

CAS-003.166q

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

CAS-003



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vceplus.com>

**CompTIA Advanced Security Practitioner (CASP)**

**Exam A**

**QUESTION 1**

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

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

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

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



<https://vceplus.com>

Which of the following is the engineer implementing?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

<https://vceplus.com>

## Explanation/Reference:

### QUESTION 2

An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.

```
[00:00:09] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1"
200 6863
"http://search.company.com/search/cgi/search.cgi?qs=download=&dom=s&offset=0&hits=10&switch=0&f=us"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:12] "GET /js/master.js HTTP/1.1" 200 2263
"http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
[00:00:22] "GET /internet/index.html HTTP/1.1" 200 6792
"http://www.company.com/video/streaming/http.html"
"Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413
Debian/1.6-5"
[00:00:25] "GET /showFile.action?fileName=<script> alert("an error has
occurred, please send your username and password to me@example.com")
</script> 200
[00:00:27] "GET /contracts.html HTTP/1.0" 200 4595 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-
WebCrawler/2.1-pre2 (ashen@company.net)"
[00:00:29] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096
"http://www.company.com/downloads/freeware/webdevelopment/15.html"
"Mozilla/4.7 [en]C-SYMPA (Win95; U)"
[00:00:30] "GET /pics/wpaper.gif HTTP/1.0" 200 6248
"http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"
```

Which of the following types of attack vector did the penetration tester use?

- A. SQL injection
- B. CSRF
- C. Brute force
- D. XSS
- E. TOC/TOU

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 3

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 4

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 5**

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 6**

After embracing a BYOD policy, a company is faced with new security challenges from unmanaged mobile devices and laptops. The company's IT department has seen a large number of the following incidents:

- Duplicate IP addresses
- Rogue network devices
- Infected systems probing the company's network

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

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

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

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 8**

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**

**QUESTION 9**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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 10**

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 11**

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

**QUESTION 12**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

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 13

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

- A. Install a HIPS on the web servers
- B. Disable inbound traffic from offending sources
- C. Disable SNMP on the web servers
- D. Install anti-DDoS protection in the DMZ

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 14

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 15**

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 scarce funding to address cybersecurity concerns

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 16**

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 17

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:**

<https://vceplus.com>

### QUESTION 18

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

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 19

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



<https://vceplus.com>

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

<https://vceplus.com>

- 3. Research threat intelligence and potential adversaries
- 4. Utilize threat intelligence to apply Big Data techniques
- C.
  - 1. Obtain the latest IOCs from the open source repositories
  - 2. Perform a sweep across the network to identify positive matches
  - 3. Sandbox any suspicious files
  - 4. Notify the CERT team to apply a future proof threat model
- D.
  - 1. Analyze the current threat intelligence
  - 2. Utilize information sharing to obtain the latest industry IOCs
  - 3. Perform a sweep across the network to identify positive matches
  - 4. Apply machine learning algorithms

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 21

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

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

Which of the following commands would have provided this output?

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



**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 22

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

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

E. Reject

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 23

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 24

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

- A. Black box testing
- B. Gray box testing
- C. Code review
- D. Social engineering
- E. Vulnerability assessment
- F. Pivoting
- G. Self-assessment

- H. White teaming
- I. External auditing

**Correct Answer:** AEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 25

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

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

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

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

- A. VLAN201, VLAN202, VLAN400

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 28

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 29

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 30**

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 31**

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 32**

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 33

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 34

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

<https://vceplus.com>

- C. Verifying system design documentation
- D. Using a SRTM

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 35

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 36

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



<https://vceplus.com>

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 37

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

<https://vceplus.com>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 39**

A 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 40**

<https://vceplus.com>

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 41

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 42

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 43

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 44

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

```
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 80
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 636
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 5800
PERMIT TCP FROM 74.23.2.4 TO 192.168.20.20 PORT 1433
```

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 45

An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources. Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

- A. Isolate the systems on their own network
- B. Install a firewall and IDS between systems and the LAN
- C. Employ own stratum-0 and stratum-1 NTP servers
- D. Upgrade the software on critical systems
- E. Configure the systems to use government-hosted NTP servers

**Correct Answer:** BE

**Section:** (none)

## Explanation

### Explanation/Reference:

#### QUESTION 46

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

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

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

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



**Correct Answer:** BEH

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 47

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

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

<https://vceplus.com>

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 48**

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

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

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 49**

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

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

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:



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

**QUESTION 51**

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<br>10:00:04 | 10.14.34.55  | aaaaa    | Phone            | Widget1  | None left           |
| Monday<br>10:00:04 | 10.14.34.55  | bbbbb    | Phone            | Widget1  | None left           |
| Monday<br>10:00:05 | 10.14.34.55  | cccc     | Phone            | Widget1  | ../etc/passwd       |
| Monday<br>10:01:03 | 10.14.34.55  | dddd     | Phone            | Widget1  | None left           |
| Monday<br>10:01:04 | 10.14.34.55  | eeee     | Phone            | Widget1  | None left           |
| Monday<br>10:01:05 | 10.14.34.55  | ffff     | Phone            | Widget1  | 1=1                 |
| Monday<br>10:03:05 | 172.16.34.20 | Joe      | Phone            | Widget30 | Love the<br>Widget! |
| Monday<br>10:04:01 | 10.14.34.55  | ggggg    | Phone            | Widget1  | <script>            |
| Monday<br>10:05:05 | 10.14.34.55  | hhhhh    | Phone            | Widget1  | wget cookie         |
| Monday<br>10:05:05 | 10.14.34.55  | iiii     | Phone            | Widget1  | None left           |
| Monday<br>10:05:06 | 10.14.34.55  | llll     | 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 52**

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 confidentiality of a database containing PII and medical data from clients. Based on the controls classification, which of the following controls would BEST meet these requirements?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 53

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 54

A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded.

Which of the following should be used to identify weak processes and other vulnerabilities?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 55

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

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

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



**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 56

A network engineer is attempting to design-in resiliency characteristics for an enterprise network's VPN services.

If the engineer wants to help ensure some resilience against zero-day vulnerabilities exploited against the VPN implementation, which of the following decisions would BEST support this objective?

- A. Implement a reverse proxy for VPN traffic that is defended and monitored by the organization's SOC with near-real-time alerting to administrators.
- B. Subscribe to a managed service provider capable of supporting the mitigation of advanced DDoS attacks on the enterprise's pool of VPN concentrators.

<https://vceplus.com>

- C. Distribute the VPN concentrators across multiple systems at different physical sites to ensure some backup services are available in the event of primary site loss.
- D. Employ a second VPN layer concurrently where the other layer's cryptographic implementation is sourced from a different vendor.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 57**

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

| Corporate Network |             | Secure Network |              |
|-------------------|-------------|----------------|--------------|
| james.bond        | asHU\$\$1bg | jbond          | asHU\$\$1bg  |
| tom.jones         | wit4njyt%!  | tom.jones      | wit4njyt%!om |
| dade.murphy       | mUrpHTIME7  | d.murph3       | t%w38T9)n    |
| herbie.hancock    | hh2016!#    | hhanco         | hh2016!#2    |
| suzy.smith        | 1LI*#HFadf  | ssmith         | 1LI*#HFadf   |

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

A Chief Information Security Officer (CISO) is reviewing and revising system configuration and hardening guides that were developed internally and have been used several years to secure the organization's systems. The CISO knows improvements can be made to the guides.

Which of the following would be the BEST source of reference during the revision process?

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 59**

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

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

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

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 60**

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

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

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



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 61**

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

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

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

**Correct Answer:** A

<https://vceplus.com>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

**SIMULATION**

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

The command window will be provided along with root access. You are connected via a secure shell with root access.

You may query help for a list of commands.

**Instructions:**

You need to disable and turn off unrelated services and processes.

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



```
Command Prompt Window - [X]
[root@comptia-test ~]# help
Available Commands

kill -9 <pid>
ps -A
chkconfig --list
chkconfig --level 3 <service name>
<on/off>
service <service name> <start|stop>

[root@comptia-test ~]#
```

**Correct Answer:** See the explanation below

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

<https://vceplus.com>

In Order to deactivate web services, database services and print service, we can do following things

1) deactivate its services

```
/etc/init.d/apache2 stop
```

```
/etc/init.d/mysqld stop
```

2) close ports for these services

Web Server

```
iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECT
```

```
service iptables save
```

```
iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECT
```

```
service iptables save
```

```
iptables -I INPUT -p tcp -m tcp --dport <<port number>> -j REJECT
```

```
service iptables save
```

3) Kill the process any running for the sameps -aef|grep mysql kill -9 <<process id>>

### QUESTION 63

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 64

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

User IP space: 192.168.1.0/24

Server IP space: 192.168.192.0/25

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

Which of the following should the engineer do?

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 65

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

During a security assessment, activities were divided into two phases; internal and external exploitation. The security assessment team set a hard time limit on external activities before moving to a compromised box within the enterprise perimeter.

Which of the following methods is the assessment team most likely to employ NEXT?

- A. Pivoting from the compromised, moving laterally through the enterprise, and trying to exfiltrate data and compromise devices.

- B. Conducting a social engineering attack attempt with the goal of accessing the compromised box physically.
- C. Exfiltrating network scans from the compromised box as a precursor to social media reconnaissance
- D. Open-source intelligence gathering to identify the network perimeter and scope to enable further system compromises.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 67

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

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

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



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 68

While attending a meeting with the human resources department, an organization's information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.

Additionally, each password has specific complexity requirements and different expiration time frames.

Which of the following would be the BEST solution for the information security officer to recommend?

- A. Utilizing MFA
- B. Implementing SSO
- C. Deploying 802.1X

- D. Pushing SAML adoption
- E. Implementing TACACS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 69**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 70**

Given the following code snippet:

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

Which of the following failure modes would the code exhibit?

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



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 71

A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:

- Data must be encrypted at rest.
- The device must be disabled if it leaves the facility. ▪

The device must be disabled when tampered with.

Which of the following technologies would BEST support these requirements? (Select two.)

- A. eFuse

<https://vceplus.com>

- B. NFC
- C. GPS
- D. Biometric
- E. USB 4.1
- F. MicroSD

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 72

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

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 73**

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

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

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

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 74

Given the following output from a security tool in Kali:

[12:17:41] dumping options:

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

state: <8>

lineo: <56>

literals: <74>

sequences: [34]

symbols: [0]

req\_del: <200>

mseq\_len: <1024>

plugin: <none>

s\_syms: <0>

literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdhj9]



<https://vceplus.com>

<https://vceplus.com>

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 75

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

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

Which of the following exercises has the CEO requested?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 76

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 compiled 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 77**

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 78**

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 79

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

<https://vceplus.com>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

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 81**

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

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 82

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 83

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

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

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

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

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 86**

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

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

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

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

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 87**

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



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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

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

- Encrypt all traffic between the network engineer and critical devices.
  - Segregate the different networking planes as much as possible. ▪
- Do not let access ports impact configuration tasks.

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



#### QUESTION 89

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

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 90

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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 91

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

<https://vceplus.com>

**Explanation/Reference:**

**QUESTION 92**

Click on the exhibit buttons to view the four messages.

**Message 1**

**Message 2**

**Message 3**

**Message 4**



Message 1

Send

To:

Cc:

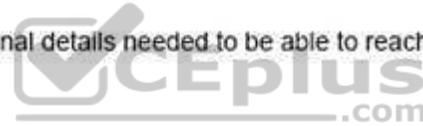
Subject:

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 originally 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 agrees 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?



Message 2

Send

To:

Cc:

Subject:

Security Vulnerability for ProjectX

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

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



**Message 3**

|             |          |                        |
|-------------|----------|------------------------|
| <b>Send</b> | To:      |                        |
|             | Cc:      |                        |
|             | Subject: | ALERT - Security Risks |

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



**Message 4**

|             |          |                    |
|-------------|----------|--------------------|
| <b>Send</b> | To:      |                    |
|             | Cc:      |                    |
|             | 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 obviusle 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 93

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 94

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 95

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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 96

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 97

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:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 98

Given the following code snippet:

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

Of which of the following is this snippet an example?

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

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 99

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**

<https://vceplus.com>

**Explanation/Reference:**

**QUESTION 100**

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 101**

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 102**

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

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

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

Which of the following BEST describes the security problem?

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



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 103

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

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

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

- A. VTC
- B. VRRP
- C. VLAN

<https://vceplus.com>

- D. VDI
- E. VPN
- F. Telnet

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 104**

A project manager is working with a team that is tasked to develop software applications in a structured environment and host them in a vendor's cloud-based infrastructure. The organization will maintain responsibility for the software but will not manage the underlying server applications. Which of the following does the organization plan to leverage?

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



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 105**

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

- A. Code repositories
- B. Security requirements traceability matrix
- C. Software development lifecycle
- D. Data design diagram
- E. Roles matrix
- F. Implementation guide

<https://vceplus.com>

**Correct Answer:** F

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 106**

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 107**

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 108**

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 109**

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 110**

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 111

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

Which of the following exercise types should the analyst perform?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://vceplus.com>

**QUESTION 112**

In the past, the risk committee at Company A has shown an aversion to even minimal amounts of risk acceptance. A security engineer is preparing recommendations regarding the risk of a proposed introducing legacy ICS equipment. The project will introduce a minor vulnerability into the enterprise. This vulnerability does not significantly expose the enterprise to risk and would be expensive against.

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

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 114**

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

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

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

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 115

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

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

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 116**

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 117**

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:**

<https://vceplus.com>

**QUESTION 118**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 119**

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

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

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

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?

<https://vceplus.com>

- A. MOU
- B. OLA
- C. BPA
- D. NDA

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 121

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 122

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

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

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 123**

Developers are working on a new feature to add to a social media platform. The new feature involves users uploading pictures of what they are currently doing. The data privacy officer (DPO) is concerned about various types of abuse that might occur due to this new feature. The DPO 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 124**

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



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

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

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

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 125

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 126

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

<https://vceplus.com>

- 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 127

Following a recent data breach, a company has hired a new Chief Information Security Officer (CISO). The CISO is very concerned about the response time to the previous breach and wishes to know how the security team expects to react to a future attack. Which of the following is the BEST method to achieve this goal while minimizing disruption?

- A. Perform a black box assessment
- B. Hire an external red team audit
- C. Conduct a tabletop exercise.
- D. Recreate the previous breach.
- E. Conduct an external vulnerability assessment.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 128

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 129

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

<https://vceplus.com>

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 130**

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

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

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 131**

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:**

<https://vceplus.com>

**QUESTION 132**

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 133**

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

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

Which of the following tools would BEST meet these requirements?

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 134**

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 135**

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 136

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 ABCDEFGHIJKLMNOPQRSTUVWXYZ&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 137

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 138**

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 139**

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

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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://vceplus.com>

#### QUESTION 140

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

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

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

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

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



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 141

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 142**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 143**

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

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 144**

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

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

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145**

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

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

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 146**

A security analyst is classifying data based on input from data owners and other stakeholders. The analyst has identified three data types:

1. Financially sensitive data
2. Project data

### 3. Sensitive project data

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

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 147

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

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

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

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

D. After successfully using a watering hole attack to deliver an exploit to a machine, which belongs to an employee of the contractor, an attacker gained access to a corporate laptop. With this access, the attacker then established a remote session over a VPN connection with the server hosting the database of sensitive information.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 148

A networking administrator was recently promoted to security administrator in an organization that handles highly sensitive data. The Chief Information Security Officer (CISO) has just asked for all IT security personnel to review a zero-day vulnerability and exploit for specific application servers to help mitigate the organization's exposure to that risk. Which of the following should the new security administrator review to gain more information? (Choose three.)

- A. CVE database
- B. Recent security industry conferences
- C. Security vendor pages
- D. Known vendor threat models
- E. Secure routing metrics
- F. Server's vendor documentation
- G. Verified security forums
- H. NetFlow analytics



**Correct Answer:** CEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 149

A company has decided to replace all the T-1 uplinks at each regional office and move away from using the existing MPLS network. All regional sites will use highspeed connections and VPNs to connect back to the main campus. Which of the following devices would MOST likely be added at each location?

- A. SIEM
- B. IDS/IPS
- C. Proxy server
- D. Firewall

E. Router

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 150

An external red team is brought into an organization to perform a penetration test of a new network-based application. The organization deploying the network application wants the red team to act like remote, external attackers, and instructs the team to use a black-box approach. Which of the following is the BEST methodology for the red team to follow?

- A. Run a protocol analyzer to determine what traffic is flowing in and out of the server, and look for ways to alter the data stream that will result in information leakage or a system failure.
- B. Send out spear-phishing emails against users who are known to have access to the network-based application, so the red team can go on-site with valid credentials and use the software.
- C. Examine the application using a port scanner, then run a vulnerability scanner against open ports looking for known, exploitable weaknesses the application and related services may have.
- D. Ask for more details regarding the engagement using social engineering tactics in an attempt to get the organization to disclose more information about the network application to make attacks easier.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 151

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 152**

A regional business is expecting a severe winter storm next week. The IT staff has been reviewing corporate policies on how to handle various situations and found some are missing or incomplete. After reporting this gap in documentation to the information security manager, a document is immediately drafted to move various personnel to other locations to avoid downtime in operations. This is an example of:

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

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 153**

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

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



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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 154

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 155**

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

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

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 156

A university's help desk is receiving reports that Internet access on campus is not functioning. The network administrator looks at the management tools and sees the 1Gbps Internet is completely saturated with ingress traffic. The administrator sees the following output on the Internet router:

```
13:45.12857 156.34.99.54.2343 > 192.168.23.78.443 S 37483928:37483928 (0) win 16384
13:45.12890 145.24.78.34.2343 > 192.168.23.78.443 S 58457854:58457854 (0) win 36638
13:45.12890 89.25.68.12.2343 > 192.168.23.78.443 S 32987488:32987488 (0) win 25411
13:45.12923 178.78.189.1.2343 > 192.168.23.78.443 S 36214896:36214869 (0) win 12225
13:45.12934 147.22.98.156.2343 > 192.168.23.78.443 S 21558745:21558745 (0) win 32663
13:45.12956 121.45.56.79.2343 > 192.168.23.78.443 S 86441289:86441289 (0) win 33225
13:45.12989 126.88.125.117.2343 > 192.168.23.78.443 S 48741688:48741688 (0) win 18412
```

The administrator calls the university's ISP for assistance, but it takes more than four hours to speak to a network engineer who can resolve the problem. Based on the information above, which of the following should the ISP engineer do to resolve the issue?

- A. The ISP engineer should null route traffic to the web server immediately to restore Internet connectivity. The university should implement a remotely triggered black hole with the ISP to resolve this more quickly in the future.
- B. A university web server is under increased load during enrollment. The ISP engineer should immediately increase bandwidth to 2Gbps to restore Internet connectivity. In the future, the university should pay for more bandwidth to handle spikes in web server traffic.
- C. The ISP engineer should immediately begin blocking IP addresses that are attacking the web server to restore Internet connectivity. In the future, the university should install a WAF to prevent this attack from happening again.
- D. The ISP engineer should begin refusing network connections to the web server immediately to restore Internet connectivity on campus. The university should purchase an IPS device to stop DDoS attacks in the future.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 157**

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

- A. Perform a penetration test.
- B. Conduct a regulatory audit.
- C. Hire a third-party consultant.
- D. Define the threat model.
- E. Review the existing BIA.
- F. Perform an attack path analysis.

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 158**

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

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<https://vceplus.com>

**QUESTION 159**

A manufacturing company recently recovered from an attack on its ICS devices. It has since reduced the attack surface by isolating the affected components. The company now wants to implement detection capabilities. It is considering a system that is based on machine learning. Which of the following features would BEST describe the driver to adopt such nascent technology over mainstream commercial IDSs?

- A. Trains on normal behavior and identifies deviations therefrom
- B. Identifies and triggers upon known bad signatures and behaviors
- C. Classifies traffic based on logical protocols and messaging formats
- D. Automatically reconfigures ICS devices based on observed behavior

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<https://vceplus.com>

**QUESTION 160**

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

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

**Correct Answer:** DE

<https://vceplus.com>

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 161**

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

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

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

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



**Correct Answer: BD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 162**

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

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 163**

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

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

- A. The SSH keys were given to another department.
- B. A MITM attack is being performed by an APT.
- C. The terminal emulator does not support SHA-256.
- D. An incorrect username or password was entered.
- E. A key rotation has occurred as a result of an incident.
- F. The workstation is not syncing with the correct NTP server.



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 164**

Following a recent outage, a systems administrator is conducting a study to determine a suitable bench stock on server hard drives. Which of the following metrics is MOST valuable to the administrator in determining how many hard drives to keep-on hand?

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

**Correct Answer:** C

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 165**

A school contracts with a vendor to devise a solution that will enable the school library to lend out tablet computers to students while on site. The tablets must adhere to string security and privacy practices. The school's key requirements are to:

- Maintain privacy of students in case of loss
- Have a theft detection control in place
- Be compliant with defined disability requirements
- Have a four-hour minimum battery life

Which of the following should be configured to BEST meet the requirements? (Choose two.)

- A. Remote wiping
- B. Geofencing
- C. Antivirus software
- D. TPM
- E. FDE
- F. Tokenization



**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 166**

A project manager is working with a software development group to collect and evaluate user scenarios related to the organization's internally designed data analytics tool. While reviewing stakeholder input, the project manager would like to formally document the needs of the various stakeholders and the associated organizational compliance objectives supported by the project.

Which of the following would be MOST appropriate to use?

- A. Roles matrix
- B. Peer review
- C. BIA

D. SRTM

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



<https://vceplus.com>



<https://vceplus.com>