----	-----	-----	-----	--------	---	---

Answer: A

NEW QUESTION 171

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer dat

- A. The Chief Risk Officer (CRO) is concerned about the outsourcingplan
- B. Which of the following risks are MOST likely to occur if adequate controls are not implemented?
- C. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
- D. Improper handling of client data, interoperability agreement issues and regulatory issues
- E. Cultural differences, increased cost of doing business and divestiture issues
- F. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

Explanation:

The risk of security violations or compromised intellectual property (IP) rights is inherently elevated when working internationally. A key concern with outsourcing arrangements is making sure that there is sufficient protection and security in place for personal information being transferred and/or accessed under an outsourcing agreement.

Incorrect Answers:

- A: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
 - B: Interoperability agreement issues are not a major risk when outsourcing to a third party company in another country.
 - C: Divestiture is the disposition or sale of an asset that is not performing well, and which is not vital to the company's core business, or which is worth more to a potential buyer or as a separate entity than as part of the company.
- References: <http://www.lexology.com/library>
"http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e- 940e14e94ce4"/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4
<http://www.investorwords.com/1508/divestiture.html#ixzz3knAHr58A>

NEW QUESTION 175

An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

- A. Ensure the SaaS provider supports dual factor authentication.
- B. Ensure the SaaS provider supports encrypted password transmission and storage.

- C. Ensure the SaaS provider supports secure hash file exchange.
- D. Ensure the SaaS provider supports role-based access control.
- E. Ensure the SaaS provider supports directory services federatio

Answer: E

Explanation:

A SaaS application that has a federation server within the customer's network that interfaces with the customer's own enterprise user-directory service can provide single sign-on authentication. This federation server has a trust relationship with a corresponding federation server located within the SaaS provider's network. Single sign-on will mitigate the risk of managing separate user credentials. Incorrect Answers:

A: Dual factor authentication will provide identification of users via a combination of two different components. It will not, however, mitigate the risk of managing separate user credentials.

B: The transmission and storage of encrypted passwords will not mitigate the risk of managing separate user credentials.

C: A hash file is a file that has been converted into a numerical string by a mathematical algorithm, and has to be unencrypted with a hash key to be understood. It will not, however, mitigate the risk of managing separate user credentials.

D: Role-based access control (RBAC) refers to the restriction of system access to authorized users. It will not, however, mitigate the risk of managing separate user credentials.

References:

<https://msdn.microsoft.com/en-us/library/aa905332.aspx> https://en.wikipedia.org/wiki/Two-factor_authentication <https://en.wikipedia.org/wiki/Encryption>

<http://www.wisegeek.com/what-are-hash-files.htm> https://en.wikipedia.org/wiki/Role-based_access_control

NEW QUESTION 176

After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

- A. Least privilege
- B. Job rotation
- C. Mandatory vacation
- D. Separation of duties

Answer: B

Explanation:

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

A: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

C: Mandatory vacation is used to discover misuse and allow the organization time to audit a suspected employee while they are away from work.

D: Separation of duties requires more than one person to complete a task. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 245

NEW QUESTION 178

A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and require two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

- A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
- B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
- C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.
- D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
- E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: AD

Explanation:

Privacy could be compromised because patient records can be from a doctor's personal device. This can then be shown to persons not authorized to view this information. Similarly, the doctor's personal device could have malware on it.

Incorrect Answers:

B: Device encryption is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

C: The guest WiFi network is isolated from the internal network with appropriate security controls and the doctors and specialists can interact with the hospital's system via a remote desktop type interface.

E: Remote wiping is a BYOD concern, but the question asks "Which of the following are of MOST concern?" Patient privacy and Malware threats would be of more concern.

References:

<http://www.gwava.com/blog/top-10-byod-business-concerns>

NEW QUESTION 182

A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

- A. The malware file's modify, access, change time properties.
- B. The timeline analysis of the file system.
- C. The time stamp of the malware in the swap file.
- D. The date/time stamp of the malware detection in the antivirus log

Answer: B

Explanation:

Timelines can be used in digital forensics to identify when activity occurred on a computer. Timelines are mainly used for data reduction or identifying specific state changes that have occurred on a computer.

Incorrect Answers:

A: This option will not help to determine when the system became infected.

C: A swap file is a space on a hard disk used as the virtual memory extension of a computer's real memory, which allows your computer's operating system to pretend that you have more RAM than you actually do.

D: This will tell you when the antivirus detected the malware, not when the system became infected. References:

<http://www.basistech.com/autopsy-feature-graphical-timeline-analysis-for-cyber-forensics/> <http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile>

"<http://searchwindowsserver.techtarget.com/definition/swap-file-swap-space-or-pagefile>"

NEW QUESTION 187

A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

- A. Begin a chain-of-custody on for the user's communicatio
- B. Next, place a legal hold on the user's email account.
- C. Perform an e-discover using the applicable search term
- D. Next, back up the user's email for a future investigation.
- E. Place a legal hold on the user's email accoun
- F. Next, perform e-discovery searches to collect applicable emails.
- G. Perform a back up of the user's email accoun
- H. Next, export the applicable emails that match the search terms.

Answer: C

Explanation:

A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

Incorrect Answers:

A: Chain of custody (CoC) refers to the chronological documentation showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

B: Potentially relevant data has to be placed on hold before e-discovery takes place. D: This option could still allow the email to be tampered with.

References: https://en.wikipedia.org/wiki/Electronic_discovery#Types_of_ESI https://en.wikipedia.org/wiki/Chain_of_custody

"https://en.wikipedia.org/wiki/Chain_of_custody" https://en.wikipedia.org/wiki/Legal_hold

NEW QUESTION 190

The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

- A. Review the flow data against each server's baseline communications profile.
- B. Configure the server logs to collect unusual activity including failed logins and restarted services.
- C. Correlate data loss prevention logs for anomalous communications from the server.
- D. Setup a packet capture on the firewall to collect all of the server communication

Answer: A

Explanation:

Network logging tools such as Syslog, DNS, NetFlow, behavior analytics, IP reputation, honeypots, and DLP solutions provide visibility into the entire infrastructure. This visibility is important because signature-based systems are no longer sufficient for identifying the advanced attacker that relies heavily on custom malware and zero-day exploits. Having knowledge of each host's communications, protocols, and traffic volumes as well as the content of the data in question is key to identifying zeroday and APT (advance persistent threat) malware and agents. Data intelligence allows forensic analysis to identify anomalous or suspicious communications by comparing suspected traffic patterns against normal data communication behavioral baselines. Automated network intelligence and next-generation live forensics provide insight into network events and rely on analytical decisions based on known vs. unknown behavior taking place within a corporate network. Incorrect Answers:

B: The attack has already happened; the server has already been compromised. Configuring the server logs to collect unusual activity including failed logins and restarted services might help against future attacks but it will not provide information on an attack that has already happened.

C: It is unlikely the DLP logs would contain anomalous communications from the server that would identify where the server collected the information.

D: The attack has already happened; the server has already been compromised. Setting up a packet capture on the firewall to collect all of the server communications might help against future attacks but it will not provide information on an attack that has already happened.

References:

[https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952](https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics-35952) [https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics- 35952](https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics-35952)

"<https://www.sans.org/reading-room/whitepapers/forensics/ids-fileforensics-35952>"le-forensics- 35952, p. 6

NEW QUESTION 191

A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

- A. Background checks
- B. Job rotation
- C. Least privilege
- D. Employee termination procedures

Answer: B

Explanation:

Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.

Incorrect Answers:

A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.

C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.

D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246

NEW QUESTION 195

During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non-volatile storage, implement chain of custody, and analyze original media.

B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.

C. Implement chain of custody, take inventory, secure the scene, capture volatile and non-volatile storage, and document the findings.

D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Answer: D

Explanation:

The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.

Incorrect Answers:

A: To prevent contamination, the scene should be secured first. B: The scene should be secured before taking inventory.

C: Implementing a chain of custody can only occur once evidence has been accessed. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 250-254

NEW QUESTION 199

A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual's experience.

B. Requires a high degree of upfront work to gather environment details.

C. Difficult to differentiate between high, medium, and low risks.

D. Allows for cost and benefit analysis.

E. Calculations can be extremely complex to manage

Answer: A

Explanation:

Using likelihood and consequence to determine risk is known as qualitative risk analysis.

With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system. After qualitative analysis has been performed, you can then perform quantitative risk analysis. A

Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.

Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.

Incorrect Answers:

B: Qualitative risk analysis does not require a high degree of upfront work to gather environment details. This answer applies more to quantitative risk analysis.

C: Although qualitative risk analysis does not use numeric values to quantify likelihood or consequence compared to quantitative analysis, we can all differentiate between the terms high, medium, and low when talking about risk.

D: Qualitative risk analysis does not allow for cost and benefit analysis, quantitative risk analysis does.

E: Calculations for qualitative risk analysis are not extremely complex to manage; they can be quantitative risk analysis.

References: <https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmpconcept-1>

"<https://www.passionatepm.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmpconcept-1>"

NEW QUESTION 202

The IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.

B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.

C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.

D. Refer the issue to management for handling according to the incident response process

Answer: D

Explanation:

The database contains PII (personally identifiable information) so the natural response is to want to get the issue addressed as soon as possible. However, in this question we have an IT Security Analyst working on a customer's system. Therefore, this IT Security Analyst does not know what the customer's incident response process is. In this case, the IT Security Analyst should refer the issue to company management so they can handle the issue (with your help if required) according to their incident response procedures.

Incorrect Answers:

A: Contacting the local authorities so an investigation can be started as quickly as possible would not be the first step. Apart from the fact an investigation could take any amount of time; this action does nothing to actually stop the unauthorized access.

B: Shutting down the production network interfaces on the server and changing all of the DBMS account passwords may be a step in the company's incident response procedure. However, as the IT Security Analyst does not know what the customer's incident response process is, he should notify management so they can make that decision.

C: Disabling the front-end web server may or may not stop the unauthorized access to the database server. However, taking a company web server offline may have a damaging impact on the company so the IT Security Analyst should not make that decision without consulting the management. Using email to determine how the customer would like to proceed is not appropriate method of communication. For something this urgent, a face-to-face meeting or at least a phone call would be more appropriate.

NEW QUESTION 207

A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

- A. Code review
- B. Penetration testing
- C. Grey box testing
- D. Code signing
- E. White box testing

Answer: AE

Explanation:

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization.

White box testing assumes that the penetration test team has full knowledge of the network and the infrastructure per se thus rendering the testing to follow a more structured approach.

Incorrect Answers:

B: Penetration testing is a broad term to refer to all the different types of tests such as back box-, white box and gray box testing.

C: Grey Box testing is similar to white box testing, but not as insightful.

D: Code signing is the term used to refer to the process of digitally signing executables and scripts to confirm the author. This is not applicable in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 18, 168-169

NEW QUESTION 210

A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

- A. RAS
- B. Vulnerability scanner
- C. HTTP intercept
- D. HIDS
- E. Port scanner
- F. Protocol analyzer

Answer: DF

Explanation:

A protocol analyzer can be used to capture and analyze signals and data traffic over a communication channel which makes it ideal for use to assess a company's network from within under the circumstances.

HIDS is used as an intrusion detection system that can monitor and analyze the internal company network especially the dynamic behavior and the state of the computer systems; behavior such as network packets targeted at that specific host, which programs accesses what resources etc. Incorrect Answers:

A: RAS is a term that refers to any combination of hardware or software that will enable the remote access tools or information that typically reside on a network of IT devices. This tool will not allow you to detect the presence of a malicious actor physical accessing the network from within.

B: Vulnerability scanners are used to identify vulnerable systems and applications that may be in need of patching.

C: A HTTP Interceptor is a program that is used to assess and analyze web traffic and works by acting as a proxy for the traffic between the web client and the web server, not useful in this scenario.

E: Port Scanners are used to scan the TCP and UDP ports as well as their status. Port scanning makes allowance to run probes to check which services are running on a targeted computer.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 137-138, 181, 399-402
https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

NEW QUESTION 213

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company.

Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be \$150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.

Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.

Bundled offering expected to be \$100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be \$80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

- A. Based on cost alone, having an outsourced solution appears cheaper.
- B. Based on cost alone, having an outsourced solution appears to be more expensive.
- C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
- D. Based on cost alone, having a purchased product solution appears cheaper

Answer: A

Explanation:

The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if \$80,000 per year per FTE.

For the company to go alone it will cost \$80,000 per annum per FTE = \$400,000 over 5 years. With Vendor a \$150,000 + \$200,000 (½ FTE) = \$350,000

With Vendor B = \$100,000 it will be more expensive. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 130

NEW QUESTION 218

Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).

- A. Check log files for logins from unauthorized IPs.
- B. Check /proc/kmem for fragmented memory segments.
- C. Check for unencrypted passwords in /etc/shadow.
- D. Check timestamps for files modified around time of compromise.
- E. Use Isot to determine files with future timestamps.
- F. Use gpg to encrypt compromised data files.
- G. Verify the MD5 checksum of system binaries.
- H. Use vmstat to look for excessive disk I/

Answer: ADG

Explanation:

The MD5 checksum of the system binaries will allow you to carry out a forensic analysis of the compromised Linux system. Together with the log files of logins into the compromised system from unauthorized IPs and the timestamps for those files that were modified around the time that the compromise occurred will serve as useful forensic tools.

Incorrect Answers:

B: Checking for fragmented memory segments' is not a forensic analysis tool to be used in this case. C: The ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account. This is a useful tool for Linux passwords and shadow file formats and is in essence used to keep user account information.

E: Isot is used on Linux as a future timestamp tool and not a forensic analysis tool. F: Gpg is an encryption tool that works on Mac OS X.

H: vmstat reports information about processes, memory, paging, block IO, traps, and cpu activity. The first report produced gives averages since the last reboot. Additional reports give information on a sampling period of length delay. The process and memory reports are instantaneous in either case. This is more of an administrator tool.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 387

https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

NEW QUESTION 223

A system worth \$100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system's SLE?

- A. \$2,000
- B. \$8,000
- C. \$12,000
- D. \$32,000

Answer: B

Explanation:

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF) SLE = AV x EF = \$100 000 x 8% = \$ 8 000

References: http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

NEW QUESTION 228

An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

- A. Implement data analytics to try and correlate the occurrence times.
- B. Implement a honey pot to capture traffic during the next attack.
- C. Configure the servers for high availability to handle the additional bandwidth.
- D. Log all traffic coming from the competitor's public IP address

Answer: A

Explanation:

There is a time aspect to the traffic flood and if you correlate the data analytics with the times that the incidents happened, you will be able to prove the theory.

Incorrect Answers:

B: A honey pot is designed to attract traffic and this will not prove the theory.

C: Configuring any of your servers for high availability will only accommodate the competitor and not prove your theory.

D: Logging all incoming traffic will not prove the theory as you want to check whether the incidents occur when the competitor makes major announcement a not all of the incoming traffic, even it if is from the competitor.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 114-115

NEW QUESTION 229

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM. Requirement 1: The system shall provide confidentiality for data in transit and data at rest. Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme. Requirement 4: The system shall provide integrity for all data at rest. Requirement 5: The system shall perform CRC checks on all files.

- A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5
- B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4
- C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2
- D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Answer: B

Explanation:

Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are Level 1 requirements.

Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files. In the SRTM hierarchy, the enforcement methods would fall under the Level requirement. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

NEW QUESTION 230

The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems. The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

- A. Web cameras
- B. Email
- C. Instant messaging
- D. BYOD
- E. Desktop sharing
- F. Presence

Answer: CE

Explanation:

C: Instant messaging (IM) allows two-way communication in near real time, allowing users to collaborate, hold informal chat meetings, and share files and information. Some IM platforms have added encryption, central logging, and user access controls. This can be used to replace calls between the end-user and the helpdesk.

E: Desktop sharing allows a remote user access to another user's desktop and has the ability to function as a remote system administration tool. This can allow the helpdesk to determine the cause of the problem on the end-users desktop.

Incorrect Answers:

A: Web cameras can be used for videoconferencing. This can be used to replace calls between the end-user and the helpdesk but would require the presence of web cameras and sufficient bandwidth. B: Email can be used to replace calls between the end-user and the helpdesk but email communication is not in real-time.

D: Bring your own device (BYOD) is a relatively new phenomena in which company employees are allowed to connect their personal devices, such as smart phones and tablets to the corporate network and use those devices for work purposes.

F: Presence is an Apple software product that is similar to Windows Remote Desktop. It gives users access to their Mac's files wherever they are. It also allows users to share files and data between a Mac, iPhone, and iPad.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 347, 348, 351

NEW QUESTION 231

An intruder was recently discovered inside the data center, a highly sensitive are

- A. To gain access, the intruder circumvented numerous layers of physical and electronic security measure
- B. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again
- C. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).
- D. Facilities management
- E. Human resources
- F. Research and development
- G. Programming
- H. Data center operations
- I. Marketing
- J. Information technology

Answer: AEG

Explanation:

A: Facilities management is responsible for the physical security measures in a facility or building. E: The breach occurred in the data center, therefore the Data center operations would be greatly concerned.

G: Data centers are important aspects of information technology (IT) in large corporations. Therefore the IT department would be greatly concerned.

Incorrect Answers:

B: Human Resources security is concerned with employees joining an organization, moving between different positions in the organization, and leaving the organization.

C: Research and Development is concerned with security at the design and development stage of a system.

D: Programming security is concerned with application code and application vulnerabilities. F: Marketing is not concerned with security.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 281, 326-328

NEW QUESTION 236

An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data

sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

- A. Implement hashing of data in transit
- B. Session recording and capture
- C. Disable cross session cut and paste
- D. Monitor approved credit accounts
- E. User access audit reviews
- F. Source IP whitelisting

Answer: CEF

Explanation:

Data sovereignty is a legal concern where the data is governed by the laws of the country in which the data resides. In this scenario the company does not want the data to fall under the law of the country of the organization to whom back office process has be outsourced to. Therefore we must ensure that data can only be accessed on local servers and no copies are held on computers of the outsource partner. It is important therefore to prevent cut and paste operations.

Privacy concerns can be addressed by ensuring the unauthorized users do not have access to the dat

A. This can be accomplished though user access auditing, which needs to be reviewed on an ongoing basis; and source IP whitelisting, which is a list of IP addresses that are explicitly allowed access to the system.

Incorrect Answers:

A: Hashing is used to ensure data integrity. In other words, it ensures that the data has not been altered and is in its true, original state. This does not address data sovereignty and privacy concerns. B: Session recording and capture would represent an additional potential threat for privacy concerns should an unauthorized user access the recorded session data.

D: The monitoring of approved credit accounts is a processing issue. It is not related to data sovereignty or privacy concerns.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 17-19, 204, 247

NEW QUESTION 238

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CAS-003 Practice Exam Features:

- * CAS-003 Questions and Answers Updated Frequently
- * CAS-003 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-003 Practice Test Here](#)