CAS-003

Number: CAS-003
Passing Score: 800
Time Limit: 120 min
File Version: 1

CAS-003

Exam A

QUESTION 1
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 2
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues
B. Posing as a copier service technician and indicating the equipment had “phoned home” to alert the technician for a service call
C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed
D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication
Network Server: Digitally sign communication

A storage administrator in a remote location with a legacy storage array, which contains time-sensitive data, reports employees can no longer connect to their department shares. Which of the following mitigation strategies should an information security manager recommend to the data owner?

A. Accept the risk, reverse the settings for the remote location, and have the remote location file a risk exception until the legacy storage device can be upgraded
B. Accept the risk for the remote location, and reverse the settings indefinitely since the legacy storage device will not be upgraded
C. Mitigate the risk for the remote location by suggesting a move to a cloud service provider. Have the remote location request an indefinite risk exception for the use of cloud storage
D. Avoid the risk, leave the settings alone, and decommission the legacy storage device

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

A. Blue team
B. Red team
C. Black box
D. White team

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref

QUESTION 7
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.

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

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

A. High confidentiality, high availability

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 8
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A security incident responder discovers an attacker has gained access to a network and has overwritten key system files with backdoor software. The server was reimaged and patched offline. Which of the following tools should be implemented to detect similar attacks?

A. Vulnerability scanner
B. TPM

C. Host-based firewall
D. File integrity monitor
E. NIPS

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 10
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

A. Identify a third-party source for IDS rules and change the configuration on the applicable IDSs to pull in the new rulesets
B. Encourage cybersecurity analysts to review open-source intelligence products and threat database to generate new IDS rules based on those sources
C. Leverage the latest TCP- and UDP-related RFCs to arm sensors and IDSs with appropriate heuristics for anomaly detection
D. Use annual hacking conventions to document the latest attacks and threats, and then develop IDS rules to counter those threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Following a security assessment, the Chief Information Security Officer (CISO) is reviewing the results of the assessment and evaluating potential risk treatment strategies. As part of the CISO's evaluation, a judgment of potential impact based on the identified risk is performed. To prioritize response actions, the CISO uses past experience to take into account the exposure factor as well as the external accessibility of the weakness identified. Which of the following is the CISO performing?

A. Documentation of lessons learned
B. Quantitative risk assessment
C. Qualitative assessment of risk
D. Business impact scoring
E. Threat modeling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
QUESTION 14
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.
- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

Which of the following need specific attention to meet the requirements listed above? (Choose three.)

A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
The board of a financial services company has requested that the senior security analyst acts as a cybersecurity advisor in order to comply with recent federal legislation. The analyst is required to give a report on current cybersecurity and threat trends in the financial services industry at the next board meeting. Which of the following would be the BEST methods to prepare this report? (Choose two.)

A. Review the CVE database for critical exploits over the past year
B. Use social media to contact industry analysts
C. Use intelligence gathered from the Internet relay chat channels
D. Request information from security vendors and government agencies
E. Perform a penetration test of the competitor's network and share the results with the board

Correct Answer: AD
Section: (none)
Explanation
Explanation/Reference:

QUESTION 16
A security consultant is attempting to discover if the company is utilizing databases on client machines to store the customer data. The consultant reviews the following information:

```
Protocol   Local Address     Foreign Address       Status
TCP        127.0.0.1         172.16.10.101:25      Connection established
TCP        127.0.0.1         172.16.20.45:443      Connection established
UDP        127.0.0.1         172.16.20.80:53       Waiting listening
TCP        172.16.10.10:1433 172.16.10.34          Connection established
```

Which of the following commands would have provided this output?

A. `arp -s`
B. `netstat -a`
C. `ifconfig -arp`
D. `sqlmap -w`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Management is reviewing the results of a recent risk assessment of the organization's policies and procedures. During the risk assessment it is determined that procedures associated with background checks have not been effectively implemented. In response to this risk, the organization elects to revise policies and procedures related to background checks and use a third-party to perform background checks on all new employees. Which of the following risk management strategies has the organization employed?

A. Transfer
B. Mitigate
C. Accept
D. Avoid
E. Reject

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A security engineer must establish a method to assess compliance with company security policies as they apply to the unique configuration of individual endpoints, as well as to the shared configuration policies of common devices.

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

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

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 19
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 FDED. The device is rooted

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

A. SPF
B. S/MIME
C. TLS
D. DKIM

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/DMARC

QUESTION 21
An organization is preparing to develop a business continuity plan. The organization is required to meet regulatory requirements relating to confidentiality and availability, which are well-defined. Management has expressed concern following initial meetings that the organization is not fully aware of the requirements associated with the regulations. Which of the following would be MOST appropriate for the project manager to solicit additional resources for during this phase of the project?

A. After-action reports
B. Gap assessment
C. Security requirements traceability matrix
D. Business impact assessment
E. Risk analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 23
An agency has implemented a data retention policy that requires tagging data according to type before storing it in the data repository. The policy requires all business emails be automatically deleted after two years. During an open records investigation, information was found on an employee's work computer concerning a conversation that occurred three years prior and proved damaging to the agency's reputation. Which of the following MOST likely caused the data leak?

A. The employee manually changed the email client retention settings to prevent deletion of emails
B. The file that contained the damaging information was mistagged and retained on the server for longer than it should have been
C. The email was encrypted and an exception was put in place via the data classification application
D. The employee saved a file on the computer's hard drive that contained archives of emails, which were more than two years old

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 require S/MIME with AES-256.
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following BEST represents a risk associated with merging two enterprises during an acquisition?

A. The consolidation of two different IT enterprises increases the likelihood of the data loss because there are now two backup systems

B. Integrating two different IT systems might result in a successful data breach if threat intelligence is not shared between the two enterprises
C. Merging two enterprise networks could result in an expanded attack surface and could cause outages if trust and permission issues are not handled carefully
D. Expanding the set of data owners requires an in-depth review of all data classification decisions, impacting availability during the review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN
C. Configure all management traffic to be tunneled into the enterprise via TLS

D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: "`<object object_ref=… />`" and "`<state state_ref=… />`". Which of the following tools BEST supports the use of these definitions?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A deployment manager is working with a software development group to assess the security of a new version of the organization's internally developed ERP tool. The organization prefers to not perform assessment activities following deployment, instead focusing on assessing security throughout the life cycle. Which of the following methods would BEST assess the security of the product?

A. Static code analysis in the IDE environment
B. Penetration testing of the UAT environment
C. Vulnerability scanning of the production environment
D. Penetration testing of the production environment
E. Peer review prior to unit testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.computer-forensics-recruiter.com/order-of-volatility/

QUESTION 32
A company wants to extend its help desk availability beyond business hours. The Chief Information Officer (CIO) decides to augment the help desk with a thirdparty service that will answer calls and provide Tier 1 problem resolution, such as password resets and remote assistance. The security administrator implements the following firewall change:

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800

PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

The administrator provides the appropriate path and credentials to the third-party company. Which of the following technologies is MOST likely being used to provide access to the third company?

A. LDAP
B. WAYF
C. OpenID
D. RADIUS
E. SAML

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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

Correct Answer: BEH

Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

A. Use a protocol analyzer against the site to see if data input can be replayed from the browser
B. Scan the website through an interception proxy and identify areas for the code injection
C. Scan the site with a port scanner to identify vulnerable services running on the web server
D. Use network enumeration tools to identify if the server is running behind a load balancer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data?

A. Data aggregation
B. Data sovereignty
C. Data isolation
D. Data volume
E. Data analytics

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.

Which of the following methods could be used in addition to an integrated development environment to reduce the severity of the issue?

A. Conduct a penetration test on each function as it is developed
B. Develop a set of basic checks for common coding errors
C. Adopt a waterfall method of software development
D. Implement unit tests that incorporate static code analyzers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Given the code snippet below:

```
#include <stdio.h>
#include <stdlib.h>
int main(void) {
  char username[8];
  printf("Enter your username: ");
  gets(username)
  printf("\n";
  if (username == NULL) {
    printf("you did not enter a username\n");
  }
  it strcmp(username, "admin") {
   printf("%s", "Admin user, enter your physical token value: ");
  // rest of conditional logic here has been snipped for brevity
  } else [
  printf("Standard user, enter your password: ");
  // rest of conditional logic here has been snipped for brevity
  }
}
```


Which of the following vulnerability types in the MOST concerning?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
To meet an SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

A. BPA
B. OLA
C. MSA
D. MOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

QUESTION 39
An organization has established the following controls matrix:

	Minimum	Moderate	High
Physical Security	Cylinder Lock	Cipher Lock	Proximity Access Card
Environmental Security	Surge Protector	UPS	Generator
Data Security	Context-Based Authentication	MFA	FDE
Application Security	Peer Review	Static Analysis	Penetration Testing
Logical Security	HIDS	NIDS	NIPS

The following control sets have been defined by the organization and are applied in aggregate fashion:

- Systems containing PII are protected with the minimum control set.
- Systems containing medical data are protected at the moderate level.
- Systems containing cardholder data are protected at the high level.

The organization is preparing to deploy a system that protects the confidentially of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

A. Proximity card access to the server room, context-based authentication, UPS, and full-disk encryption for the database server.
B. Cipher lock on the server room door, FDE, surge protector, and static analysis of all application code.
C. Peer review of all application changes, static analysis of application code, UPS, and penetration testing of the complete system.
D. Intrusion detection capabilities, network-based IPS, generator, and context-based authentication.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

Which of the following MOST likely need to be configured to ensure the system are mitigated accordingly? (Choose two.)

A. Antivirus
B. HIPS
C. Application whitelisting
D. Patch management
E. Group policy implementation
F. Firmware updates

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42

A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.
If the engineer wants to help ensure some resilience against zero-day vulnerabilities exploited against the VPN implementation, which of the following decisions would BEST support this objective?

A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.
C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloudbased log aggregation solution for all traffic that is logged.

Which of the following presents a long-term risk to user privacy in this scenario?

A. Confidential or sensitive documents are inspected by the firewall before being logged.
B. Latency when viewing videos and other online content may increase.
C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.
D. Stored logs may contain non-encrypted usernames and passwords for personal websites.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators.
Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources.

Which of the following should the analyst use to remediate the vulnerabilities?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points.

Which of the following solutions BEST meets the engineer's goal?

A. Schedule weekly reviews of al unit test results with the entire development team and follow up between meetings with surprise code inspections.
B. Develop and implement a set of automated security tests to be installed on each development team leader's workstation.
C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.
D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Given the following information about a company's internal network:

User IP space: 192.168.1.0/24
Server IP space: 192.168.192.0/25

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

Which of the following should the engineer do?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

During a security assessment, activities were divided into two phases: internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.
Which of the following methods is the assessment team most likely to employ NEXT?

A. Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices.
B. Conducting a social engineering attack attempt with the goal of accessing the compromised box physically.
C. Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
D. Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
An organization's network engineering team recently deployed a new software encryption solution to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data read-write requests in storage, impacting business operations.

Which of the following alternative approaches would BEST address performance requirements while meeting the intended security objective?

A. Employ hardware FDE or SED solutions.
B. Utilize a more efficient cryptographic hash function.
C. Replace HDDs with SSD arrays.
D. Use a FIFO pipe a multithreaded software solution.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Given the following code snippet:

```
SecCond = "1SS"
SecStatus = false
try (
if (SecStatus)
            SecCond = "2SS"
            console.log("ship to ship")
else
        SecCond = "normal operations"
        console.log("nothing to see here")
} catch (e) {
SecCond = "normal operations"
 console.log(e)
 console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit?

A. Open
B. Secure
C. Halt
D. Exception

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

- Involve business owners and stakeholders
- Create an applicable scenario
- Conduct a biannual verbal review of the incident response plan
- Report on the lessons learned and gaps identified

Which of the following exercises has the CEO requested?

A. Parallel operations
B. Full transition
C. Internal review
D. Tabletop
E. Partial simulation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 56

A security researcher is gathering information about a recent spoke 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. Hacktivists seeking to make a political statement because of socio-economic factors.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.

After network enumeration, the analyst's NEXT step is to perform:

A. a gray-box penetration test
B. a risk analysis
C. a vulnerability assessment
D. an external security audit
E. a red team exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58

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

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: non-sensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive.

Which of the following actions should the engineer take regarding the data?

A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlled.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60

The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues.

Which of the following is the MOST important information to reference in the letter?

A. After-action reports from prior incidents.
B. Social engineering techniques
C. Company policies and employee NDAs
D. Data classification processes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization's systems to the greatest extent possible.

Which of the following principles is being demonstrated?

A. Administrator accountability
B. PII security
C. Record transparency
D. Data minimization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

Which of the following tools would show this type of output?

A. Log analysis tool
B. Password cracker
C. Command-line tool
D. File integrity monitoring tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

Configuration file 1:
```
Operator ALL=/sbin/reboot
```
Configuration file 2:
```
Command="/sbin/shutdown now", no-x11-forwarding, no-pty, ssh-dss
```
Configuration file 3:
Operator:x:1000:1000::/home/operator:/bin/bash

Which of the following explains why an intended operator cannot perform the intended action?

A. The sudoers file is locked down to an incorrect command
B. SSH command shell restrictions are misconfigured
C. The passwd file is misconfigured
D. The SSH command is not allowing a pty session

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
QUESTION 64
The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code.

Which of the following is an SDLC best practice that should have been followed?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

A. Following new requirements that result from contractual obligations
B. Answering requests from auditors that relate to e-discovery
C. Responding to changes in regulatory requirements
D. Developing organizational policies that relate to hiring and termination procedures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Company.org has requested a black-box security assessment be performed on key cyber terrain. One area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing.
Which of the following commands should the assessor use to determine this information?

A. `dnsrecon -d company.org -t SOA`
B. `dig company.org mx`
C. `nc -v company.org`
D. `whois company.org`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

	Date	Subject	Message
1	5/12/2017	Change of room	Patient John Doe is now in room 201
2	5/12/2017	Prescription change	Ann Smith – add 5mg
3	5/13/2017	Appointment cancelled	John Doe cancelled
4	5/14/2017	Follow-up visit	Ann Smith scheduled a follow-up
5	5/20/2017	Emergency room	Ann Doe – patient #37125 critical
6	5/25/2017	Prescription overdose	John Smith – patient #25637 in room 37

Which of the following represents the BEST solution for preventing future fines?

A. Implement a secure text-messaging application for mobile devices and workstations.
B. Write a policy requiring this information to be given over the phone only.
C. Provide a courier service to deliver sealed documents containing public health informatics.
D. Implement FTP services between clinics to transmit text documents with the information.
E. Implement a system that will tokenize patient numbers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:

- Encrypt all traffic between the network engineer and critical devices.
- Segregate the different networking planes as much as possible.

Do not let access ports impact configuration tasks.

Which of the following would be the BEST recommendation for the network security engineer to present?

A. Deploy control plane protections.
B. Use SSH over out-of-band management.
C. Force only TACACS to be allowed.
D. Require the use of certificates for AAA.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the frontend user registration web form accepts invalid input in the user's age field. The developer was notified and asked to fix the issue.

Which of the following is the MOST secure solution for the developer to implement?

A. `IF $AGE == "!@#$%^&*()_+<>?":{}[]" THEN ERROR`
B. `IF $AGE == [1234567890] {1,3} THEN CONTINUE`
C. `IF $AGE != "a-bA-Z!@#$%^&*()_+<>?":{}[]" THEN CONTINUE`
D. `IF $AGE == [1-0] {0,2} THEN CONTINUE`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70

At a meeting, the systems administrator states the security controls a company wishes to implement seem excessive, since all of the information on the company's web servers can be obtained publicly and is not proprietary in any way. The next day the company's website is defaced as part of an SQL injection attack, and the company receives press inquiries about the message the attackers displayed on the website.

Which of the following is the FIRST action the company should take?

A. Refer to and follow procedures from the company's incident response plan.
B. Call a press conference to explain that the company has been hacked.
C. Establish chain of custody for all systems to which the systems administrator has access.
D. Conduct a detailed forensic analysis of the compromised system.
E. Inform the communications and marketing department of the attack details.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
As a result of an acquisition, a new development team is being integrated into the company. The development team has BYOD laptops with IDEs installed, build servers, and code repositories that utilize SaaS. To have the team up and running effectively, a separate Internet connection has been procured.
A stand up has identified the following additional requirements:

1. Reuse of the existing network infrastructure
2. Acceptable use policies to be enforced
3. Protection of sensitive files
4. Access to the corporate applications

Which of the following solution components should be deployed to BEST meet the requirements? (Choose three.)

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC

G. WAF
H. Load balancer

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

Which of the following solutions BEST meets all of the architect's objectives?

A. An internal key infrastructure that allows users to digitally sign transaction logs
B. An agreement with an entropy-as-a-service provider to increase the amount of randomness in generated keys.
C. A publicly verified hashing algorithm that allows revalidation of message integrity at a future date.
D. An open distributed transaction ledger that requires proof of work to append entries.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES-256-GCM on VPNs between sites.

Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.
B. Upgrade the cipher suite to use an authenticated AES mode of operation.
C. Use a stronger elliptic curve cryptography algorithm.

D. Implement an IDS with sensors inside (clear-text) and outside (cipher-text) of each tunnel between sites.
E. Ensure cryptography modules are kept up to date from vendor supplying them.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Given the following code snippet:

```
<FORM ACTION="http://192.168.51.10/cgi-bin/order.pl" method="post">
<input type=hidden name="price" value="199.99">
<input type=hidden name="prd_id" value="X190">
QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>
</FORM>
```


Of which of the following is this snippet an example?

A. Data execution prevention
B. Buffer overflow
C. Failure to use standard libraries
D. Improper filed usage
E. Input validation

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

A company has created a policy to allow employees to use their personally owned devices. The Chief Information Security Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices.

Which of the following security controls would BEST reduce the risk of exposure?

A. Disk encryption on the local drive
B. Group policy to enforce failed login lockout
C. Multifactor authentication
D. Implementation of email digital signatures

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

A. Distribute a NAC client and use the client to push the company's private key to all the new devices.
B. Distribute the device connection policy and a unique public/private key pair to each new employee's device.
C. Install a self-signed SSL certificate on the company's RADIUS server and distribute the certificate's public key to all new client devices.
D. Install an 802.1X supplicant on all new devices and let each device generate a self-signed certificate to use for network access.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 78
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

```
dd if=/dev/ram of=/tmp/mem/dmp
```

The analyst then reviews the associated output:

```
^34^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/bin/bash^21^03#45
```

However, the analyst is unable to find any evidence of the running shell.

Which of the following of the MOST likely reason the analyst cannot find a process ID for the shell?

A. The NX bit is enabled
B. The system uses ASLR
C. The shell is obfuscated
D. The code uses dynamic libraries

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back.

Which of the following BEST describes how the manager should respond?

A. Determine if the data still exists by inspecting to ascertain if the laptop has already been wiped and if the storage team has recent backups.
B. Inform Ann that the laptop was for company data only and she should not have stored personal photos on a company asset.
C. Report the email because it may have been a spoofed request coming from an attacker who is trying to exfiltrate data from the company laptop.
D. Consult with the legal and/or human resources department and check company policies around employment and termination procedures. **Correct Answer:** D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredder, and the waste will be burned. The system drives and removable media have been removed prior to ecycling the hardware.

Which of the following would ensure no data is recovered from the system drives once they are disposed of?

A. Overwriting all HDD blocks with an alternating series of data.
B. Physically disabling the HDDs by removing the drive head.
C. Demagnetizing the hard drive using a degausser.
D. Deleting the UEFI boot loaders from each HDD.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 82
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.

Which of the following is the MOST appropriate order of steps to be taken?

A. Firmware update, OS patching, HIDS, antivirus, baseline, monitoring agent
B. OS patching, baseline, HIDS, antivirus, monitoring agent, firmware update
C. Firmware update, OS patching, HIDS, antivirus, monitoring agent, baseline
D. Baseline, antivirus, OS patching, monitoring agent, HIDS, firmware update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

Which of the following BEST meets the needs of the board?

A. KRI:
- Compliance with regulations
- Backlog of unresolved security investigations
- Severity of threats and vulnerabilities reported by sensors - Time to patch critical issues on a monthly basis KPI:
- Time to resolve open security items
- % of suppliers with approved security control frameworks
- EDR coverage across the fleet
- Threat landscape rating

B. KRI:
- EDR coverage across the fleet
- Backlog of unresolved security investigations
- Time to patch critical issues on a monthly basis
- Threat landscape ratingKPI:
- Time to resolve open security items
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors

C. KRI:

- EDR coverage across the fleet
- % of suppliers with approved security control framework
- Backlog of unresolved security investigations- Threat landscape rating KPI:
- Time to resolve open security items
- Compliance with regulations
- Time to patch critical issues on a monthly basis
- Severity of threats and vulnerabilities reported by sensors

D. KPI:
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors - Threat landscape rating KRI:
- Time to resolve open security items
- Backlog of unresolved security investigations
- EDR coverage across the fleet
- Time to patch critical issues on a monthly basis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

Which of the following would be the MOST cost-effective solution to meet the company's needs?

A. Select one of the IT personnel to obtain information security training, and then develop all necessary policies and documents in-house.
B. Accept all risks associated with information security, and then bring up the issue again at next year's annual board meeting.
C. Release an RFP to consultancy firms, and then select the most appropriate consultant who can fulfill the requirements.
D. Hire an experienced, full-time information security team to run the startup company's information security department.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

A. the collection of data as part of the continuous monitoring program.
B. adherence to policies associated with incident response.
C. the organization's software development life cycle.
D. changes in operating systems or industry trends.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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 server . 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

An engineer needs to provide access to company resources for several offshore contractors. The contractors require:

- Access to a number of applications, including internal websites
- Access to database data and the ability to manipulate it
- The ability to log into Linux and Windows servers remotely

Which of the following remote access technologies are the BEST choices to provide all of this access securely? (Choose two.)

A. VTC
B. VRRP
C. VLAN
D. VDI
E. VPN
F. Telnet

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 91
A consulting firm was hired to conduct assessment for a company. During the first stage, a penetration tester used a tool that provided the following output:

TCP 80 open

TCP 443 open
TCP 1434 filtered

The penetration tester then used a different tool to make the following requests:

GET / script/login.php?token=45$MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF

Which of the following tools did the penetration tester use?

A. Protocol analyzer
B. Port scanner
C. Fuzzer
D. Brute forcer
E. Log analyzer
F. HTTP interceptor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.

Which of the following procedures should the security responder apply to the situation? (Choose two.)

A. Contain the server.
B. Initiate a legal hold.
C. Perform a risk assessment.
D. Determine the data handling standard.
E. Disclose the breach to customers.
F. Perform an IOC sweep to determine the impact.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An organization, which handles large volumes of PII, allows mobile devices that can process, store, and transmit PII and other sensitive data to be issued to employees. Security assessors can demonstrate recovery and decryption of remnant sensitive data from device storage after MDM issues a successful wipe command. Assuming availability of the controls, which of the following would BEST protect against the loss of sensitive data in the future?

A. Implement a container that wraps PII data and stores keying material directly in the container's encrypted application space.
B. Use encryption keys for sensitive data stored in an eFuse-backed memory space that is blown during remote wipe.
C. Issue devices that employ a stronger algorithm for the authentication of sensitive data stored on them.
D. Procure devices that remove the bootloader binaries upon receipt of an MDM-issued remote wipe command.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A large company with a very complex IT environment is considering a move from an on-premises, internally managed proxy to a cloud-based proxy solution managed by an external vendor. The current proxy provides caching, content filtering, malware analysis, and URL categorization for all staff connected behind the proxy. Staff members connect directly to the Internet outside of the corporate network. The cloud-based version of the solution would provide content filtering, TLS decryption, malware analysis, and URL categorization. After migrating to the cloud solution, all internal proxies would be decommissioned. Which of the following would MOST likely change the company's risk profile?

A. 1. There would be a loss of internal intellectual knowledge regarding proxy configurations and application data flows.
   2. There would be a greater likelihood of Internet access outages due to lower resilience of cloud gateways.
   3. There would be data sovereignty concerns due to changes required in routing and proxy PAC files.
B. 1. The external vendor would have access to inbound and outbound gateway traffic.
   2. The service would provide some level of protection for staff working from home.
   3. Outages would be likely to occur for systems or applications with hard-coded proxy information.
C. 1. The loss of local caching would dramatically increase ISP charges and impact existing bandwidth.
   2. There would be a greater likelihood of Internet access outages due to lower resilience of cloud gateways.
   3. There would be a loss of internal intellectual knowledge regarding proxy configurations and application data flows.
D. 1. Outages would be likely to occur for systems or applications with hard-coded proxy information.
   2. The service would provide some level of protection for staff members working from home.
   3. Malware detection times would decrease due to third-party management of the service.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Choose two.)

A. Access control
B. Whitelisting
C. Signing
D. Validation
E. Boot attestation

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security analyst is reviewing the following company requirements prior to selecting the appropriate technical control configuration and parameter:

RTO: 2 days
RPO: 36 hours
MTTR: 24 hours
MTBF: 60 days

Which of the following solutions will address the RPO requirements?

A. Remote Syslog facility collecting real-time events
B. Server farm behind a load balancer delivering five-nines uptime
C. Backup solution that implements daily snapshots
D. Cloud environment distributed across geographic regions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98

A penetration test is being scoped for a set of web services with API endpoints. The APIs will be hosted on existing web application servers. Some of the new APIs will be available to unauthenticated users, but some will only be available to authenticated users. Which of the following tools or activities would the penetration tester MOST likely use or do during the engagement? (Choose two.)

A. Static code analyzer
B. Intercepting proxy
C. Port scanner
D. Reverse engineering
E. Reconnaissance gathering
F. User acceptance testing

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A recent overview of the network's security and storage applications reveals a large amount of data that needs to be isolated for security reasons. Below are the critical applications and devices configured on the network:

- Firewall
- Core switches
- RM server
- Virtual environment
- NAC solution

The security manager also wants data from all critical applications to be aggregated to correlate events from multiple sources. Which of the following must be configured in certain applications to help ensure data aggregation and data isolation are implemented on the critical applications and devices? (Choose two.)

A. Routing tables
B. Log forwarding
C. Data remanants
D. Port aggregation
E. NIC teaming
F. Zones

Correct Answer: BF
Section: (none)
Explanation
Explanation/Reference:

QUESTION 100
A security analyst who is concerned about sensitive data exfiltration reviews the following:

```
10:01:32. 384853 IP (tos 0x0, ttl 64, id 40587, offset 0, flags [DF], proto ICMP (1), length 1500
192.168.1.20 -> 100.61.100.2: ICMP echo reply, id 1592, seq 8, length 1500
```

Which of the following tools would allow the analyst to confirm if data exfiltration is occuring?

A. Port scanner
B. SCAP tool
C. File integrity monitor
D. Protocol analyzer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
As part of the development process for a new system, the organization plans to perform requirements analysis and risk assessment. The new system will replace a legacy system, which the organization has used to perform data analytics.

Which of the following is MOST likely to be part of the activities conducted by management during this phase of the project?

A. Static code analysis and peer review of all application code
B. Validation of expectations relating to system performance and security
C. Load testing the system to ensure response times is acceptable to stakeholders
D. Design reviews and user acceptance testing to ensure the system has been deployed properly
E. Regression testing to evaluate interoperability with the legacy system during the deployment

Correct Answer: B

Section: (none)
Explanation
Explanation/Reference:

QUESTION 102
During a criminal investigation, the prosecutor submitted the original hard drive from the suspect's computer as evidence. The defense objected during the trial proceedings, and the evidence was rejected. Which of the following practices should the prosecutor's forensics team have used to ensure the suspect's data would be admissible as evidence? (Select TWO.)

A. Follow chain of custody best practices
B. Create an identical image of the original hard drive, store the original securely, and then perform forensics only on the imaged drive.
C. Use forensics software on the original hard drive and present generated reports as evidence
D. Create a tape backup of the original hard drive and present the backup as evidence
E. Create an exact image of the original hard drive for forensics purposes, and then place the original back in service

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
An organization just merged with an organization in another legal jurisdiction and must improve its network security posture in ways that do not require additional resources to implement data isolation. One recommendation is to block communication between endpoint PCs. Which of the following would be the BEST solution?

A. Installing HIDS
B. Configuring a host-based firewall
C. Configuring EDR
D. Implementing network segmentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
After several industry competitors suffered data loss as a result of cyberattacks, the Chief Operating Officer (COO) of a company reached out to the information security manager to review the organization's security stance. As a result of the discussion, the COO wants the organization to meet the following criteria:

- Blocking of suspicious websites
- Prevention of attacks based on threat intelligence
- Reduction in spam
- Identity-based reporting to meet regulatory compliance
- Prevention of viruses based on signature
- Protect applications from web-based threats

Which of the following would be the BEST recommendation the information security manager could make?

A. Reconfigure existing IPS resources
B. Implement a WAF
C. Deploy a SIEM solution
D. Deploy a UTM solution
E. Implement an EDR platform

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
With which of the following departments should an engineer for a consulting firm coordinate when determining the control and reporting requirements for storage of sensitive, proprietary customer information?

A. Human resources
B. Financial
C. Sales
D. Legal counsel

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 106
A company wants to confirm sufficient executable space protection is in place for scenarios in which malware may be attempting buffer overflow attacks. Which of the following should the security engineer check?

A. NX/XN
B. ASLR
C. strcpy
D. ECC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

A. NDA
B. MOU
C. BIA
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

Developers are working on a new feature to add to a social media platform. The new feature involves users uploading pictures of what they are currently doing. The data privacy officer (DPO) is concerned about various types of abuse that might occur due to this new feature. The DPO states the new feature cannot be released without addressing the physical safety concerns of the platform's users.

Which of the following controls would BEST address the DPO's concerns?

A. Increasing blocking options available to the uploader
B. Adding a one-hour delay of all uploaded photos
C. Removing all metadata in the uploaded photo file
D. Not displaying to the public who uploaded the photo
E. Forcing TLS for all connections on the platform

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A Chief Information Security Officer (CISO) is reviewing the controls in place to support the organization's vulnerability management program. The CISO finds patching and vulnerability scanning policies and procedures are in place. However, the CISO is concerned the organization is siloed and is not maintaining awareness of new risks to the organization. The CISO determines systems administrators need to participate in industry security events. Which of the following is the CISO looking to improve?

A. Vendor diversification
B. System hardening standards
C. Bounty programs
D. Threat awareness
E. Vulnerability signatures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A technician is validating compliance with organizational policies. The user and machine accounts in the AD are not set to expire, which is non-compliant. Which of the following network tools would provide this type of information?

A. SIEM server
B. IDS appliance
C. SCAP scanner D. HTTP interceptor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A Chief Security Officer (CSO) is reviewing the organization's incident response report from a recent incident. The details of the event indicate:

1. A user received a phishing email that appeared to be a report from the organization's CRM tool.
2. The user attempted to access the CRM tool via a fraudulent web page but was unable to access the tool.
3. The user, unaware of the compromised account, did not report the incident and continued to use the CRM tool with the original credentials.
4. Several weeks later, the user reported anomalous activity within the CRM tool.
5. Following an investigation, it was determined the account was compromised and an attacker in another country has gained access to the CRM tool.
6. Following identification of corrupted data and successful recovery from the incident, a lessons learned activity was to be led by the CSO.

Which of the following would MOST likely have allowed the user to more quickly identify the unauthorized use of credentials by the attacker?

A. Security awareness training
B. Last login verification
C. Log correlation
D. Time-of-check controls
E. Time-of-use controls
F. WAYF-based authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
An organization's Chief Financial Officer (CFO) was the target of several different social engineering attacks recently. The CFO has subsequently worked closely with the Chief Information Security Officer (CISO) to increase awareness of what attacks may look like. An unexpected email arrives in the CFO's inbox from a familiar name with an attachment. Which of the following should the CISO task a security analyst with to determine whether or not the attachment is safe?

A. Place it in a malware sandbox.
B. Perform a code review of the attachment.
C. Conduct a memory dump of the CFO's PC.
D. Run a vulnerability scan on the email server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A Chief Information Security Officer (CISO) is reviewing technical documentation from various regional offices and notices some key differences between these groups. The CISO has not discovered any governance documentation. The CISO creates the following chart to visualize the differences among the networking used:

	Switch Vendor	Trunking Protocol	Minimum Cabling Requirement	Active Support
Group A	Vendor 1	802.1q	Cat 5E	YES
Group B	Vendor 1	ISL	Cat 5E	YES
Group C	Vendor 2	802.1q	Cat 5	NO
Group D	Vendor 2	802.1q	Cat 5	YES

Which of the following would be the CISO's MOST immediate concern?

A. There are open standards in use on the network.
B. Network engineers have ignored defacto standards.
C. Network engineers are not following SOPs.
D. The network has competing standards in use.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 114
A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

1. Long-lived sessions are required, as users do not log in very often.
2. The solution has multiple SPs, which include mobile and web applications.
3. A centralized IdP is utilized for all customer digital channels.
4. The applications provide different functionality types such as forums and customer portals.
5. The user experience needs to be the same across both mobile and web-based applications.

Which of the following would BEST improve security while meeting these requirements?

A. Social login to IdP, securely store the session cookies, and implement one-time passwords sent to the mobile device
B. Certificate-based authentication to IdP, securely store access tokens, and implement secure push notifications.
C. Username and password authentication to IdP, securely store refresh tokens, and implement context-aware authentication.
D. Username and password authentication to SP, securely store Java web tokens, and implement SMS OTPs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115

A security analyst, who is working in a Windows environment, has noticed a significant amount of IPv6 traffic originating from a client, even though IPv6 is not currently in use. The client is a stand-alone device, not connected to the AD that manages a series of SCADA devices used for manufacturing. Which of the following is the appropriate command to disable the client's IPv6 stack? A.

```
C:\>netsh ipsec static set policy name=MYIPPolicy /v Disable TCPIP6
```

B.

```
C:\>reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\IPV6" /v disallowRun /t
REG_DWORD /d "0000001" /f
```

C.

```
C:\>reg add HKLM\system\CurrentControlSet\services\TCPIP6\Parameters /v DisabledComponents
/t REG_DWORD /d 255 /f
```

D.

```
C:\>reg add 'HKLM\SYSTEM\CurrentControlSet\IPV6" /f /v fDenyIPV6Connections /t
```


Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A security administrator is troubleshooting RADIUS authentication issues from a newly implemented controller-based wireless deployment. The RADIUS server contains the following information in its logs:

```
A RADIUS message was received from the invalid RADIUS client IP address 10.35.55.10
```

Based on this information, the administrator reconfigures the RADIUS server, which results in the following log data:

```
An Access-Request was received from RADIUS client 10.35.55.10
with a Message-Authenticator attribute that is not valid
```

To correct this error message, the administrator makes an additional change to the RADIUS server. Which of the following did the administrator reconfigure on the

RADIUS server? (Choose two.)

A. Added the controller address as an authorized client
B. Registered the RADIUS server to the wireless controller
C. Corrected a mismatched shared secret
D. Renewed the expired client certificate
E. Reassigned the RADIUS policy to the controller
F. Modified the client authentication method

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 117
An organization is improving its web services to enable better customer engagement and self-service. The organization has a native mobile application and a rewards portal provided by a third party. The business wants to provide customers with the ability to log in once and have SSO between each of the applications. The integrity of the identity is important so it can be propagated through to back-end systems to maintain a consistent audit trail. Which of the following authentication and authorization types BEST meet the requirements? (Choose two.)

A. SAML
B. Social login
C. OpenID connect
D. XACML
E. SPML
F. OAuth

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
After the departure of a developer under unpleasant circumstances, the company is concerned about the security of the software to which the developer has access. Which of the following is the BEST way to ensure security of the code following the incident?

A. Hire an external red team to conduct black box testing
B. Conduct a peer review and cross reference the SRTM
C. Perform white-box testing on all impacted finished products
D. Perform regression testing and search for suspicious code

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A Chief Information Security Officer (CISO) requests the following external hosted services be scanned for malware, unsecured PII, and healthcare data:

- Corporate intranet site
- Online storage application
- Email and collaboration suite

Security policy also is updated to allow the security team to scan and detect any bulk downloads of corporate data from the company's intranet and online storage site. Which of the following is needed to comply with the corporate security policy and the CISO's request?

A. Port scanner
B. CASB
C. DLP agent
D. Application sandbox
E. SCAP scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Several recent ransomware outbreaks at a company have cost a significant amount of lost revenue. The security team needs to find a technical control mechanism that will meet the following requirements and aid in preventing these outbreaks:

- Stop malicious software that does not match a signature
- Report on instances of suspicious behavior
- Protect from previously unknown threats
- Augment existing security capabilities

Which of the following tools would BEST meet these requirements?

A. Host-based firewall
B. EDR
C. HIPS
D. Patch management

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 121
A security analyst is reviewing the following packet capture of communication between a host and a company's router:

```
1 192.168.1.10 -> 10.5.10.1 icmp echo request 33 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZ
2 10.5.10.1 -> 192.168.1.10 icmp echo reply 34 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZA%MDKF8
```

Which of the following actions should the security analyst take to remove this vulnerability?

A. Update the router code
B. Implement a router ACL
C. Disconnect the host from the network
D. Install the latest antivirus definitions
E. Deploy a network-based IPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
An information security manager conducted a gap analysis, which revealed a 75% implementation of security controls for high-risk vulnerabilities, 90% for medium vulnerabilities, and 10% for low-risk vulnerabilities. To create a road map to close the identified gaps, the assurance team reviewed the likelihood of exploitation of each vulnerability and the business impact of each associated control. To determine which controls to implement, which of the following is the MOST important to consider?

A. KPI
B. KRI
C. GRC
D. BIA

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 123
A legacy web application, which is being used by a hospital, cannot be upgraded for 12 months. A new vulnerability is found in the legacy application, and the networking team is tasked with mitigation. Middleware for mitigation will cost $100,000 per year. Which of the following must be calculated to determine ROI? (Choose two.)

A. ALE
B. RTO
C. MTBF
D. ARO
E. RPO

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A security engineer is assisting a developer with input validation, and they are studying the following code block:

```
string accountIdRegexp = "TODO, help!";
private static final Pattern accountIdPattern = Pattern.compile
("accountIdRegexp");
String accountId = request.getParameter("accountNumber");
if (!accountIdPattern.matcher(accountId).matches() {
     System.out.println("account ID format incorrect");
} else {
     // continue
}
```

The security engineer wants to ensure strong input validation is in place for customer-provided account identifiers. These identifiers are ten-digit numbers. The developer wants to ensure input validation is fast because a large number of people use the system.

Which of the following would be the BEST advice for the security engineer to give to the developer?

A. Replace code with Java-based type checks
B. Parse input into an array
C. Use regular expressions
D. Canonicalize input into string objects before validation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A network printer needs Internet access to function. Corporate policy states all devices allowed on the network must be authenticated. Which of the following is the MOST secure method to allow the printer on the network without violating policy?

A. Request an exception to the corporate policy from the risk management committee
B. Require anyone trying to use the printer to enter their username and password
C. Have a help desk employee sign in to the printer every morning
D. Issue a certificate to the printer and use certificate-based authentication

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
The Chief Information Security Officer (CISO) of an e-retailer, which has an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on-site, the authorities ask a security engineer to create a point-in-time copy of the running database in their presence. This is an example of:

A. creating a forensic image
B. deploying fraud monitoring
C. following a chain of custody
D. analyzing the order of volatility

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

A. Bug bounty websites
B. Hacker forums
C. Antivirus vendor websites
D. Trade industry association websites
E. CVE database
F. Company's legal department

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A security assessor is working with an organization to review the policies and procedures associated with managing the organization's virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to:

A. segment dual-purpose systems on a hardened network segment with no external access
B. assess the risks associated with accepting non-compliance with regulatory requirements
C. update system implementation procedures to comply with regulations
D. review regulatory requirements and implement new policies on any newly provisioned servers

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 129
The Chief Information Security Officer (CISO) suspects that a database administrator has been tampering with financial data to the administrator's advantage. Which of the following would allow a third-party consultant to conduct an on-site review of the administrator's activity?

A. Separation of duties
B. Job rotation
C. Continuous monitoring
D. Mandatory vacation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
While investigating suspicious activity on a server, a security administrator runs the following report:

```
File system integrity check report
Total number of files:      3321
Added files:                12
Removed files:              0
Changed files:              1

Change files:
changed: /etc/passwd
-----------------------------------------------
Detailed information about changes:
File: /etc/passwd
Perm: -rw-r--r-- , -rw-r--rw-
Hash: md5:ab8e9acb928dfac35de2ac2bef918cae,md5:def9a24cdb68deaf4cb15acfed93eedb
```

In addition, the administrator notices changes to the /etc/shadow file that were not listed in the report. Which of the following BEST describe this scenario? (Choose two.)

A. An attacker compromised the server and may have used a collision hash in the MD5 algorithm to hide the changes to the /etc/shadow file
B. An attacker compromised the server and may have also compromised the file integrity database to hide the changes to the /etc/shadow file
C. An attacker compromised the server and may have installed a rootkit to always generate valid MD5 hashes to hide the changes to the /etc/shadow file
D. An attacker compromised the server and may have used MD5 collision hashes to generate valid passwords, allowing further access to administrator accounts on the server
E. An attacker compromised the server and may have used SELinux mandatory access controls to hide the changes to the /etc/shadow file

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
Following a recent network intrusion, a company wants to determine the current security awareness of all of its employees. Which of the following is the BEST way to test awareness?

A. Conduct a series of security training events with comprehensive tests at the end
B. Hire an external company to provide an independent audit of the network security posture
C. Review the social media of all employees to see how much proprietary information is shared
D. Send an email from a corporate account, requesting users to log onto a website with their enterprise account

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A company's security policy states any remote connections must be validated using two forms of network-based authentication. It also states local administrative accounts should not be used for any remote access. PKI currently is not configured within the network. RSA tokens have been provided to all employees, as well as a mobile application that can be used for 2FA authentication. A new NGFW has been installed within the network to provide security for external connections, and the company has decided to use it for VPN connections as well. Which of the following should be configured? (Choose two.) A. Certificate-based authentication

B. TACACS+
C. 802.1X
D. RADIUS
E. LDAP
F. Local user database

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used?

A. Avoid
B. Mitigate

C. Transfer
D. Accept

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A security administrator is updating a company's SCADA authentication system with a new application. To ensure interoperability between the legacy system and the new application, which of the following stakeholders should be involved in the configuration process before deployment? (Choose two.)

A. Network engineer
B. Service desk personnel
C. Human resources administrator
D. Incident response coordinator
E. Facilities manager
F. Compliance manager

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
A security analyst is classifying data based on input from data owners and other stakeholders. The analyst has identified three data types:
1. Financially sensitive data
2. Project data
3. Sensitive project data

The analyst proposes that the data be protected in two major groups, with further access control separating the financially sensitive data from the sensitive project data. The normal project data will be stored in a separate, less secure location. Some stakeholders are concerned about the recommended approach and insist that commingling data from different sensitive projects would leave them vulnerable to industrial espionage.

Which of the following is the BEST course of action for the analyst to recommend?

A. Conduct a quantitative evaluation of the risks associated with commingling the data and reject or accept the concerns raised by the stakeholders.
B. Meet with the affected stakeholders and determine which security controls would be sufficient to address the newly raised risks.
C. Use qualitative methods to determine aggregate risk scores for each project and use the derived scores to more finely segregate the data.
D. Increase the number of available data storage devices to provide enough capacity for physical separation of non-sensitive project data.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
First responders, who are part of a core incident response team, have been working to contain an outbreak of ransomware that also led to data loss. In a rush to isolate the three hosts that were calling out to the NAS to encrypt whole directories, the hosts were shut down immediately without investigation and then isolated. Which of the following were missed? (Choose two.)

A. CPU, process state tables, and main memory dumps
B. Essential information needed to perform data restoration to a known clean state
C. Temporary file system and swap space
D. Indicators of compromise to determine ransomware encryption
E. Chain of custody information needed for investigation

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A security engineer successfully exploits an application during a penetration test. As proof of the exploit, the security engineer takes screenshots of how data was compromised in the application. Given the information below from the screenshot.

```
2019-11-21 13:11:45 POST https://company.com/store
         <-- 200 text/plain 2.02kB 0.9s
.......Request.....**Response**.......Detail......
:Status: 200
Content-Types:text/plain
Content-Length: 2022
Date: Sun, 21 Nov 2019 18:11:45 GMT
.......RAW.........................................
Method: POST
Protocol: HTTP/2.0
RemoteAddr: v10.10.45.00:443
RequestURI:   "/store"
.......................
"product": [
{ "item": "745"
  "name": "Deluxe Pencil Case"
  "price": "0.10"
  "discount": "0.10"
} ,
}
```


Which of the following tools was MOST likely used to exploit the application?

A. The engineer captured the data with a protocol analyzer, and then utilized Python to edit the data
B. The engineer queried the server and edited the data using an HTTP proxy interceptor
C. The engineer used a cross-site script sent via curl to edit the data
D. The engineer captured the HTTP headers, and then replaced the JSON data with a banner-grabbing tool

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A security engineer is analyzing an application during a security assessment to ensure it is configured to protect against common threats. Given the output below:

```
Response Headers
Cache-Control:no-cache
Content-Type:text/event-stream
Date:Mon, 17 Sep 2018 15:58:37 GMT
Expires:-1
Pragma:no-cache
Transfer-Encoding:chunked
X-Content-Type-Options:nosniff
X-Frame-Options:SAMEORIGIN

Request Headers
Host: secure.comptia.org
Connection: keep-alive
Accept: text/event-stream
Cache-Control: no-cache
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US, en;q=0.9
```


Which of the following tools did the security engineer MOST likely use to generate this output?

A. Application fingerprinter
B. Fuzzer
C. HTTP interceptor
D. Vulnerability scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139

The Chief Financial Officer (CFO) of a major hospital system has received a ransom letter that demands a large sum of cryptocurrency be transferred to an anonymous account. If the transfer does not take place within ten hours, the letter states that patient information will be released on the dark web. A partial listing of recent patients is included in the letter. This is the first indication that a breach took place. Which of the following steps should be done FIRST?

A. Review audit logs to determine the extent of the breach
B. Pay the hacker under the condition that all information is destroyed
C. Engage a counter-hacking team to retrieve the data
D. Notify the appropriate legal authorities and legal counsel

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A Chief Information Security Officer (CISO) is working with a consultant to perform a gap assessment prior to an upcoming audit. It is determined during the assessment that the organization lacks controls to effectively assess regulatory compliance by third-party service providers. Which of the following should be revised to address this gap?

A. Privacy policy
B. Work breakdown structure
C. Interconnection security agreement
D. Vendor management plan
E. Audit report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
A security administrator is advocating for enforcement of a new policy that would require employers with privileged access accounts to undergo periodic inspections and review of certain job performance data. To which of the following policies is the security administrator MOST likely referring?

A. Background investigation
B. Mandatory vacation
C. Least privilege
D. Separation of duties

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
An organization is reviewing endpoint security solutions. In evaluating products, the organization has the following requirements:

1. Support server, laptop, and desktop infrastructure
2. Due to limited security resources, implement active protection capabilities
3. Provide users with the ability to self-service classify information and apply policies
4. Protect data-at-rest and data-in-use

Which of the following endpoint capabilities would BEST meet the above requirements? (Choose two.)

A. Data loss prevention
B. Application whitelisting
C. Endpoint detect and respond
D. Rights management
E. Log monitoring
F. Antivirus

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143

A Chief Information Security Officer (CISO) implemented MFA for all accounts in parallel with the BYOD policy. After the implementation, employees report the increased authentication method is causing increased time to tasks. This applies both to accessing the email client on the workstation and the online collaboration portal. Which of the following should be the CISO implement to address the employees' concerns?

A. Create an exception for the company's IPs.
B. Implement always-on VPN.
C. Configure the use of employee PKI authentication for email.
D. Allow the use of SSO.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A Chief Information Security Officer (CISO) of a large financial institution undergoing an IT transformation program wants to embed security across the business rapidly and across as many layers of the business as possible to achieve quick wins and reduce risk to the organization. Which of the following business areas should the CISO target FIRST to best meet the objective?

A. Programmers and developers should be targeted to ensure secure coding practices, including automated code reviews with remediation processes, are implemented immediately.
B. Human resources should be targeted to ensure all new employees undertake security awareness and compliance training to reduce the impact of phishing and ransomware attacks.
C. The project management office should be targeted to ensure security is managed and included at all levels of the project management cycle for new and inflight projects.
D. Risk assurance teams should be targeted to help identify key business unit security risks that can be aggregated across the organization to produce a risk posture dashboard for executive management.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145

A security engineer is investigating a compromise that occurred between two internal computers. The engineer has determined during the investigation that one computer infected another. While reviewing the IDS logs, the engineer can view the outbound callback traffic, but sees no traffic between the two computers. Which of the following would BEST address the IDS visibility gap?

A. Install network taps at the edge of the network.
B. Send syslog from the IDS into the SIEM.
C. Install HIDS on each computer.
D. SPAN traffic form the network core into the IDS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Staff members are reporting an unusual number of device thefts associated with time out of the office. Thefts increased soon after the company deployed a new social networking application. Which of the following should the Chief Information Security Officer (CISO) recommend implementing?

A. Automatic location check-ins
B. Geolocated presence privacy
C. Integrity controls
D. NAC checks to quarantine devices

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 147
A security engineer is assessing a new IoT product. The product interfaces with the ODBII port of a vehicle and uses a Bluetooth connection to relay data to an onboard data logger located in the vehicle. The data logger can only transfer data over a custom USB cable. The engineer suspects a relay attack is possible against the cryptographic implementation used to secure messages between segments of the system. Which of the following tools should the engineer use to confirm the analysis?

A. Binary decompiler

B. Wireless protocol analyzer
C. Log analysis and reduction tools
D. Network-based fuzzer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A recent security assessment revealed a web application may be vulnerable to clickjacking. According to the application developers, a fix may be months away. Which of the following should a security engineer configure on the web server to help mitigate the issue?

A. File upload size limits
B. HttpOnly cookie field
C. X-Frame-Options header
D. Input validation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
A developer is reviewing the following transaction logs from a web application:

```
Username: John Doe
Street name: Main St.
Street number: <script>alert('test')</alert>
```

Which of the following code snippets should the developer implement given the above transaction logs?

A. `if ($input != strcmp($var1, "<>")) {die();}`
B. `<form name ="form1" action="/submit.php" onsubmit="return validate()" action=POST>`

C. `$input=strip_tags(trim($_POST['var1']));`

D. `<html><form name="myform" action="www.server.com/php/submit.php action=GET"`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
An engineer is reviewing the security architecture for an enterprise network. During the review, the engineer notices an undocumented node on the network. Which of the following approaches can be utilized to determine how this node operates? (Choose two.)

A. Use reverse engineering and techniques
B. Assess the node within a continuous integration environment
C. Employ a static code analyzer
D. Review network and traffic logs
E. Use a penetration testing framework to analyze the node
F. Analyze the output of a ping sweep

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A security administrator is reviewing the following output from an offline password audit:

Username	Password	Crack Time
User1	Teleportation1	4s
User2	Amphitheater!	2s
User3	Undetermined4u.	10s

Which of the following should the systems administrator implement to BEST address this audit finding? (Choose two.)

A. Cryptoprocessor
B. Bcrypt
C. SHA-256
D. PBKDF2
E. Message authentication

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A corporate forensic investigator has been asked to acquire five forensic images of an employee database application. There are three images to capture in the United States, one in the United Kingdom, and one in Germany. Upon completing the work, the forensics investigator saves the images to a local workstation. Which of the following types of concerns should the forensic investigator have about this work assignment?

A. Environmental
B. Privacy
C. Ethical
D. Criminal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 153
Ann, a corporate executive, has been the recent target of increasing attempts to obtain corporate secrets by competitors through advanced, well-funded means. Ann frequently leaves her laptop unattended and physically unsecure in hotel rooms during travel. A security engineer must find a practical solution for Ann that minimizes the need for user training. Which of the following is the BEST solution in this scenario?

A. Full disk encryption
B. Biometric authentication
C. An eFuse-based solution
D. Two-factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A security appliance vendor is reviewing an RFP that is requesting solutions for the defense of a set of web-based applications. This RFP is from a financial institution with very strict performance requirements. The vendor would like to respond with its solutions.

Before responding, which of the following factors is MOST likely to have an adverse effect on the vendor's qualifications?

A. The solution employs threat information-sharing capabilities using a proprietary data model.
B. The RFP is issued by a financial institution that is headquartered outside of the vendor's own country.
C. The overall solution proposed by the vendor comes in less that the TCO parameter in the RFP.
D. The vendor's proposed solution operates below the KPPs indicated in the RFP.

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:

QUESTION 155
Company leadership believes employees are experiencing an increased number of cyber attacks; however, the metrics do not show this. Currently, the company uses “Number of successful phishing attacks” as a KRI, but it does not show an increase.

Which of the following additional information should be the Chief Information Security Officer (CISO) include in the report?

A. The ratio of phishing emails to non-phishing emails
B. The number of phishing attacks per employee
C. The number of unsuccessful phishing attacks
D. The percent of successful phishing attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A laptop is recovered a few days after it was stolen.

Which of the following should be verified during incident response activities to determine the possible impact of the incident?

A. Full disk encryption status
B. TPM PCR values
C. File system integrity
D. Presence of UEFI vulnerabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
Ann, a security administrator, is conducting an assessment on a new firewall, which was placed at the perimeter of a network containing PII. Ann runs the following commands on a server (10.0.1.19) behind the firewall:

```
service iptables stop
service sshd stop
```

From her own workstation (192.168.2.45) outside the firewall, Ann then runs a port scan against the server and records the following packet capture of the port scan:

```
0.872299   192.168.2.45 -> 10.0.1.19 TCP   62  49188 > 22  [SYN] Seq=0 Len=0 MSS=1460
0.872899   10.0.1.19 -> 192.168.2.45 TCP   62  22 > 49188  [RST] Seq=0 Len=0 MSS=1460
0.891308   192.168.2.45 ->10.0.1.19  TCP   62  49189 > 23  [SYN] Seq=0 Len=0 MSS=1460
0.891809   10.0.1.19 -> 192.168.2.45 TCP   62  23 > 49189  [RST] Seq=0 Len=0 MSS=1460
0.901234   192.168.2.45 -> 10.0.1.19 TCP   62  49190 > 24  [SYN] Seq=0 Len=0 MSS=1460
0.901454   10.0.1.19 -> 192.168.2.45 TCP   62  24 > 49190  [RST] Seq=0 Len=0 MSS=1460
0.925657   192.168.2.45 -> 10.0.1.19 TCP   62  49191 > 25  [SYN] Seq=0 Len=0 MSS=1460
0.929872   10.0.1.19 -> 192.168.2.45 TCP   62  25 > 49191  [RST] Seq=0 Len=0 MSS=1460
```

Connectivity to the server from outside the firewall worked as expected prior to executing these commands.

Which of the following can be said about the new firewall?

A. It is correctly dropping all packets destined for the server.
B. It is not blocking or filtering any traffic to the server.
C. Iptables needs to be restarted.
D. The IDS functionality of the firewall is currently disabled.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
A new database application was added to a company's hosted VM environment. Firewall ACLs were modified to allow database users to access the server remotely. The company's cloud security broker then identified abnormal from a database user on-site. Upon further investigation, the security team noticed the user ran code on a VM that provided access to the hypervisor directly and access to other sensitive data.

Which of the following should the security team do to help mitigate future attacks within the VM environment? (Choose two.)

A. Install the appropriate patches.
B. Install perimeter NGFW.
C. Configure VM isolation.
D. Deprovision database VM.
E. Change the user's access privileges.
F. Update virus definitions on all endpoints.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A penetration testing manager is contributing to an RFP for the purchase of a new platform. The manager has provided the following requirements:

- Must be able to MITM web-based protocols
- Must be able to find common misconfigurations and security holes

Which of the following types of testing should be included in the testing platform? (Choose two.)

A. Reverse engineering tool
B. HTTP intercepting proxy
C. Vulnerability scanner
D. File integrity monitor
E. Password cracker
F. Fuzzer

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 160

An incident responder wants to capture volatile memory comprehensively from a running machine for forensic purposes. The machine is running a very recent release of the Linux OS.

Which of the following technical approaches would be the MOST feasible way to accomplish this capture?

A. Run the `memdump` utility with the `-k` flag.
B. Use a loadable kernel module capture utility, such as LiME.
C. Run `dd` on/dev/mem.
D. Employ a stand-alone utility, such as FTK Imager.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
An online bank has contracted with a consultant to perform a security assessment of the bank's web portal. The consultant notices the login page is linked from the main page with HTTPS, but when the URL is changed to HTTP, the browser is automatically redirected back to the HTTPS site. Which of the following is a concern for the consultant, and how can it be mitigated?

A. XSS could be used to inject code into the login page during the redirect to the HTTPS site. The consultant should implement a WAF to prevent this.
B. The consultant is concerned the site is using an older version of the SSL 3.0 protocol that is vulnerable to a variety of attacks. Upgrading the site to TLS 1.0 would mitigate this issue.
C. The HTTP traffic is vulnerable to network sniffing, which could disclose usernames and passwords to an attacker. The consultant should recommend disabling HTTP on the web server.
D. A successful MITM attack Could intercept the redirect and use `sslstrip t`o decrypt further HTTPS traffic. Implementing HSTS on the web server would prevent this.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162

A security administrator wants to implement controls to harden company-owned mobile devices. Company policy specifies the following requirements:

- Mandatory access control must be enforced by the OS.
- Devices must only use the mobile carrier data transport.

Which of the following controls should the security administrator implement? (Choose three.)

A. Enable DLP
B. Enable SEAndroid
C. Enable EDR
D. Enable secure boot
E. Enable remote wipe
F. Disable Bluetooth
G. Disable 802.11
H. Disable geotagging

Correct Answer: BFG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
While conducting online research about a company to prepare for an upcoming penetration test, a security analyst discovers detailed financial information on an investor website the company did not make public. The analyst shares this information with the Chief Financial Officer (CFO), who confirms the information is accurate, as it was recently discussed at a board of directors meeting. Many of the details are verbatim discussion comments captured by the board secretary for purposes of transcription on a mobile device. Which of the following would MOST likely prevent a similar breach in the future?

A. Remote wipe
B. FDE
C. Geolocation
D. eFuse
E. VPN

Correct Answer: B
Section: (none)

Explanation
Explanation/Reference:

QUESTION 164
An infrastructure team within an energy organization is at the end of a procurement process and has selected a vendor's SaaS platform to deliver services. As part of the legal negotiation, there are a number of outstanding risks, including:

1. There are clauses that confirm a data retention period in line with what is in the energy organization's security policy.
2. The data will be hosted and managed outside of the energy organization's geographical location.

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

A. Develop a security exemption, as the solution does not meet the security policies of the energy organization.
B. Require a solution owner within the energy organization to accept the identified risks and consequences.
C. Mititgate the risks by asking the vendor to accept the in-country privacy principles and modify the retention period.
D. Review the procurement process to determine the lessons learned in relation to discovering risks toward the end of the process.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A developer emails the following output to a security administrator for review:

```
curl -X TRACE host1
User-Agent: curl/7.25.0
Host: host1
Accept: */*
Cookie: user=badguy: path=/; HttpOnly
```

Which of the following tools might the security administrator use to perform further security assessment of this issue?

A. Port scanner

B. Vulnerability scanner
C. Fuzzer
D. HTTP interceptor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
After significant vulnerabilities and misconfigurations were found in numerous production web applications, a security manager identified the need to implement better development controls.
Which of the following controls should be verified? (Choose two.)

A. Input validation routines are enforced on the server side.
B. Operating systems do not permit null sessions.
C. Systems administrators receive application security training.
D. VPN connections are terminated after a defined period of time.
E. Error-handling logic fails securely.
F. OCSP calls are handled effectively.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A financial institution's information security officer is working with the risk management officer to determine what to do with the institution's residual risk after all security controls have been implemented. Considering the institution's very low risk tolerance, which of the following strategies would be BEST?

A. Transfer the risk.
B. Avoid the riskC. Mitigate the risk.
D. Accept the risk.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A security engineer is assessing the controls that are in place to secure the corporate-Internet-facing DNS server. The engineer notices that security ACLs exist but are not being used properly. The DNS server should respond to any source but only provide information about domains it has authority over. Additionally, the DNS administrator have identified some problematic IP addresses that should not be able to make DNS requests. Given the ACLs below:

```
acl secondary-dns {
      192.168.1.54;
};
acl internal-nets {
      192.168.1.0/24;
};
acl blacklist-ips {
      244.0.22.39;
      12.122.1.0/24;
      122.64.8.80;
};
```


Which of the following should the security administrator configure to meet the DNS security needs?

A.
```
zone "company.com" in {
      type "master";
      file "company.hosts";
      allow-query { any; };
      allow-transfer { !blacklist-ips; };
};
```

```
zone "company.com" in {
      type "master";
      file "company.hosts";
      allow-query { secondary-dns; internal-nets; !blacklist-ips; ; };
      allow-transfer {none; };
};
```

B.

```
zone "company.com" in {
      type "master";
      file "company.hosts";
      allow-query { internal-nets; !blacklist-ips; };
      allow-transfer {none; };
};
```

C.

```
zone "company.com" in {
      type "master";
      file "company.hosts";
      allow-query {any; !blacklist-ips; };
      allow-transfer { secondary-dns; };
};
```

D.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
An organization is deploying IoT locks, sensors, and cameras, which operate over 802.11, to replace legacy building access control systems. These devices are capable of triggering physical access changes, including locking and unlocking doors and gates. Unfortunately, the devices have known vulnerabilities for which the vendor has yet to provide firmware updates.

Which of the following would BEST mitigate this risk?

A. Direct wire the IoT devices into physical switches and place them on an exclusive VLAN.
B. Require sensors to sign all transmitted unlock control messages digitally.
C. Associate the devices with an isolated wireless network configured for WPA2 and EAP-TLS.
D. Implement an out-of-band monitoring solution to detect message injections and attempts.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
During a sprint, developers are responsible for ensuring the expected outcome of a change is thoroughly evaluated for any security impacts. Any impacts must be reported to the team lead. Before changes are made to the source code, which of the following MUST be performed to provide the required information to the team lead?

A. Risk assessment
B. Regression testing
C. User story development
D. Data abstraction
E. Business impact assessment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data? (Choose two.)

A. Data aggregation
B. Data sovereignty
C. Data isolation
D. Data volume
E. Data analytics
F. Data precision

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A company recently implemented a new cloud storage solution and installed the required synchronization client on all company devices. A few months later, a breach of sensitive data was discovered. Root cause analysis shows the data breach happened from a lost personal mobile device.

Which of the following controls can the organization implement to reduce the risk of similar breaches?

A. Biometric authentication
B. Cloud storage encryption
C. Application containerization
D. Hardware anti-tamper

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
An enterprise's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise's growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise's website.

Which of the following should the CISO be MOST concerned about?

A. Poor capacity planning could cause an oversubscribed host, leading to poor performance on the company's website.
B. A security vulnerability that is exploited on the website could expose the accounting service.
C. Transferring as many services as possible to a CSP could free up resources.
D. The CTO does not have the budget available to purchase required resources and manage growth.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
A company is moving all of its web applications to an SSO configuration using SAML. Some employees report that when signing in to an application, they get an error message on the login screen after entering their username and password, and are denied access. When they access another system that has been converted to the new SSO authentication model, they are able to authenticate successfully without being prompted for login.

Which of the following is MOST likely the issue?

A. The employees are using an old link that does not use the new SAML authentication.
B. The XACML for the problematic application is not in the proper format or may be using an older schema.
C. The web services methods and properties are missing the required WSDL to complete the request after displaying the login page.
D. A threat actor is implementing an MITM attack to harvest credentials.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A penetration tester is trying to gain access to a remote system. The tester is able to see the secure login page and knows one user account and email address, but has not yet discovered a password.

Which of the following would be the EASIEST method of obtaining a password for the known account?

A. Man-in-the-middle
B. Reverse engineering
C. Social engineering
D. Hash cracking
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Due to a recent acquisition, the security team must find a way to secure several legacy applications. During a review of the applications, the following issues are documented:

- The applications are considered mission-critical.
- The applications are written in code languages not currently supported by the development staff.
- Security updates and patches will not be made available for the applications.
- Username and passwords do not meet corporate standards.
- The data contained within the applications includes both PII and PHI.

▪ The applications communicate using TLS 1.0. ▪
Only internal users access the applications.

Which of the following should be utilized to reduce the risk associated with these applications and their current architecture?

A. Update the company policies to reflect the current state of the applications so they are not out of compliance.
B. Create a group policy to enforce password complexity and username requirements.
C. Use network segmentation to isolate the applications and control access.
D. Move the applications to virtual servers that meet the password and account standards.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A new security policy states all wireless and wired authentication must include the use of certificates when connecting to internal resources within the enterprise LAN by all employees.

Which of the following should be configured to comply with the new security policy? (Choose two.)
A. SSO
B. New pre-shared key
C. 802.1X
D. OAuth
E. Push-based authentication
F. PKI

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A security consultant was hired to audit a company's password are account policy. The company implements the following controls:

- Minimum password length: 16
- Maximum password age: 0
- Minimum password age: 0
- Password complexity: disabled
- Store passwords in plain text: disabled
- Failed attempts lockout: 3 ▪

Lockout timeout: 1 hour

The password database uses salted hashes and PBKDF2. Which of the following is MOST likely to yield the greatest number of plain text passwords in the shortest amount of time?

A. Offline hybrid dictionary attack
B. Offline brute-force attack
C. Online hybrid dictionary password spraying attack
D. Rainbow table attack
E. Online brute-force attack
F. Pass-the-hash attack

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 179
As part of the asset management life cycle, a company engages a certified equipment disposal vendor to appropriately recycle and destroy company assets that are no longer in use. As part of the company's vendor due diligence, which of the following would be MOST important to obtain from the vendor?

A. A copy of the vendor's information security policies.
B. A copy of the current audit reports and certifications held by the vendor.
C. A signed NDA that covers all the data contained on the corporate systems.
D. A copy of the procedures used to demonstrate compliance with certification requirements.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
The audit team was only provided the physical and logical addresses of the network without any type of access credentials.

Which of the following methods should the audit team use to gain initial access during the security assessment? (Choose two.)

A. Tabletop exercise
B. Social engineering
C. Runtime debugging
D. Reconnaissance
E. Code review
F. Remote access tool

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
A product manager is concerned about the unintentional sharing of the company's intellectual property through employees' use of social media. Which of the following would BEST mitigate this risk?

A. Virtual desktop environment
B. Network segmentation
C. Web application firewall
D. Web content filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
A company uses an application in its warehouse that works with several commercially available tablets and can only be accessed inside the warehouse. The support department would like the selection of tablets to be limited to three models to provide better support and ensure spares are on hand. Users often keep the tablets after they leave the department, as many of them store personal media items.

Which of the following should the security engineer recommend to meet these requirements?

A. COPE with geofencing
B. BYOD with containerization
C. MDM with remote wipe
D. CYOD with VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
After an employee was terminated, the company discovered the employee still had access to emails and attached content that should have been destroyed during the off-boarding. The employee's laptop and cell phone were confiscated and accounts were disabled promptly. Forensic investigation suggests the company's DLP was effective, and the content in question was not sent outside of work or transferred to removable media. Personality owned devices are not permitted to access company systems or information.
Which of the following would be the MOST efficient control to prevent this from occurring in the future?

A. Install application whitelist on mobile devices.
B. Disallow side loading of applications on mobile devices.
C. Restrict access to company systems to expected times of day and geographic locations.
D. Prevent backup of mobile devices to personally owned computers.
E. Perform unannounced insider threat testing on high-risk employees.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: