**CAS-003.119q**

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

**CAS-003**




**CompTIA Advanced Security Practitioner (CASP)**

**Exam A**

**QUESTION 1**
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 2**
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:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
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:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 4**
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 5**
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:

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



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

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

**Correct Answer:** BE

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
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 7**
After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:
- Duplicate IP addresses
- Rogue network devices
- Infected systems probing the company's network

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

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

**Correct Answer:** BC

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
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 9**
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

A. Call the CIO and ask for an interview, posing as a job seeker interested in an open position
B. Compromise the email server to obtain a list of attendees who responded to the invitation who is on the IT staff
C. Notify the CIO that, through observation at events, malicious actors can identify individuals to befriend
D. Understand the CIO is a social drinker, and find the means to befriend the CIO at establishments the CIO frequents

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

**QUESTION 10**
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

A. Vulnerability assessment
B. Risk assessment
C. Patch management
D. Device quarantine
E. Incident management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
A systems administrator at a medical imaging company discovers protected health information (PHI) on a general purpose file server. Which of the following steps should the administrator take NEXT?



A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2
B. Immediately encrypt all PHI with AES 256
C. Delete all PHI from the network until the legal department is consulted
D. Consult the legal department to determine legal requirements

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
A Chief Information Security Officer (CISO) is reviewing the results of a gap analysis with an outside cybersecurity consultant. The gap analysis reviewed all procedural and technical controls and found the following:
- High-impact controls implemented: 6 out of 10
- Medium-impact controls implemented: 409 out of 472
- Low-impact controls implemented: 97 out of 1000

The report includes a cost-benefit analysis for each control gap. The analysis yielded the following information:

- Average high-impact control implementation cost: $15,000; Probable ALE for each high-impact control gap: $95,000
- Average medium-impact control implementation cost: $6,250; Probable ALE for each medium-impact control gap: $11,000

Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

A. Too much emphasis has been placed on eliminating low-risk vulnerabilities in the past
B. The enterprise security team has focused exclusively on mitigating high-level risks
C. Because of the significant ALE for each high-risk vulnerability, efforts should be focused on those controls
D. The cybersecurity team has balanced residual risk for both high and medium controls

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**
After investigating virus outbreaks that have cost the company $1000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

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

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

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?



A. Update and deploy GPOs
B. Configure and use measured boot
C. Strengthen the password complexity requirements
D. Update the antivirus software and definitions

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 15**
A company monitors the performance of all web servers using WMI. A network administrator informs the security engineer that web servers hosting the company's client-facing portal are running slowly today. After some investigation, the security engineer notices a large number of attempts at enumerating host information via SNMP from multiple IP addresses. Which of the following would be the BEST technique for the security engineer to employ in an attempt to prevent reconnaissance activity?

A. Install a HIPS on the web servers
B. Disable inbound traffic from offending sources
C. Disable SNMP on the web servers

D. Install anti-DDoS protection in the DMZ

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 16**
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 17**
A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

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

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

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

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
An advanced threat emulation engineer is conducting testing against a client's network. The engineer conducts the testing in as realistic a manner as possible. Consequently, the engineer has been gradually ramping up the volume of attacks over a long period of time. Which of the following combinations of techniques would the engineer MOST likely use in this testing? (Choose three.)

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



**Correct Answer:** AEF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 19**
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 20**
A newly hired systems administrator is trying to connect a new and fully updated, but very customized, Android device to access corporate resources. However, the MDM enrollment process continually fails. The administrator asks a security team member to look into the issue. Which of the following is the MOST likely reason the MDM is not allowing enrollment?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 21**

A hospital uses a legacy electronic medical record system that requires multicast for traffic between the application servers and databases on virtual hosts that support segments of the application. Following a switch upgrade, the electronic medical record is unavailable despite physical connectivity between the hypervisor and the storage being in place. The network team must enable multicast traffic to restore access to the electronic medical record. The ISM states that the network team must reduce the footprint of multicast traffic on the network.

| VLAN | Description |
|---|---|
| 201 | Server VLAN1 |
| 202 | Server VLAN2 |
| 400 | Hypervisor Management VLAN |
| 680 | Storage Management VLAN |
| 700 | Database Server VLAN |



Using the above information, on which VLANs should multicast be enabled?

A. VLAN201, VLAN202, VLAN400
B. VLAN201, VLAN202, VLAN700
C. VLAN201, VLAN202, VLAN400, VLAN680, VLAN700
D. VLAN400, VLAN680, VLAN700

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
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 23**
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 24**
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 25**
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 26**
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 27**
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

A. RA
B. BIA
C. NDA D. RFI
E. RFQ
F. MSA

**Correct Answer:** CF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**

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

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

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
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 30**
Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

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

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-47.pdf

**QUESTION 31**
A company is developing requirements for a customized OS build that will be used in an embedded environment. The company procured hardware that is capable of reducing the likelihood of successful buffer overruns while executables are processing. Which of the following capabilities must be included for the OS to take advantage of this critical hardware-based countermeasure?

A. Application whitelisting
B. NX/XN bit
C. ASLR
D. TrustZone
E. SCP



**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 32**
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 33**
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 34**
After multiple service interruptions caused by an older datacenter design, a company decided to migrate away from its datacenter. The company has successfully completed the migration of all datacenter servers and services to a cloud provider. The migration project includes the following phases:

- Selection of a cloud provider
- Architectural design
- Microservice segmentation
- Virtual private cloud
- Geographic service redundancy
- Service migration

The Chief Information Security Officer (CISO) is still concerned with the availability requirements of critical company applications. Which of the following should the company implement NEXT?

A. Multicloud solution
B. Single-tenancy private cloud
C. Hybrid cloud solution
D. Cloud access security broker

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
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 36**
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 37**
A web developer has implemented HTML5 optimizations into a legacy web application. One of the modifications the web developer made was the following client side optimization:

```
localStorage.setItem("session-cookie", document.cookie);
```

Which of the following should the security engineer recommend?

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

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**



**QUESTION 38**
A hospital's security team recently determined its network was breached and patient data was accessed by an external entity. The Chief Information Security Officer
(CISO) of the hospital approaches the executive management team with this information, reports the vulnerability that led to the breach has already been remediated, and explains the team is continuing to follow the appropriate incident response plan. The executive team is concerned about the hospital's brand reputation and asks the CISO when the incident should be disclosed to the affected patients. Which of the following is the MOST appropriate response?

A. When it is mandated by their legal and regulatory requirements
B. As soon as possible in the interest of the patients
C. As soon as the public relations department is ready to be interviewed
D. When all steps related to the incident response plan are completed
E. Upon the approval of the Chief Executive Officer (CEO) to release information to the public

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 39**

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 40**
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 41**
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

A. Multi-tenancy SaaS
B. Hybrid IaaS
C. Single-tenancy PaaS
D. Community IaaS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 42**
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 43**
SIMULATION

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





**Correct Answer:** Please see the explanation below **Section: (none) Explanation**

**Explanation/Reference:**
Step 1: Verify that the certificate is valid or not. In case of any warning message, cancel the download.
Step 2: If certificate issue is not there then, download the file in your system.
Step 3: Calculate the hash value of the downloaded file.
Step 4: Match the hash value of the downloaded file with the one which you selected on the website.
Step 5: Install the file if the hash value matches.

**QUESTION 44**
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 45**
To meet a 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 46**
A security analyst sees some suspicious entries in a log file from a web server website, which has a form that allows customers to leave feedback on the company's products. The analyst believes a malicious actor is scanning the web form. To know which security controls to put in place, the analyst first needs to determine the type of activity occurring to design a control. Given the log below:

| Timestamp | SourceIP | CustName | PreferredContact | ProdName | Comments |
|---|---|---|---|---|---|
| Monday 10:00:04 | 10.14.34.55 | aaaaa | Phone | Widget1 | None left |
| Monday 10:00:04 | 10.14.34.55 | bbbbb | Phone | Widget1 | None left |
| Monday 10:00:05 | 10.14.34.55 | cccc | Phone | Widget1 | ../../etc/passwd |
| Monday 10:01:03 | 10.14.34.55 | ddddd | Phone | Widget1 | None left |
| Monday 10:01:04 | 10.14.34.55 | eeeee | Phone | Widget1 | None left |
| Monday 10:01:05 | 10.14.34.55 | fffff | Phone | Widget1 | 1=1 |
| Monday 10:03:05 | 172.16.34.20 | Joe | Phone | Widget30 | Love the Widget! |
| Monday 10:04:01 | 10.14.34.55 | ggggg | Phone | Widget1 | <script> |
| Monday 10:05:05 | 10.14.34.55 | hhhhh | Phone | Widget1 | wget cookie |
| Monday 10:05:05 | 10.14.34.55 | iiiii | Phone | Widget1 | None left |
| Monday 10:05:06 | 10.14.34.55 | lllll | Phone | Widget1 | None left |

Which of the following is the MOST likely type of activity occurring?

A. SQL injection
B. XSS scanning
C. Fuzzing
D. Brute forcing

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 47**
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:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 48**
A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.

Which of the following is the BEST way to address these issues and mitigate risks to the organization?

A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for end-user categorization and malware analysis.
B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short team.
D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 49**
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 50**
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? (Select two.)



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

**Correct Answer:** DF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 51**
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 52**
An information security officer is responsible for one secure network and one office network. Recent intelligence suggests there is an opportunity for attackers to gain access to the secure network due to similar login credentials across networks. To determine the users who should change their information, the information security officer uses a tool to scan a file with hashed values on both networks and receives the following data:

| Corporate Network | | Secure Network | |
|---|---|---|---|
| james.bond | asHU8$1bg | jbond | asHU8$1bg |
| tom.jones | wit4njyt%I | tom.jones | wit4njyt%I |
| dade.murphy | mUrpHTIME7 | d.murph3 | t%w3BT9)n |
| herbie.hancock | hh2016!# | hhanco | hh2016!#2 |
| suzy.smith | 1Li*#HFadf | ssmith | 1LI*#HFadf |

Which of the following tools was used to gather this information from the hashed values in the file?

A. Vulnerability scanner
B. Fuzzer
C. MD5 generator
D. Password cracker
E. Protocol analyzer

**Correct Answer:** C
**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 53**
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 54**
A systems administrator recently joined an organization and has been asked to perform a security assessment of controls on the organization's file servers, which contain client data from a number of sensitive systems. The administrator needs to compare documented access requirements to the access implemented within the file system.

Which of the following is MOST likely to be reviewed during the assessment? (Select two.)

A. Access control list
B. Security requirements traceability matrix
C. Data owner matrix
D. Roles matrix
E. Data design document
F. Data access policies

**Correct Answer:** DF
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 55**
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 56**
Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees. Source records will be email, PC, network shares, and applications.

After all restrictions have been lifted, which of the following should the information manager review?

A. Data retention policy
B. Legal hold
C. Chain of custody D. Scope statement

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 57**
SIMULATION

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.
This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.
The command window will be provided along with root access. You are connected via a secure shell with root access.
You may query help for a list of commands.

**Instructions:**

You need to disable and turn off unrelated services and processes.
It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


**Correct Answer:** See the explanation below
**Section: (none)**
**Explanation**
**Explanation/Reference:**
Explanation:

In Order to deactivate web services, database services and print service, we can do following things
1) deactivate its services
/etc/init.d/apache2 stop
/etc/init.d/mysqld stop
2) close ports for these services
Web Server
iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECT
service iptables save Print Server
iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECT
service iptables save Database Server
iptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECT
service iptables save
3) Kill the process any running for the sameps -aef|grep mysql kill -9 <<process id>>

**QUESTION 58**
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 59**
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 60**
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 61**
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

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

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 62**
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an exploit.


 Which of the following would provide greater insight on the potential impact of this attempted attack?

A. Run an antivirus scan on the finance PC.
B. Use a protocol analyzer on the air-gapped PC.
C. Perform reverse engineering on the document.
D. Analyze network logs for unusual traffic.
E. Run a baseline analyzer against the user's computer.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 63**

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

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

**Correct Answer:** BF
**Section: (none)**
**Explanation**

**Explanation/Reference:**



**QUESTION 64**
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 65**
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers. Which of the following BEST describes the contents of the supporting document the engineer is creating?

A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.
B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.
C. A set of formal methods that apply to one or more of the programing languages used on the development project.
D. A methodology to verify each security control in each unit of developed code prior to committing the code.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 66**
A security technician is incorporating the following requirements in an RFP for a new SIEM:

- New security notifications must be dynamically implemented by the SIEM engine
- The SIEM must be able to identify traffic baseline anomalies
- Anonymous attack data from all customers must augment attack detection and risk scoring

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



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

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 67**
An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

- Active full-device encryption

- Enabled remote-device wipe
- Blocking unsigned applications
- Containerization of email, calendar, and contacts

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

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 68**
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 69**
The Chief Information Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and two-factor authentication is not provided natively.

Which of the following would BEST address the CIO's concerns?

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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 70**
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 71**
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 72**
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

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

| | |
|---|---|
| **Password complexity** | **Disabled** |
| Require authentication from a domain controller before sign in | Enabled |
| Allow guest user access | Enabled |
| Allow anonymous enumeration of groups | Disabled |

A. Vulnerability scanner
B. SCAP scanner
C. Port scanner
D. Interception proxy

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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 74**
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 75**
A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it.

Which of the following is the MOST likely reason for the team lead's position?

A. The organization has accepted the risks associated with web-based threats.
B. The attack type does not meet the organization's threat model.
C. Web-based applications are on isolated network segments.
D. Corporate policy states that NIPS signatures must be updated every hour.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 76**
A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

To ensure the process provides the intended results, an auditor reviews the following content from a randomly selected decommissioned hard disk:

```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qjkehd
```



Which of the following should be included in the auditor's report based on the above findings?

A. The hard disk contains bad sectors
B. The disk has been degaussed.
C. The data represents part of the disk BIOS.
D. Sensitive data might still be present on the hard drives.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 77**
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 78**
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 79**
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 80**
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 81**

A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software.

Which of the following would BEST ensure the software and instruments are working as designed?

A. System design documentation
B. User acceptance testing
C. Peer review
D. Static code analysis testing
E. Change control documentation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 82**
A company has gone through a round of phishing attacks. More than 200 users have had their workstation infected because they clicked on a link in an email. An incident analysis has determined an executable ran and compromised the administrator account on each workstation. Management is demanding the information security team prevent this from happening again.

Which of the following would BEST prevent this from happening again?

A. Antivirus
B. Patch management
C. Log monitoring
D. Application whitelisting
E. Awareness training

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 83**

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 84**

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 85**
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 86**

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.

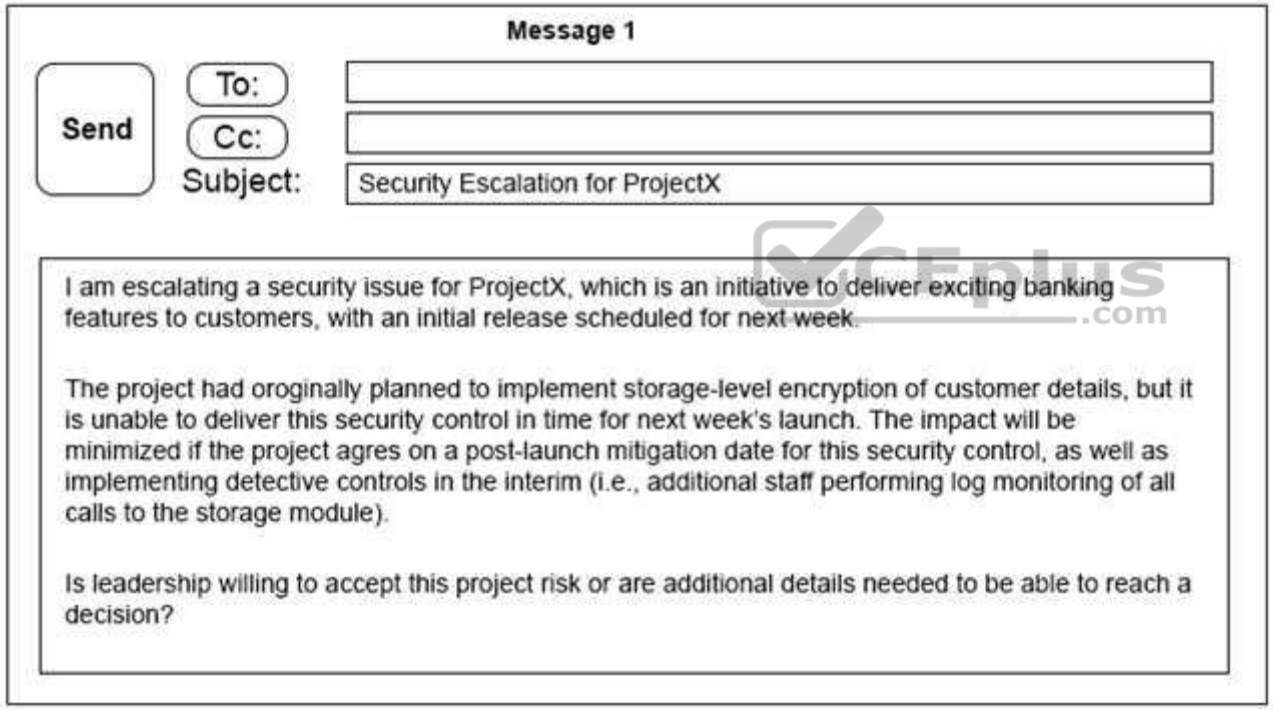
**Correct Answer:** A
**Section: (none)**
**Explanation**

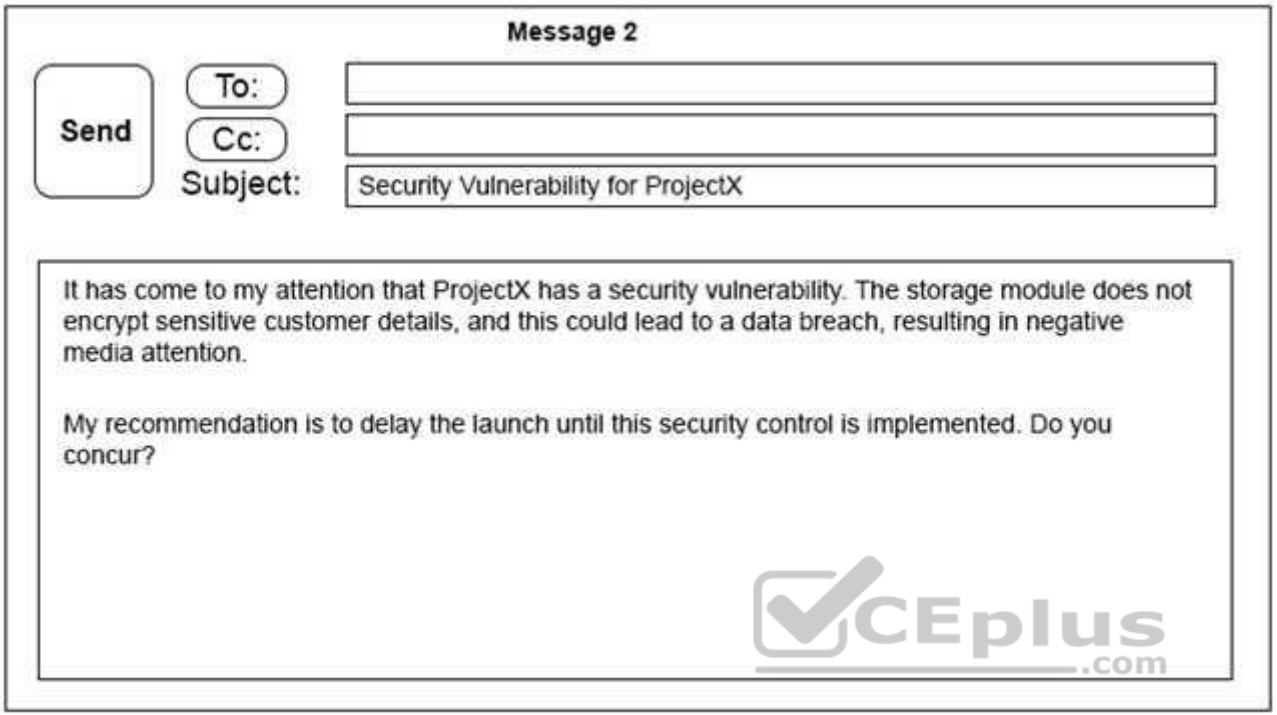
**Explanation/Reference:**

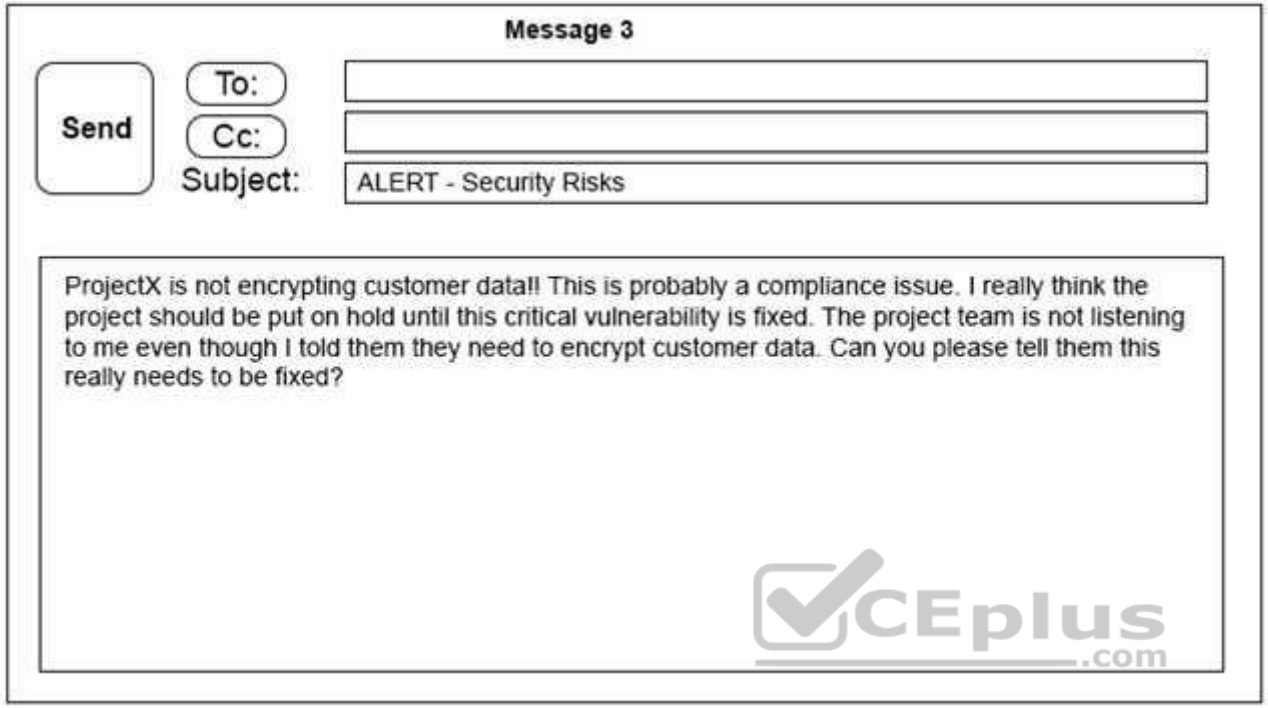


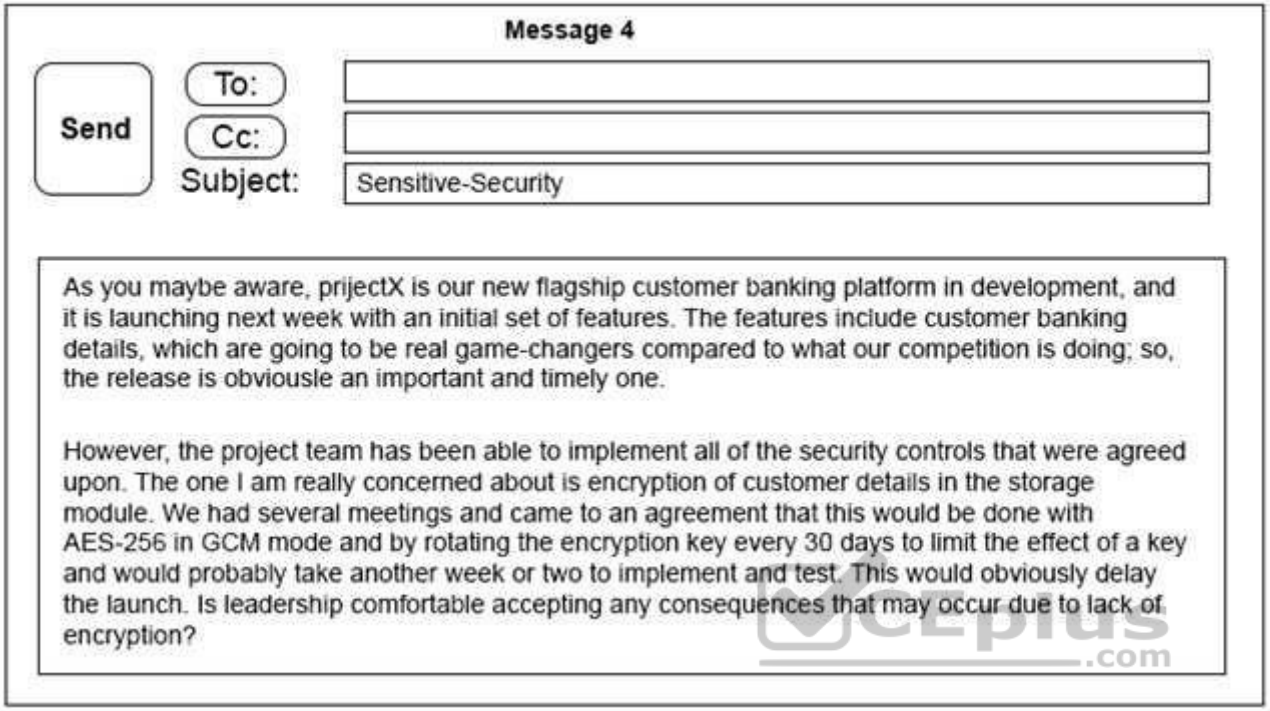
**QUESTION 87**
Click on the exhibit buttons to view the four messages.

| Message 1 | Message 2 |
| --- | --- |
| Message 3 | Message 4 |




Message 2
Send
To:
Cc:
Subject:
Security Vulnerability for ProjectX
It has come to my attention that ProjectX has a security vulnerability. The storage module does not encrypt sensitive customer details, and this could lead to a data breach, resulting in negative media attention.
My recommendation is to delay the launch until this security control is implemented. Do you concur?
VCEplus.com


Message 3
Send
To:
Cc:
Subject:
ALERT - Security Risks
ProjectX is not encrypting customer data!! This is probably a compliance issue. I really think the project should be put on hold until this critical vulnerability is fixed. The project team is not listening to me even though I told them they need to encrypt customer data. Can you please tell them this really needs to be fixed?
VCEplus.com




A security architect is working with a project team to deliver an important service that stores and processes customer banking details. The project, internally known as ProjectX, is due to launch its first set of features publicly within a week, but the team has not been able to implement encryption-at-rest of the customer records. The security architect is drafting an escalation email to senior leadership.

Which of the following BEST conveys the business impact for senior leadership?

A. Message 1
B. Message 2
C. Message 3
D. Message 4

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

**QUESTION 88**
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? (Select 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 89**
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:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 90**
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 91**
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

- End-to-end encryption of all inbound and outbound communication, including personal email and chat sessions that allow soldiers to securely communicate with families.
- Layer 7 inspection and TCP/UDP port restriction, including firewall rules to only allow TCP port 80 and 443 and approved applications
- A host-based whitelist of approved websites and applications that only allow mission-related tools and sites

The use of satellite communication to include multiple proxy servers to scramble the source IP address

Which of the following is of MOST concern in this scenario?

A. Malicious actors intercepting inbound and outbound communication to determine the scope of the mission
B. Family members posting geotagged images on social media that were received via email from soldiers
C. The effect of communication latency that may negatively impact real-time communication with mission control
D. The use of centrally managed military network and computers by soldiers when communicating with external parties

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 92**
A company has created a policy to allow employees to use their personally owned devices. The Chief Information 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 93**
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 94**
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 95**
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 96**
In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.

Which of the following strategies should the engineer recommended be approved FIRST?



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

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 97**
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? (Select 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 98**
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:** A
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 99**
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:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 100**
A system owner has requested support from data owners to evaluate options for the disposal of equipment containing sensitive data. Regulatory requirements state the data must be rendered unrecoverable via logical means or physically destroyed. Which of the following factors is the regulation intended to address?

A. Sovereignty
B. E-waste
C. Remanence
D. Deduplication



**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 101**
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 102**
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 103**
After several industry comnpetitors suffered data loss as a result of cyebrattacks, 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 104**
A company is not familiar with the risks associated with IPv6. The systems administrator wants to isolate IPv4 from IPv6 traffic between two different network segments. Which of the following should the company implement? (Select TWO)

A. Use an internal firewall to block UDP port 3544.
B. Disable network discovery protocol on all company routers.
C. Block IP protocol 41 using Layer 3 switches.
D. Disable the DHCPv6 service from all routers.
E. Drop traffic for ::/0 at the edge firewall.
F. Implement a 6in4 proxy server.

**Correct Answer:** DE
**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**
The Chief Executive Officers (CEOs) from two different companies are discussing the highly sensitive prospect of merging their respective companies together. Both have invited their Chief Information Officers (CIOs) to discern how they can securely and digitaly communicate, and the following criteria are collectively determined:

- Must be encrypted on the email servers and clients
- Must be OK to transmit over unsecure Internet connections

Which of the following communication methods would be BEST to recommend?

A. Force TLS between domains.
B. Enable STARTTLS on both domains.
C. Use PGP-encrypted emails.
D. Switch both domains to utilize DNSSEC.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**



**QUESTION 107**
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 108**

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. Create-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 109**
Given the following:

```
//TDO - should thid be odbc or jdbc?
var odbcString = getParameterByName ("queryString", "dbConnector");
doc.innerHTML = "DB connector: <b>" + odbcString + "</b>";
document.body.appendChild (doc);
```

Which of the following vulnerabilities is present in the above code snippet?

A. Disclosure of database credential
B. SQL-based string concatenation
C. DOM-based injection
D. Information disclosure in comments

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 110**
An organization is currently performing a market scan for managed security services and EDR capability. Which of the following business documents should be released to the prospective vendors in the first step of the process? (Select TWO).

A. MSA
B. RFP
C. NDA
D. RFI
E. MOU
F. RFQ

**Correct Answer:** CD
**Section: (none)**
**Explanation**



**Explanation/Reference:**
**QUESTION 111**
When reviewing KRIs of the email security appliance with the Chief Information Security Officer (CISO) of an insurance company, the security engineer notices the following:

| Month | Encrypted Email | Unencrypted Email | Contains PII |
|---|---|---|---|
| 1 | 200 | 0 | 0 |
| 2 | 230 | 10 | 5 |
| 3 | 185 | 15 | 10 |
| 4 | 198 | 60 | 40 |
| 5 | 204 | 75 | 45 |

Which of the following measures should the security engineer take to ensure PII is not intercepted in transit while also preventing interruption to business?

A. Quarantine emails sent to external domains containing PII and release after inspection.
B. Prevent PII from being sent to domains that allow users to sign up for free webmail.
C. Enable transport layer security on all outbound email communications and attachments.

D. Provide security awareness training regarding transmission of PII.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 112**
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:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 113**
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 tem 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 114**
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 115**
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 116**
A project manager is working with a software development group to collect and evaluate user stories related to the organization's internally designed CRM tool. After defining requirements, the project manager would like to validate the developer's interpretation and understanding of the user's request. Which of the following would BEST support this objective?



A. Peer review
B. Design review
C. Scrum
D. User acceptance testing
E. Unit testing

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 117**
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 118**
A technician is configuring security options on the mobile device manager for users who often utilize public Internet connections while travelling. After ensuring that full disk encryption is enabled, which of the following security measures should the technician take? (Choose two.)

A. Require all mobile device backups to be encrypted
B. Ensure all mobile devices back up using USB OTG
C. Issue a remote wipe of corporate and personal partitions
D. Restrict devices from making long-distance calls during business hours
E. Implement an always-on VPN

**Correct Answer:** CE
**Section: (none)**
**Explanation**



**Explanation/Reference:**

**QUESTION 119**
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:** EF
**Section: (none)**
**Explanation**

**Explanation/Reference:**


https://www.vceplus.com/