



CompTIA

Exam Questions CAS-003

CompTIA Advanced Security Practitioner (CASP)

NEW QUESTION 1

A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control answer. The total cost of the device must be kept to a minimum in case the device is discovered during an assessment. Which of the following tools should the engineer load onto the device being designed?

- A. Custom firmware with rotating key generation
- B. Automatic MITM proxy
- C. TCP beacon broadcast software
- D. Reverse shell endpoint listener

Answer: B

NEW QUESTION 2

A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

The person extracts the following data from the phone and EXIF data from some files:

DCIM Images folder

Audio books folder Torrentz

My TAX.xls

Consultancy HR Manual.doc Camera: SM-G950F Exposure time: 1/60s

Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

- A. MicroSD is not encrypted and also contains personal data.
- B. MicroSD contains a mixture of personal and work data.
- C. MicroSD is not encrypted and contains geotagging information.
- D. MicroSD contains pirated software and is not encrypted

Answer: A

NEW QUESTION 3

A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

- A. Reconfigure the firewall to block external UDP traffic.
- B. Establish a security baseline on the IDS.
- C. Block echo reply traffic at the firewall.
- D. Modify the edge router to not forward broadcast traffic

Answer: B

NEW QUESTION 4

An administrator is working with management to develop policies related to the use of the cloud-based resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

- A. MDM
- B. Sandboxing
- C. Mobile tokenization
- D. FDE
- E. MFA

Answer: A

NEW QUESTION 5

Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company. Which of the following should the systems administrator do to BEST address this problem?

- A. Add an ACL to the firewall to block VoIP.
- B. Change the settings on the phone system to use SIP-TLS.
- C. Have the phones download new configurations over TFTP.
- D. Enable QoS configuration on the phone VLAN

Answer: B

NEW QUESTION 6

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements: The data is for internal consumption only and shall not be distributed to outside individuals. The systems administrator should not have access to the data processed by the server.

The integrity of the kernel image is maintained.

Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

- A. SELinux
- B. DLP

- C. HIDS
- D. Host-based firewall
- E. Measured boot
- F. Data encryption
- G. Watermarking

Answer: CEF

NEW QUESTION 7

An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

- A. Secure storage policies
- B. Browser security updates
- C. Input validation
- D. Web application firewall
- E. Secure coding standards
- F. Database activity monitoring

Answer: CF

NEW QUESTION 8

A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

- A. ISA
- B. BIA
- C. SLA
- D. RA

Answer: C

NEW QUESTION 9

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 10

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

```
C:\>nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org      Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

- A. The public/private views on the Comptia.org DNS servers are misconfigured
- B. Comptia.org is running an older mail server, which may be vulnerable to exploits
- C. The DNS SPF records have not been updated for Comptia.org
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Answer: B

NEW QUESTION 10

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 14

During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

- A. Air gaps
- B. Access control lists
- C. Spanning tree protocol
- D. Network virtualization
- E. Elastic load balancing

Answer: D

NEW QUESTION 15

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 20

A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)#ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

Which of the following is the engineer implementing?

- A. Remotely triggered black hole
- B. Route protection
- C. Port security
- D. Transport security
- E. Address space layout randomization

Answer: B

NEW QUESTION 25

A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

Antivirus	Enabled
AV Engine	Current
AV Signatures	Auto Update
Update Status	Success
Heuristic Scanning	Enabled
Scan Type	On Access Scanning
Malware Engine	Enabled
Auto System Update	Enabled
Last System Update	Yesterday 2 PM
DLP Agent	Disabled
DLP DB Update	Poll every 5 mins
Proxy Settings	Auto

Which of the following would BEST prevent the problem from reoccurring in the future? (Choose two.)

- A. Install HIPS
- B. Enable DLP
- C. Install EDR
- D. Install HIDS
- E. Enable application blacklisting
- F. Improve patch management processes

Answer: BE

NEW QUESTION 30

An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

- A. Deploy virtual desktop infrastructure with an OOB management network
- B. Employ the use of vTPM with boot attestation
- C. Leverage separate physical hardware for sensitive services and data
- D. Use a community CSP with independently managed security services
- E. Deploy to a private cloud with hosted hypervisors on each physical machine

Answer: AC

NEW QUESTION 31

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 36

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 37

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 39

A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

- A. Issue digital certificates to all users, including owners of group mailboxes, and enable S/MIME
- B. Federate with an existing PKI provider, and reject all non-signed emails
- C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
- D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Answer: A

NEW QUESTION 40

A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

- A. Implementing regression testing
- B. Completing user acceptance testing
- C. Verifying system design documentation
- D. Using a SRTM

Answer: D

NEW QUESTION 44

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 49

A business is growing and starting to branch out into other locations. In anticipation of opening an office in a different country, the Chief Information Security Officer (CISO) and legal team agree they need to meet the following criteria regarding data to open the new office:

Store taxation-related documents for five years
Store customer addresses in an encrypted format
Destroy customer information after one year
Keep data only in the customer's home country

Which of the following should the CISO implement to BEST meet these requirements? (Choose three.)

- A. Capacity planning policy
- B. Data retention policy
- C. Data classification standard
- D. Legal compliance policy
- E. Data sovereignty policy
- F. Backup policy
- G. Acceptable use policy
- H. Encryption standard

Answer: BCH

NEW QUESTION 50

The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, "criticalValue" indicates if an emergency is underway:

```
try {
    if (criticalValue)
        openDoors=true
    else
        OpenDoors=false
} catch (e) {
    OpenDoors=true
}
```

Which of the following is the BEST course of action for a security analyst to recommend to the software developer?

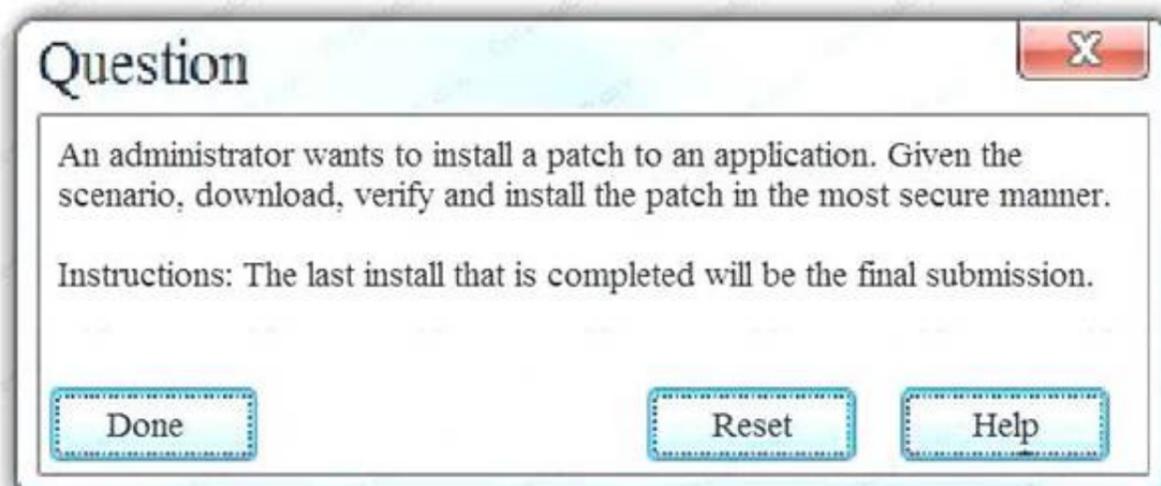
- A. Rewrite the software to implement fine-grained, conditions-based testing
- B. Add additional exception handling logic to the main program to prevent doors from being opened
- C. Apply for a life-safety-based risk exception allowing secure doors to fail open
- D. Rewrite the software's exception handling routine to fail in a secure state

Answer: B

NEW QUESTION 53

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		



- A. Step 1: Verify that the certificate is valid or no
- B. 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 websit
- C. Step 4: Install the file if the hash value matches.
- D. Step 1: Verify that the certificate is valid or no
- E. In case of any warning message, cancel the download.Step 2: If certificate issue is not there then, download the file in your syste
- F. 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 websit
- G. Step 5: Install the file if the hash value matches.

Answer: B

NEW QUESTION 56

A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded. Which of the following should be used to identify weak processes and other vulnerabilities?

- A. Gap analysis
- B. Benchmarks and baseline results
- C. Risk assessment
- D. Lessons learned report

Answer: D

NEW QUESTION 59

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides. Which of the following would be the BEST source of reference during the revision process?

- A. CVE database
- B. Internal security assessment reports
- C. Industry-accepted standards
- D. External vulnerability scan reports
- E. Vendor-specific implementation guides

Answer: A

NEW QUESTION 61

A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

- A. Effective deployment of network taps
- B. Overall bandwidth available at Internet PoP
- C. Optimal placement of log aggregators
- D. Availability of application layer visualizers

Answer: D

NEW QUESTION 63

A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials. Which of the following tools should be used? (Choose two.)

- A. Fuzzer
- B. SCAP scanner
- C. Packet analyzer
- D. Password cracker
- E. Network enumerator
- F. SIEM

Answer: BF

NEW QUESTION 68

A security technician is incorporating the following requirements in an RFP for a new SIEM: New security notifications must be dynamically implemented by the SIEM engine

The SIEM must be able to identify traffic baseline anomalies

Anonymous attack data from all customers must augment attack detection and risk scoring

Based on the above requirements, which of the following should the SIEM support? (Choose two.)

- A. Autoscaling search capability
- B. Machine learning
- C. Multisensor deployment
- D. Big Data analytics
- E. Cloud-based management
- F. Centralized log aggregation

Answer: BD

NEW QUESTION 71

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 72

Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth.

The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50 Mbps	20 Mbps
Des Moines	12	25 Mbps	19 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

- A. Vendor C for small remote sites, and Vendor B for large sites.
- B. Vendor B for all remote sites
- C. Vendor C for all remote sites
- D. Vendor A for all remote sites
- E. Vendor D for all remote sites

Answer: D

NEW QUESTION 73

A security researcher is gathering information about a recent spike in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

Based on the information available to the researcher, which of the following is the MOST likely threat profile?

- A. Nation-state-sponsored attackers conducting espionage for strategic gain.
- B. Insiders seeking to gain access to funds for illicit purposes.
- C. Opportunists seeking notoriety and fame for personal gain.
- D. Hackvisits seeking to make a political statement because of socio-economic factor

Answer: D

NEW QUESTION 74

An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations. Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

- A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.
- B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.
- C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.
- D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

Answer: B

NEW QUESTION 76

A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

Which of the following tools is the engineer utilizing to perform this assessment?

F. Tabletop exercise

Answer: AC

NEW QUESTION 92

A cybersecurity analyst is conducting packet analysis on the following:

Time	Source	Destination	Info
0.000673	00:48:c2:5f:39:57	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:57
0.001173	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.6 is at 00:48:c2:5f:39:9a
0.002346	00:48:c2:5f:39:2b	00:43:b3:3f:23:e3	172.16.1.12 is at 00:48:c2:5f:39:2b
0.005123	00:48:c2:5f:39:42	00:43:b3:3f:23:e3	172.16.1.13 is at 00:48:c2:5f:39:42
0.010201	00:48:c2:5f:39:6b	00:43:b3:3f:23:e3	172.16.1.2 is at 00:48:c2:5f:39:6b
0.021597	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a
0.044612	00:48:c2:5f:39:3c	00:43:b3:3f:23:e3	172.16.1.21 is at 00:48:c2:5f:39:3c
0.06512	00:48:c2:5f:39:9a	00:43:b3:3f:23:e3	172.16.1.7 is at 00:48:c2:5f:39:9a

Which of the following is occurring in the given packet capture?

- A. ARP spoofing
- B. Broadcast storm
- C. Smurf attack
- D. Network enumeration
- E. Zero-day exploit

Answer: A

NEW QUESTION 94

Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

- A. Enable multipath to increase availability
- B. Enable deduplication on the storage pools
- C. Implement snapshots to reduce virtual disk size
- D. Implement replication to offsite datacenter

Answer: B

Explanation:

Storage-based data deduplication reduces the amount of storage needed for a given set of files. It is most effective in applications where many copies of very similar or even identical data are stored on a single disk.

It is common for multiple copies of files to exist on a SAN. By eliminating (deduplicating) repeated copies of the files, we can reduce the disk space used on the existing SAN. This solution is a cost effective alternative to buying a new SAN.

Incorrect Answers:

A: Multipathing enables multiple links to transfer the data to and from the SAN. This improves performance and link redundancy. However, it has no effect on the amount of data on the SAN. C: Snapshots would not reduce the amount of data stored on the SAN.

D: Replicating the data on the SAN to an offsite datacenter will not reduce the amount of data stored on the SAN. It would just create another copy of the data on the SAN in the offsite datacenter. References:

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

NEW QUESTION 95

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

- A. vTPM
- B. HSM
- C. TPM
- D. INE

Answer: A

Explanation:

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus.

A vTPM is a virtual Trusted Platform Module.

IBM extended the current TPM V1.2 command set with virtual TPM management commands that allow us to create and delete instances of TPMs. Each created instance of a TPM holds an association with a virtual machine (VM) throughout its lifetime on the platform.

Incorrect Answers:

B: A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. This solution would require hardware pass-through.

C: A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer, and it communicates with the remainder of the system by using a hardware bus. Virtual machines cannot access a hardware TPM.

D: INE (intelligent network element) is not used for storing cryptographic keys. References:

https://en.wikipedia.org/wiki/Hardware_security_module <http://HYPERLINK>

"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"researcher.watson.ibm.com/researcher/HYPERLINK

"http://researcher.watson.ibm.com/researcher/view_group.php?id=2850"view_group.php?id=2850

NEW QUESTION 98

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 102

An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

- A. Deploy custom HIPS signatures to detect and block the attacks.
- B. Validate and deploy the appropriate patch.
- C. Run the application in terminal services to reduce the threat landscape.
- D. Deploy custom NIPS signatures to detect and block the attack

Answer: B

Explanation:

If an application has a known issue (such as susceptibility to buffer overflow attacks) and a patch is released to resolve the specific issue, then the best solution is always to deploy the patch.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: This question is asking for the MOST comprehensive way to resolve the issue. A HIPS (Host Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

C: This question is asking for the MOST comprehensive way to resolve the issue. Running the application in terminal services may reduce the threat landscape. However, it doesn't resolve the issue. Patching the application to eliminate the threat is a better solution.

D: This question is asking for the MOST comprehensive way to resolve the issue. A NIPS (Network Intrusion Prevention System) with custom signatures may offer some protection against an application that is vulnerable to buffer overflow attacks. However, an application that is NOT vulnerable to buffer overflow attacks (a patched application) is a better solution.

References: <http://searchsecurity.techtarget.com/definition/buffer-overflow>

NEW QUESTION 107

An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

- A. Intermediate Root Certificate
- B. Wildcard Certificate
- C. EV x509 Certificate
- D. Subject Alternative Names Certificate

Answer: D

Explanation:

Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field. You can then add other names in the Subject Alternative Names field.

Incorrect Answers:

A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be used to secure multiple domains on a web server.

B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "*.example.com" can secure an unlimited number of domains that end in 'example.com' such as domain1.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.

C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NEW QUESTION 111

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 112

Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

- A. Jailbroken mobile device
- B. Reconnaissance tools
- C. Network enumerator
- D. HTTP interceptor
- E. Vulnerability scanner
- F. Password cracker

Answer: DE

Explanation:

Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor. To assess the security of the application server itself, you should use a vulnerability scanner.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

Incorrect Answers:

- A: A jailbroken mobile device is a mobile device with an operating system that has any built-in security restrictions removed. This enables you to install software and perform actions that the manufacturer did not intend. However, a jailbroken mobile device is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.
- B: Reconnaissance in terms of IT security is the process of learning as much as possible about a target business usually over a long period of time with a view to discovering security flaws. It is not used by security administrators for security assessment of client-server applications.
- C: Network enumeration is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It is not used to assess the security between the mobile web application and the RESTful application server.
- F: A password cracker is used to guess passwords. It is not a suitable security tool to assess the security between the mobile web application and the RESTful application server.

References: <http://www.webopedia.com/TERM/V/vulneHYPERLINK>

"http://www.webopedia.com/TERM/V/vulnerability_scanning.html"rability_scanning.html

NEW QUESTION 115

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 117

An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.

Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

- A. Static and dynamic analysis is run as part of integration
- B. Security standards and training is performed as part of the project
- C. Daily stand-up meetings are held to ensure security requirements are understood
- D. For each major iteration penetration testing is performed
- E. Security requirements are story boarded and make it into the build
- F. A security design is performed at the end of the requirements phase

Answer: AD

Explanation:

SDLC stands for systems development life cycle. An agile project is completed in small sections called iterations. Each iteration is reviewed and critiqued by the project team. Insights gained from the critique of an iteration are used to determine what the next step should be in the project. Each project iteration is typically scheduled to be completed within two weeks.

Static and dynamic security analysis should be performed throughout the project. Static program analysis is the analysis of computer software that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis). In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code.

For each major iteration penetration testing is performed. The output of a major iteration will be a functioning part of the application. This should be penetration tested to ensure security of the application.

Incorrect Answers:

B: Security standards and training does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

C: Ensuring security requirements are understood does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

E: Storyboarding security requirements does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

F: A security design does not ensure code quality from a security perspective. The only way to ensure code quality is to test the code itself.

References: https://en.wikipedia.org/wiki/Static_program_analysis

<http://searchcio.techtarget.com/definition/Agile-projectmanagement>

NEW QUESTION 120

ABC Corporation uses multiple security zones to protect systems and information, and all of the VM hosts are part of a consolidated VM infrastructure. Each zone has different VM administrators. Which of the following restricts different zone administrators from directly accessing the console of a VM host from another zone?

- A. Ensure hypervisor layer firewalling between all VM hosts regardless of security zone.
- B. Maintain a separate virtual switch for each security zone and ensure VM hosts bind to only the correct virtual NIC(s).
- C. Organize VM hosts into containers based on security zone and restrict access using an ACL.
- D. Require multi-factor authentication when accessing the console at the physical VM hos

Answer: C

Explanation:

Access Control Lists (ACLs) are used to restrict access to the console of a virtual host. Virtual hosts are often managed by centralized management servers (for example: VMware vCenter Server). You can create logical containers that can contain multiple hosts and you can configure ACLs on the containers to provide access to the hosts within the container. Incorrect Answers:

A: Hypervisor layer firewalling is used to restrict the network traffic that can access the host. It does not prevent a user from directly accessing the console of the host.

B: Maintaining a separate virtual switch for each security zone and ensuring VM hosts bind to only the correct virtual NIC(s) will restrict the network access of the VM hosts. It does not prevent a user from directly accessing the console of the host.

D: Multi-factor authentication is a secure way of authenticating a user. However, that's all it does: authenticates someone. In other words, it only proves that the person is who they say they are. You would still need an ACL to determine whether that person is allowed or not allowed to access the console of the host.

NEW QUESTION 125

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 128

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/hackerto HYPERLINK

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

NEW QUESTION 129

An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are: Each lab must be on a separate network segment.

Labs must have access to the Internet, but not other lab networks.

Student devices must have network access, not simple access to hosts on the lab networks. Students must have a private certificate installed before gaining access.

Servers must have a private certificate installed locally to provide assurance to the students. All students must use the same VPN connection profile.

Which of the following components should be used to achieve the design in conjunction with directory services?

- A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
- B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
- C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment
- D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C

Explanation:

IPSec VPN with mutual authentication meets the certificates requirements. RADIUS can be used with the directory service for the user authentication.

ACLs (access control lists) are the best solution for restricting access to network hosts. Incorrect Answers:

A: This solution has no provision for restricting access to hosts on the lab networks. B: This solution has no provision for restricting access to hosts on the lab networks. D: This solution has no provision for restricting access to hosts on the lab networks.

NEW QUESTION 134

A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

- A. Insider threat
- B. Network reconnaissance
- C. Physical security
- D. Industrial espionage

Answer: C

Explanation:

If all company users worked in the same office with one corporate network and using company supplied laptops, then it is easy to implement all sorts of physical security controls. Examples of physical security include intrusion detection systems, fire protection systems, surveillance cameras or simply a lock on the office door.

However, in this question we have dispersed employees using their own devices and frequently traveling internationally. This makes it extremely difficult to implement any kind of physical security. Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Incorrect Answers:

A: An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. Dispersed employees using presence technology does not increase the risk of insider threat when compared to employees working together in an office.

B: The risk of network reconnaissance is reduced by having dispersed employees using presence technology. The risk of network reconnaissance would be higher with employees working together in a single location such as an office.

D: Industrial espionage is a threat to any business whose livelihood depends on information. However, this threat is not increased by having dispersed employees using presence technology. The risk would be the same with dispersed employees using presence technology or employees working together in a single location such as an office.

References: <http://searchsecurity.techtarget.com/deHYPERLINK>

"<http://searchsecurity.techtarget.com/definition/physical-security>"finition/physical-security

NEW QUESTION 138

DRAG DROP

IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.

Security concerns	Security controls or gaps
Vendor may accidentally or maliciously make changes to IT system	
Desktop sharing traffic may be intercepted by network attackers	
No guarantees that shoulder surfing attacks are not occurring at the vendor	
Vendor may inadvertently see confidential material from the company, such as email or IM notifications	

Perform remote sessions over SSL/TLS	Full-disk encryption for data at rest	Limit desktop sharing to specific application windows
Implement data loss prevention	Allow view-only access to third parties	Require code signing
Identified control gap		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Vendor may accidentally or maliciously make changes to the IT system – Allow view-only access. With view-only access, the third party can view the desktop but cannot interact with it. In other words, they cannot control the keyboard or mouse to make any changes.

Desktop sharing traffic may be intercepted by network attackers – Use SSL for remote sessions. SSL (Secure Sockets Layer) encrypts data in transit between computers. If an attacker intercepted the traffic, the data would be encrypted and therefore unreadable to the attacker.

No guarantees that shoulder surfing attacks are not occurring at the vendor – Identified control gap. Shoulder surfing is where someone else gains information by looking at your computer screen. This should be identified as a risk. A control gap occurs when there are either insufficient or no actions taken to avoid or mitigate a significant risk.

Vendor may inadvertently see confidential material from the company such as email and IMs – Limit desktop session to certain windows.

The easiest way to prevent a third party from viewing your emails and IMs is to close the email and IM application windows for the duration of the desktop sharing session.

NEW QUESTION 142

An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

- A. Review switch and router configurations
- B. Review the security policies and standards
- C. Perform a network penetration test
- D. Review the firewall rule set and IPS logs

Answer: B

Explanation:

IT security professionals should have a chance to review the security controls and practices of a company targeted for acquisition. Any irregularities that are found should be reported to management so that expenses and concerns are properly identified.

Incorrect Answers:

A: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing switch and router configurations are not part of this process. C: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Performing a network penetration test is not part of this process.

D: Due diligence entails ensuring controls implemented by an organization continues to provide the required level of protection. Reviewing the firewall rule set and IPS logs are not part of this process. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 270, 332

NEW QUESTION 146

A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

- A. Memorandum of Agreement
- B. Interconnection Security Agreement
- C. Non-Disclosure Agreement
- D. Operating Level Agreement

Answer: B

Explanation:

The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

Incorrect Answers:

A: A memorandum of agreement (MOA) is a document composed between parties to cooperate on an agreed upon project or meet an agreed objective.

C: A nondisclosure agreement (NDA) is designed to protect confidential information.

D: An operating level agreement (OLA) defines the responsibilities of each partner's internal support group.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 237, 238

NEW QUESTION 147

An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

- A. Independent verification and validation
- B. Security test and evaluation
- C. Risk assessment
- D. Ongoing authorization

Answer: D

Explanation:

Ongoing assessment and authorization is often referred to as continuous monitoring. It is a process that determines whether the set of deployed security controls in an information system continue to be effective with regards to planned and unplanned changes that occur in the system and its environment over time.

Continuous monitoring allows organizations to evaluate the operating effectiveness of controls on or near a real-time basis. Continuous monitoring enables the enterprise to detect control failures quickly because it transpires immediately or closely after events in which the key controls are utilized.

Incorrect Answers:

A: Independent verification and validation (IV&V) is executed by a third party organization not involved in the development of a product. This is not considered continuous monitoring of authorized information systems.

B: Security test and evaluation is not considered continuous monitoring of authorized information systems.

C: Risk assessment is the identification of potential risks and threats. It is not considered continuous monitoring of authorized information systems.

References:

<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring>
<http://www.fedramp.net/ongoing-assessment-and-authorization-continuous-monitoring>
<https://www.techopedia.com/definition/24836/independent-verification-and-validation>
<https://www.techopedia.com/definition/24836/independent-verification-and-validation>
<https://www.techopedia.com/definition/24836/independent-verification-and-validation>
<https://www.techopedia.com/definition/24836/independent-verification-and-validation>
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 213, 219

NEW QUESTION 151

A firm's Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product's reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO's requirements?

- A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.
- B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.
- C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.
- D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Answer: C

Explanation:

Gray box testing has limited knowledge of the system as an attacker would. The base code would remain confidential. This would further be enhanced by a Non-disclosure agreement (NDA) which is designed to protect confidential information.

Incorrect Answers:

- A: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. They do not typically cover vulnerabilities and penetration / vulnerability testing. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.
- B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities. Black box testing is integrity-based testing that uses random user inputs. Code confidentiality is maintained but testing is limited.
- D: White box testing requires full access to the code base as it involves validating the program logic. This does not test against vulnerabilities. Furthermore, the CEO is concerned that IT staff lacks the knowledge to identify complex vulnerabilities.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 148, 167-168, 238-239
https://en.wikipedia.org/wiki/Non-disclosure_agreement
https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION 156

Company policy requires that all company laptops meet the following baseline requirements: Software requirements:

- Antivirus
- Anti-malware
- Anti-spyware
- Log monitoring
- Full-disk encryption
- Terminal services enabled for RDP
- Administrative access for local users
- Hardware restrictions:
 - Bluetooth disabled
 - FireWire disabled
 - WiFi adapter disabled

Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

- A. Group policy to limit web access
- B. Restrict VPN access for all mobile users
- C. Remove full-disk encryption
- D. Remove administrative access to local users
- E. Restrict/disable TELNET access to network resources
- F. Perform vulnerability scanning on a daily basis
- G. Restrict/disable USB access

Answer: DG

Explanation:

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software. A bootkit is similar to a rootkit except the malware infects the master boot record on a hard disk. Malicious software such as bootkits or rootkits typically require administrative privileges to be installed.

Therefore, one method of preventing such attacks is to remove administrative access for local users. A common source of malware infections is portable USB flash drives. The flash drives are often plugged into less secure computers such as a user's home computer and then taken to work and plugged in to a work computer. We can prevent this from happening by restricting or disabling access to USB devices.

Incorrect Answers:

- A: Using a group policy to limit web access is not a practical solution. Users in a company often require Web access so restricting it will affect their ability to do their jobs.
- B: Rootkits or Bootkits would not be caught by connecting to the network over a VPN so disabling VPN access will not help.
- C: Removing full-disk encryption will not prevent Bootkits.
- E: Bootkits are not caught by connecting to network resources using Telnet connection so disabling Telnet access to resources will not help.
- F: Performing vulnerability scanning on a daily basis might help you to quickly detect Bootkits. However, vulnerability scanning does nothing to actually prevent the Bootkits.

References: <https://en.wikipedia.org/wiki/Rootkit>

NEW QUESTION 159

A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

- A. Isolate the system on a secure network to limit its contact with other systems
- B. Implement an application layer firewall to protect the payroll system interface
- C. Monitor the system's security log for unauthorized access to the payroll application
- D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

Explanation:

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the payroll system and limit any damage to other systems if the payroll system is attacked.

Incorrect Answers:

B: An application layer firewall may provide some protection to the application. However, the operating system is vulnerable due to being unpatched. It is unlikely that an application layer firewall will protect against the operating system vulnerabilities.

C: Monitoring the system's security log for unauthorized access to the payroll application will not actually provide any protection against unauthorized access. It would just enable you to see that unauthorized access has occurred.

D: Reconciling the payroll transactions on a daily basis would keep the accounts up to date but it would provide no protection for the system and so does not mitigate the vulnerability of missing OS patches as required in this question.

NEW QUESTION 160

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 162

A web services company is planning a one-time high-profile event to be hosted on the corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

- A. Ensure web services hosting the event use TCP cookies and deny_hosts.
- B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.
- C. Contract and configure scrubbing services with third-party DDoS mitigation providers.
- D. Purchase additional bandwidth from the company's Internet service provide

Answer: C

Explanation:

Scrubbing is an excellent way of dealing with this type of situation where the company wants to stay connected no matter what during the one-time high profile event. It involves deploying a multi-layered security approach backed by extensive threat research to defend against a variety of attacks with a guarantee of always-on.

Incorrect Answers:

A: Making use of TCP cookies will not be helpful in this event since cookies are used to maintain selections on previous pages and attackers can assess cookies in transit or in storage to carry out their attacks.

B: Using intrusion prevention systems blocking IPs is contra productive for a one-time high profile event if you want to attract and reach many clients and the same time.

D: Purchasing additional bandwidth from the ISP not going to prevent attackers from hi-jacking your one-time event.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 159, 165, 168
<http://www.level3.com/en/products/ddos-mitigation/>

NEW QUESTION 163

The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social medi

- A. Which of the following decisions is BEST for the CEO to make?
- B. Social media is an effective solution because it is easily adaptable to new situations.
- C. Social media is an ineffective solution because the policy may not align with the business.
- D. Social media is an effective solution because it implements SSL encryption.
- E. Social media is an ineffective solution because it is not primarily intended for business applications.

Answer: B

Explanation:

Social media networks are designed to draw people's attention quickly and to connect people is thus the main focus; security is not the main concern. Thus the CEO should decide that it would be ineffective to use social media in the company as it does not align with the company business. Incorrect Answers:

A: Social media is not designed to be easily adaptable to new situations in a workplace.

C: Social media does not necessarily make use of SSL encryption since it is designed to draw people's attention and connect them quickly.

D: Social media, though a great channel for communication is not intended for business applications. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 290-293

NEW QUESTION 166

A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

- A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
- B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
- C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
- D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A

Explanation:

A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.

Incorrect Answers:

B: Calling the regional Internet registry will not provide you with the correct information.

C: The telecom billing information will not have information as to whether the legacy backup may have Internet connections on the network.

D: DNS server queries are used to resolve the name with each query message containing a DNS domain name, a specified query type and a specified class. This is not what the security consultant requires.

References:

[https://technet.microsoft.com/en-us/HYPERLINK \"https://technet.microsoft.com/enus/ library/cc958823.aspx\"library/cc958823.aspx](https://technet.microsoft.com/en-us/HYPERLINK \)

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 60-66

NEW QUESTION 171

A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

- A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
- B. Interview employees and managers to discover the industry hot topics and trends
- C. Attend meetings with staff, internal training, and become certified in software management
- D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Answer: D

Explanation:

Conferences represent an important method of exchanging information between researchers who are usually experts in their respective fields. Together with webinars and training to remain current on the subject the manager will be able to gain valuable insight into the cyber defense industry and be able to recruit personnel.

Incorrect Answers:

A: Merely interviewing candidates and hiring a staffing company will not provide the human resources manager with the necessary insight into a new cyber defense division for the company. B: Interviewing the employees and managers to pick up on hot, new trends is not the best possible way to gain the appropriate insight.

C: It is not guaranteed that the existing staff would be on top of new developments that would make them in tune with the new division that is being envisaged by the company. It would be best to gain insight from more knowledgeable sources such as conferences, etc.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 293

NEW QUESTION 172

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:

Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0

Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0

Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0

All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a

A packet capture shows the following:

09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)

09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1, length 65534
09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2, length 65534
09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3, length 65534
Which of the following is occurring on the network?

- A. A man-in-the-middle attack is underway on the network.
- B. An ARP flood attack is targeting at the router.
- C. The default gateway is being spoofed on the network.
- D. A denial of service attack is targeting at the route

Answer: D

Explanation:

The above packet capture shows an attack where the attacker is busy consuming your resources (in this case the router) and preventing normal use. This is thus a Denial Of Service Attack.

Incorrect Answers:

A: A man-in-the-middle attack is when an attacker intercepts and perhaps changes the data that is transmitted between two users. The packet capture is not indicative of a man-in-the-middle attack. B: With an ARP flood attack thousands of spoofed data packets with different physical addresses are sent to a device. This is not the case here.

C: A gateway being spoofed show up as any random number that the attacker feels like listing as the caller. This is not what is exhibited in this case.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 286

NEW QUESTION 173

Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.

```
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
```

```
ether f8:1e:af:ab:10:a3
```

```
inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5 inet 192.168.1.14 netmask 0xfffff00 broadcast 192.168.1.255 inet6
```

```
2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf
```

```
inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary nd6 options=1<PERFORMNUD>
```

```
media: autoselect status: active
```

Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

- A. The devices use EUI-64 format
- B. The routers implement NDP
- C. The network implements 6to4 tunneling
- D. The router IPv6 advertisement has been disabled
- E. The administrator must disable IPv6 tunneling
- F. The administrator must disable the mobile IPv6 router flag
- G. The administrator must disable the IPv6 privacy extensions
- H. The administrator must disable DHCPv6 option code 1

Answer: BG

Explanation:

IPv6 makes use of the Neighbor Discovery Protocol (NDP). Thus if your routers implement NDP you will be able to map users with IPv6 addresses. However to be able to positively map users with IPv6 addresses you will need to disable IPv6 privacy extensions.

Incorrect Answers:

A: Devices making use of the EUI-64 format means that the last 64 bits of IPv6 unicast addresses are used for interface identifiers. This is not shown in the exhibit above.

C: 6to4 tunneling is used to connect IPv6 hosts or networks to each other over an IPv4 backbone. This type of tunneling is not going to ensure positive future mapping of users on the network. Besides 6to4 does not require configured tunnels because it can be implemented in border routers without a great deals of router configuration.

D: The exhibit is not displaying that the router IPv6 has been disabled. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags. Several protocols have reserved flags in this field and others are preparing to reserve a sufficient number of flags to exhaust the field.

E: Disabling the tunneling of IPv6 does not ensure positive future IPv6 addressing.

F: The IPv6 router flag is used to maintain reachability information about paths to active neighbors, thus it should not be disabled if you want to ensure positive mapping of users in future.

H: DHCPv6 is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration data that is necessary to function properly in an IPv6 network. This should not be disabled.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 49

[http://www.HYPERLINK \"http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm\".HYPERLINK](http://www.HYPERLINK \)

[\"http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm\"tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm](http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm\)

NEW QUESTION 177

A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.

Proposal:

External cloud-based software as a service subscription costing \$5,000 per month. Expected to reduce the number of current incidents per annum by 50%.

The company currently has ten security incidents per annum at an average cost of \$10,000 per incident. Which of the following is the ROI for this proposal after three years?

- A. -\$30,000
- B. \$120,000
- C. \$150,000
- D. \$180,000

Answer: A

Explanation:

Return on investment = Net profit / Investment where: Net profit = gross profit - expenses.

or

Return on investment = (gain from investment – cost of investment) / cost of investment Subscriptions = 5,000 x 12 = 60,000 per annum

10 incidents @ 10,000 = 100,000 per annum reduce by 50% = 50,000 per annum

Thus the rate of Return is -10,000 per annum and that makes for -\$30,000 after three years. References:

<http://www.finHYPERLINK> "http://www.financeformulas.net/Return_on_Investment.html"[anceformulas.net/Return_on_Investment.html](http://www.financeformulas.net/Return_on_Investment.html)

NEW QUESTION 180

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

- A. Establish the security control baseline
- B. Build the application according to software development security standards
- C. Review the results of user acceptance testing
- D. Consult with the stakeholders to determine which standards can be omitted

Answer: A

Explanation:

A security baseline is the minimum level of security that a system, network, or device must adhere to. It is the initial point of reference for security and the document against which assessments would be done.

Incorrect Answers:

B: Building the application with secure coding is the programmers' duty. C: User acceptance testing is part of the development process

D: Standards are not security concerns. References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 272-273

NEW QUESTION 183

An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

- A. Guest users could present a risk to the integrity of the company's information.
- B. Authenticated users could sponsor guest access that was previously approved by management.
- C. Unauthenticated users could present a risk to the confidentiality of the company's information.
- D. Meeting owners could sponsor guest access if they have passed a background check

Answer: C

Explanation:

The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with unauthorized users.

Incorrect Answers:

A: Integrity of information is centered on the modification or alternation of information. Information remains unchanged and is in its true original form during transmission and storage. The issue of guests at a Web conference is related to confidentiality of information.

B: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests.

D: The issue at stake in this question is confidentiality of information. Topics covered during the web conference are considered proprietary and should remain confidential, which means it should not be shared with guests, whether they have passed background checks or not.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 3

NEW QUESTION 186

Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

Sales is asking for easy order tracking to facilitate feedback to customers.

Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.

Which of the following departments' request is in contrast to the favored solution?

- A. Manufacturing
- B. Legal
- C. Sales
- D. Quality assurance
- E. Human resources

Answer: E

Explanation:

The human resources department wanted complete access to employee data stored in the application, and an automated data interchange with their cloud-based SaaS employee management application. However, the favored solution provides read-only access and is hosted onsite. Incorrect Answers:

A: The manufacturing department wanted a quick and easy user friendly system. The favored solution is a user friendly software application that would meet the manufacturing department's requests.

B: The legal department wanted a system that provides adequate safeguards to protect trade secrets and was concerned with data ownership and legal jurisdiction. The favored solution is a user friendly software application that would be hosted onsite. This would address the legal department's concerns with data ownership and legal jurisdiction. The application also provides data encryption, which would protect trade secrets.

C: The sales department wanted an easy order tracking to facilitate feedback to customers. The favored solution is a user friendly software application that supports custom fields, which could be used for order tracking.

D: The quality assurance department was concerned about managing the end product and tracking overall performance. They also wanted read-only access to the entire workflow process for monitoring and baselining. These are met by the favored solution.

NEW QUESTION 191

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 192

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 197

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 been 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 data.

A. This can be accomplished through 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 201

A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

- A. Spiral model
- B. Incremental model
- C. Waterfall model
- D. Agile model

Answer: C

Explanation:

The waterfall model is a sequential software development process, in which progress is seen as flowing steadily downwards through identified phases.

Incorrect Answers:

A: The spiral model is a risk-driven process model generator for software projects. Based on the unique risk patterns of a given project, the spiral model guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.

B: The incremental model is used to develop a system through repeated cycles (iterative) and in smaller portions at a time (incremental), allowing software developers to take advantage of what was learned during development of earlier parts or versions of the system. Learning comes from both the development and use of the system, where possible key steps in the process start with a simple implementation of a subset of the software requirements and iteratively enhance the evolving versions until the full system is implemented. At each iteration, design modifications are made and new functional capabilities are added.

D: In the agile software development model, teams of programmers and business experts work closely together, using an iterative approach.

References: https://en.wikipedia.org/wiki/Waterfall_model

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

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

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

BOOK p. 371

NEW QUESTION 204

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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](#)