CAS-002 Dumps

CompTIA Advanced Security Practitioner (CASP)

https://www.certleader.com/CAS-002-dumps.html

NEW QUESTION 1
An administrator wants to enable policy based flexible mandatory access controls on an open source OS to prevent abnormal application modifications or executions. Which of the following would BEST accomplish this?

A. Access control lists
B. SELinux
C. IPtables firewall
D. HIPS

Answer: B

NEW QUESTION 2
Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software from running on mobile devices?

A. Single sign-on
B. Identity propagation
C. Remote attestation
D. Secure code review

Answer: C

NEW QUESTION 3
select id, firstname, lastname from authors User input= firstname= Hack;man lastname=Johnson
Which of the following types of attacks is the user attempting?

A. XML injection
B. Command injection
C. Cross-site scripting
D. SQL injection

Answer: D

NEW QUESTION 4
In order to reduce costs and improve employee satisfaction, a large corporation is creating a BYOD policy. It will allow access to email and remote connections to the corporate enterprise from personal devices; provided they are on an approved device list. Which of the following security measures would be MOST effective in securing the enterprise under the new policy? (Select TWO).

A. Provide free email software for personal devices.
B. Encrypt data in transit for remote access.
C. Require smart card authentication for all devices.
D. Implement NAC to limit insecure devices access.
E. Enable time of day restrictions for personal devices.

Answer: BD

NEW QUESTION 5
Ann, a systems engineer, is working to identify an unknown node on the corporate network. To begin her investigative work, she runs the following nmap command string:
user@hostname:~$ sudo nmap −O 192.168.1.54
Based on the output, nmap is unable to identify the OS running on the node, but the following ports are open on the device:
TCP/22 TCP/111 TCP/512-514 TCP/2049
TCP/32778
Based on this information, which of the following operating systems is MOST likely running on the unknown node?

A. Linux
B. Windows
C. Solaris
D. OSX

Answer: C

NEW QUESTION 6
A security manager has received the following email from the Chief Financial Officer (CFO):
"While I am concerned about the security of the proprietary financial data in our ERP application, we have had a lot of turnover in the accounting group and I am having a difficult time meeting our monthly performance targets. As things currently stand, we do not allow employees to work from home but this is something I am willing to allow so we can get back on track. What should we do first to securely enable this capability for my group?"
Based on the information provided, which of the following would be the MOST appropriate response to the CFO?

A. Remote access to the ERP tool introduces additional security vulnerabilities and should not be allowed.
B. Allow VNC access to corporate desktops from personal computers for the users working from home.
C. Allow terminal services access from personal computers after the CFO provides a list of the users working from home.
D. Work with the executive management team to revise policies before allowing any remote access.

Answer: D

NEW QUESTION 7
A security manager for a service provider has approved two vendors for connections to the
service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?

A. Memorandum of Agreement
B. Interconnection Security Agreement
C. Non-Disclosure Agreement
D. Operating Level Agreement

Answer: B

NEW QUESTION 8
An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?

A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs

Answer: B

NEW QUESTION 9
A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?

A. Determining how to install HIPS across all server platforms to prevent future incidents
B. Preventing the ransomware from re-infecting the server upon restore
C. Validating the integrity of the deduplicated data
D. Restoring the data will be difficult without the application configuration

Answer: D

NEW QUESTION 10
The risk manager has requested a security solution that is centrally managed, can easily be updated, and protects end users' workstations from both known and unknown malicious attacks when connected to either the office or home network. Which of the following would BEST meet this requirement?

A. HIPS
B. UTM
C. Antivirus
D. NIPS
E. DLP

Answer: A

NEW QUESTION 10
An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

A. LDAP/S
B. SAML
C. NTLM
D. OAUTH
E. Kerberos

Answer: BE

NEW QUESTION 11
A developer has implemented a piece of client-side JavaScript code to sanitize a user's provided input to a web page login screen. The code ensures that only the upper case and lower case letters are entered in the username field, and that only a 6-digit PIN is entered in the password field. A security administrator is concerned with the following web server log:
10.235.62.11 – - [02/Mar/2014:06:13:04] "GET
/site/script.php?user=admin&pass=pass%20or%201=1 HTTP/1.1" 200 5724
Given this log, which of the following is the security administrator concerned with and which fix should be implemented by the developer?

A. The security administrator is concerned with nonprintable characters being used to gain administrative access, and the developer should strip all nonprintable characters.
B. The security administrator is concerned with XSS, and the developer should normalize Unicode characters on the browser side.
C. The security administrator is concerned with SQL injection, and the developer should implement server side input validation.
D. The security administrator is concerned that someone may log on as the administrator, and the developer should ensure strong passwords are enforced.

Answer: C

NEW QUESTION 13

A large organization has recently suffered a massive credit card breach. During the months of Incident Response, there were multiple attempts to assign blame for whose fault it was that the incident occurred. In which part of the incident response phase would this be addressed in a controlled and productive manner?

A. During the Identification Phase
B. During the Lessons Learned phase
C. During the Containment Phase
D. During the Preparation Phase

Answer: B

NEW QUESTION 16

Two separate companies are in the process of integrating their authentication infrastructure into a unified single sign-on system. Currently, both companies use an AD backend and two factor authentication using TOTP. The system administrators have configured a trust relationship between the authentication backend to ensure proper process flow. How should the employees request access to shared resources before the authentication integration is complete?

A. They should logon to the system using the username concatenated with the 6-digit code and their original password.
B. They should logon to the system using the newly assigned global username: first.lastname#### where #### is the second factor code.
C. They should use the username format: LAN\first.lastname together with their original password and the next 6-digit code displayed when the token button is depressed.
D. They should use the username format: first.lastname@company.com, together with a password and their 6-digit code.

Answer: D

NEW QUESTION 18

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level. Various security requirements were also documented. Organize the following security requirements into the correct hierarchy required for an SRTM.
Requirement 1: The system shall provide confidentiality for data in transit and data at rest. Requirement 2: The system shall use SSL, SSH, or SCP for all data transport. Requirement 3: The system shall implement a file-level encryption scheme.
Requirement 4: The system shall provide integrity for all data at rest. Requirement 5: The system shall perform CRC checks on all files.

A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5
B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5under 4
C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under4; Level 3: Requirement 3 under 2
D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Answer: B

NEW QUESTION 19

The security engineer receives an incident ticket from the helpdesk stating that DNS lookup requests are no longer working from the office. The network team has ensured that Layer 2 and Layer 3 connectivity are working. Which of the following tools would a security engineer use to make sure the DNS server is listening on port 53?

A. PING
B. NESSUS
C. NSLOOKUP
D. NMAP

Answer: D

NEW QUESTION 22

A developer is determining the best way to improve security within the code being developed. The developer is focusing on input fields where customers enter their credit card details. Which of the following techniques, if implemented in the code, would be the MOST effective in protecting the fields from malformed input?

A. Client side input validation
B. Stored procedure
C. Encrypting credit card details
D. Regular expression matching

Answer: D

NEW QUESTION 23

A system administrator needs to meet the maximum amount of security goals for a new DNS infrastructure. The administrator deploys DNSSEC extensions to the domain names
and infrastructure. Which of the following security goals does this meet? (Select TWO).

A. Availability
B. Authentication
C. Integrity
D. Confidentiality
E. Encryption

Answer: BC

NEW QUESTION 25

The source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of

the following methods would BEST help with this process? (Select TWO).

A. Retrieve source system image from backup and run file comparison analysis on the two images.
B. Parse all images to determine if extra data is hidden using steganography.
C. Calculate a new hash and compare it with the previously captured image hash.
D. Ask desktop support if any changes to the images were made.
E. Check key system files to see if date/time stamp is in the past six months.

Answer: AC

NEW QUESTION 26
A security administrator wants to calculate the ROI of a security design which includes the purchase of new equipment. The equipment costs $50,000 and it will take 50 hours to install and configure the equipment. The administrator plans to hire a contractor at a rate of
$100/hour to do the installation. Given that the new design and equipment will allow the company to increase revenue and make an additional $100,000 on the first year, which of the following is the ROI expressed as a percentage for the first year?

A. -45 percent
B. 5.5 percent
C. 45 percent
D. 82 percent

Answer: D

NEW QUESTION 29
The Chief Information Officer (CIO) is reviewing the IT centric BIA and RA documentation. The documentation shows that a single 24 hours downtime in a critical business function will cost the business $2.3 million. Additionally, the business unit which depends on the critical business function has determined that there is a high probability that a threat will materialize based on historical data. The CIO's budget does not allow for full system hardware replacement in case of a catastrophic failure, nor does it allow for the purchase of additional compensating controls. Which of the following should the CIO recommend to the finance director to minimize financial loss?

A. The company should mitigate the risk.
B. The company should transfer the risk.
C. The company should avoid the risk.
D. The company should accept the risk.

Answer: B

NEW QUESTION 33
The Chief Executive Officer (CEO) of a company that allows telecommuting has challenged the Chief Security Officer's (CSO) request to harden the corporate network's perimeter. The CEO argues that the company cannot protect its employees at home, so the risk at work is no different. Which of the following BEST explains why this company should proceed with protecting its corporate network boundary?

A. The corporate network is the only network that is audited by regulators and customers.
B. The aggregation of employees on a corporate network makes it a more valuable target for attackers.
C. Home networks are unknown to attackers and less likely to be targeted directly.
D. Employees are more likely to be using personal computers for general web browsing when they are at home.

Answer: B

NEW QUESTION 34
A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?

A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted dat
B. Attempt to exploit via the proof-of-concept cod
C. Consider remediation options.
D. Hire an independent security consulting agency to perform a penetration test of the web server
E. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
F. Review vulnerability write-ups posted on the Interne
G. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
H. Notify all customers about the threat to their hosted dat
I. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.

Answer: A

NEW QUESTION 35
A mature organization with legacy information systems has incorporated numerous new processes and dependencies to manage security as its networks and infrastructure are modernized. The Chief Information Office has become increasingly frustrated with frequent releases, stating that the organization needs everything to work completely, and the vendor should already have those desires built into the software product. The vendor has been in constant communication with personnel and groups within the organization to understand its business process and capture new software requirements from users. Which of the following methods of software development is this organization's configuration management process using?

A. Agile
B. SDL
C. Waterfall
D. Joint application development

Answer: A

NEW QUESTION 36
The Chief Executive Officer (CEO) of an Internet service provider (ISP) has decided to limit the company's contribution to worldwide Distributed Denial of Service (DDoS) attacks. Which of the following should the ISP implement? (Select TWO).

A. Block traffic from the ISP's networks destined for blacklisted IPs.
B. Prevent the ISP's customers from querying DNS servers other than those hosted by the ISP.
C. Scan the ISP's customer networks using an up-to-date vulnerability scanner.
D. Notify customers when services they run are involved in an attack.
E. Block traffic with an IP source not allocated to customers from exiting the ISP's network.

Answer: DE

NEW QUESTION 38
A security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).

A. Managed security service
B. Memorandum of understanding
C. Quality of service
D. Network service provider
E. Operating level agreement

Answer: BE

NEW QUESTION 39
A security administrator wants to prevent sensitive data residing on corporate laptops and desktops from leaking outside of the corporate network. The company has already implemented full-disk encryption and has disabled all peripheral devices on its desktops and laptops. Which of the following additional controls MUST be implemented to minimize the risk of data leakage? (Select TWO).

A. A full-system backup should be implemented to a third-party provider with strong encryption for data in transit.
B. A DLP gateway should be installed at the company border.
C. Strong authentication should be implemented via external biometric devices.
D. Full-tunnel VPN should be required for all network communication.
E. Full-drive file hashing should be implemented with hashes stored on separate storage.
F. Split-tunnel VPN should be enforced when transferring sensitive data.

Answer: BD

NEW QUESTION 41
A security administrator is shown the following log excerpt from a Unix system:
2013 Oct 10 07:14:57 web14 sshd[1632]: Failed password for root from 198.51.100.23 port
37914 ssh2
2013 Oct 10 07:14:57 web14 sshd[1635]: Failed password for root from 198.51.100.23 port
37915 ssh2
2013 Oct 10 07:14:58 web14 sshd[1638]: Failed password for root from 198.51.100.23 port
37916 ssh2
2013 Oct 10 07:15:59 web14 sshd[1640]: Failed password for root from 198.51.100.23 port
37918 ssh2
2013 Oct 10 07:16:00 web14 sshd[1641]: Failed password for root from 198.51.100.23 port
37920 ssh2
2013 Oct 10 07:16:00 web14 sshd[1642]: Successful login for root from 198.51.100.23 port
37924 ssh2
Which of the following is the MOST likely explanation of what is occurring and the BEST immediate response? (Select TWO).

A. An authorized administrator has logged into the root account remotely.
B. The administrator should disable remote root logins.
C. Isolate the system immediately and begin forensic analysis on the host.
D. A remote attacker has compromised the root account using a buffer overflow in sshd.
E. A remote attacker has guessed the root password using a dictionary attack.
F. Use iptables to immediately DROP connections from the IP 198.51.100.23.
G. A remote attacker has compromised the private key of the root account.
H. Change the root password immediately to a password not found in a dictionary.

Answer: CE

NEW QUESTION 43
A popular commercial virtualization platform allows for the creation of virtual hardware. To virtual machines, this virtual hardware is indistinguishable from real hardware. By implementing virtualized TPMs, which of the following trusted system concepts can be implemented?

A. Software-based root of trust
B. Continuous chain of trust
C. Chain of trust with a hardware root of trust
D. Software-based trust anchor with no root of trust

Answer: C

NEW QUESTION 44
Which of the following describes a risk and mitigation associated with cloud data storage?

A. Risk: Shared hardware caused data leakageMitigation: Strong encryption at rest
B. Risk: Offsite replicationMitigation: Multi-site backups
C. Risk: Data loss from de-duplicationMitigation: Dynamic host bus addressing
D. Risk: Combined data archivingMitigation: Two-factor administrator authentication

Answer: A

NEW QUESTION 48
The Information Security Officer (ISO) is reviewing a summary of the findings from the last COOP tabletop exercise. The Chief Information Officer (CIO) wants to determine which additional controls must be implemented to reduce the risk of an extended customer service outage due to the VoIP system being unavailable. Which of the following BEST describes the scenario presented and the document the ISO is reviewing?

A. The ISO is evaluating the business implications of a recent telephone system failure within the BIA.
B. The ISO is investigating the impact of a possible downtime of the messaging system within the RA.
C. The ISO is calculating the budget adjustment needed to ensure audio/video system redundancy within the RFQ.
D. The ISO is assessing the effect of a simulated downtime involving the telecommunication system within the AAR.

Answer: D

NEW QUESTION 51
Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields
B. Reverse engineering any thick client software that has been provided for the test
C. Undertaking network-based denial of service attacks in production environment
D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks
E. Running a vulnerability scanning tool to assess network and host weaknesses

Answer: C

NEW QUESTION 54
An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.
B. Ensure the SaaS provider supports encrypted password transmission and storage.
C. Ensure the SaaS provider supports secure hash file exchange.
D. Ensure the SaaS provider supports role-based access control.
E. Ensure the SaaS provider supports directory services federation.

Answer: E

NEW QUESTION 58
An organization is concerned with potential data loss in the event of a disaster, and created a backup datacenter as a mitigation strategy. The current storage method is a single NAS used by all servers in both datacenters. Which of the following options increases data availability in the event of a datacenter failure?

A. Replicate NAS changes to the tape backups at the other datacenter.
B. Ensure each server has two HBAs connected through two routes to the NAS.
C. Establish deduplication across diverse storage paths.
D. Establish a SAN that replicates between datacenters.

Answer: D

NEW QUESTION 63
The risk manager is reviewing a report which identifies a requirement to keep a business critical legacy system operational for the next two years. The legacy system is out of support because the vendor and security patches are no longer released. Additionally, this is a proprietary embedded system and little is documented and known about it. Which of the following should the Information Technology department implement to reduce the security risk from a compromise of this system?

A. Virtualize the system and migrate it to a cloud provider.
B. Segment the device on its own secure network.
C. Install an antivirus and HIDS on the system.
D. Hire developers to reduce vulnerabilities in the code.

Answer: B

NEW QUESTION 66
Company ABC's SAN is nearing capacity, and will cause costly downtimes if servers run out disk space. Which of the following is a more cost effective alternative to buying a new SAN?

A. Enable multipath to increase availability
B. Enable deduplication on the storage pools
C. Implement snapshots to reduce virtual disk size

D. Implement replication to offsite datacenter

Answer: B

NEW QUESTION 67
A forensic analyst receives a hard drive containing malware quarantined by the antivirus application. After creating an image and determining the directory location of the malware file, which of the following helps to determine when the system became infected?

A. The malware file's modify, access, change time properties.
B. The timeline analysis of the file system.
C. The time stamp of the malware in the swap file.
D. The date/time stamp of the malware detection in the antivirus logs.

Answer: B

NEW QUESTION 68
A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization's customer database. The database will be accessed by both the company's users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.
B. Penetration testing of the solution to ensure that the customer data is well protected.
C. Security clauses are implemented into the contract such as the right to audit.
D. Review of the organizations security policies, procedures and relevant hosting certifications.
E. Code review of the solution to ensure that there are no back doors located in the software.

Answer: CD

NEW QUESTION 72
Which of the following provides the BEST risk calculation methodology?

A. Annual Loss Expectancy (ALE) x Value of Asset
B. Potential Loss x Event Probability x Control Failure Probability
C. Impact x Threat x Vulnerability
D. Risk Likelihood x Annual Loss Expectancy (ALE)

Answer: B

NEW QUESTION 73
The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

A. What are the protections against MITM?
B. What accountability is built into the remote support application?
C. What encryption standards are used in tracking database?
D. What snapshot or "undo" features are present in the application?
E. What encryption standards are used in remote desktop and file transfer functionality?

Answer: B

NEW QUESTION 75
A member of the software development team has requested advice from the security team to implement a new secure lab for testing malware. Which of the following is the NEXT step that the security team should take?

A. Purchase new hardware to keep the malware isolated.
B. Develop a policy to outline what will be required in the secure lab.
C. Construct a series of VMs to host the malware environment.
D. Create a proposal and present it to management for approval.

Answer: D

NEW QUESTION 76
A company has issued a new mobile device policy permitting BYOD and company-issued devices. The company-issued device has a managed middleware client that restricts the applications allowed on company devices and provides those that are approved. The middleware client provides configuration standardization for both company owned and BYOD to secure data and communication to the device according to industry best practices. The policy states that, "BYOD clients must meet the company's infrastructure requirements to permit a connection." The company also issues a memorandum separate from the policy, which provides instructions for the purchase, installation, and use of the middleware client on BYOD. Which of the following is being described?

A. Asset management
B. IT governance
C. Change management
D. Transference of risk

Answer: B

NEW QUESTION 79
The administrator is troubleshooting availability issues on an FCoE-based storage array that uses deduplication. The single controller in the storage array has failed, so the administrator wants to move the drives to a storage array from a different manufacturer in order to access the data. Which of the following issues may potentially occur?

A. The data may not be in a usable format.
B. The new storage array is not FCoE based.
C. The data may need a file system check.
D. The new storage array also only has a single controller.

Answer: A

NEW QUESTION 81
An assessor identifies automated methods for identifying security control compliance through validating sensors at the endpoint and at Tier 2. Which of the following practices satisfy continuous monitoring of authorized information systems?

A. Independent verification and validation
B. Security test and evaluation
C. Risk assessment
D. Ongoing authorization

Answer: D

NEW QUESTION 84
A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic.
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Answer: A

NEW QUESTION 85
A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.
B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.
C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.
D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Answer: A

NEW QUESTION 87
A university requires a significant increase in web and database server resources for one week, twice a year, to handle student registration. The web servers remain idle for the rest
of the year. Which of the following is the MOST cost effective way for the university to securely handle student registration?

A. Virtualize the web servers locally to add capacity during registration.
B. Move the database servers to an elastic private cloud while keeping the web servers local.
C. Move the database servers and web servers to an elastic private cloud.
D. Move the web servers to an elastic public cloud while keeping the database servers local.

Answer: D

NEW QUESTION 91
A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?

A. GRC
B. IPS
C. CMDB
D. Syslog-ng
E. IDS

Answer: A

NEW QUESTION 92
During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already

been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

A. Implement an IPS to block the application on the network
B. Implement the remote application out to the rest of the servers
C. Implement SSL VPN with SAML standards for federation
D. Implement an ACL on the firewall with NAT for remote access

Answer: C

NEW QUESTION 96
A company is deploying a new iSCSI-based SAN. The requirements are as follows: Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication
B. IPSec using AH with PKI certificates for authentication
C. Fiber channel should be used with AES
D. Initiators and targets use CHAP authentication
E. Fiber channel over Ethernet should be used
F. IPSec using AH with PSK authentication and 3DES
G. Targets have SCSI IDs for authentication

Answer: BD

NEW QUESTION 99
An analyst connects to a company web conference hosted on www.webconference.com/meetingID#01234 and observes that numerous guests have been allowed to join, without providing identifying information. The topics covered during the web conference are considered proprietary to the company. Which of the following security concerns does the analyst present to management?

A. Guest users could present a risk to the integrity of the company's information
B. Authenticated users could sponsor guest access that was previously approved by management
C. Unauthenticated users could present a risk to the confidentiality of the company's information
D. Meeting owners could sponsor guest access if they have passed a background check

Answer: C

NEW QUESTION 101
A forensic analyst works for an e-discovery firm where several gigabytes of data are processed daily. While the business is lucrative, they do not have the resources or the scalability to adequately serve their clients. Since it is an e-discovery firm where chain of custody is important, which of the following scenarios should they consider?

A. Offload some data processing to a public cloud
B. Aligning their client intake with the resources available
C. Using a community cloud with adequate controls
D. Outsourcing the service to a third party cloud provider

Answer: C

NEW QUESTION 102
A security engineer is responsible for monitoring company applications for known vulnerabilities. Which of the following is a way to stay current on exploits and information security news?

A. Update company policies and procedures
B. Subscribe to security mailing lists
C. Implement security awareness training
D. Ensure that the organization vulnerability management plan is up-to-date

Answer: B

NEW QUESTION 106
Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

A. Deploy inline network encryption devices
B. Install an SSL acceleration appliance
C. Require all core business applications to use encryption
D. Add an encryption module to the router and configure IPSec

Answer: A

NEW QUESTION 107
The helpdesk manager wants to find a solution that will enable the helpdesk staff to better serve company employees who call with computer-related problems. The helpdesk staff is currently unable to perform effective troubleshooting and relies on callers to describe their technology problems. Given that the helpdesk staff is located within the company headquarters and 90% of the callers are telecommuters, which of the following tools should the helpdesk manager use to make the staff more effective at troubleshooting while at the same time reducing company costs? (Select TWO).

A. Web cameras
B. Email
C. Instant messaging
D. BYOD
E. Desktop sharing
F. Presence

Answer: CE

NEW QUESTION 109
A systems administrator establishes a CIFS share on a UNIX device to share data to
Windows systems. The security authentication on the Windows domain is set to the highest level. Windows users are stating that they cannot authenticate to the UNIX share. Which of the following settings on the UNIX server would correct this problem?

A. Refuse LM and only accept NTLMv2
B. Accept only LM
C. Refuse NTLMv2 and accept LM
D. Accept only NTLM

Answer: A

NEW QUESTION 114
The technology steering committee is struggling with increased requirements stemming from an increase in telecommuting. The organization has not addressed telecommuting in the past. The implementation of a new SSL-VPN and a VOIP phone solution enables personnel to work from remote locations with corporate assets. Which of the following steps must the committee take FIRST to outline senior management's directives?

A. Develop an information classification scheme that will properly secure data on corporate systems.
B. Implement database views and constrained interfaces so remote users will be unable to access PII from personal equipment.
C. Publish a policy that addresses the security requirements for working remotely with company equipment.
D. Work with mid-level managers to identify and document the proper procedures for telecommuting.

Answer: C

NEW QUESTION 115
An application present on the majority of an organization's 1,000 systems is vulnerable to a buffer overflow attack. Which of the following is the MOST comprehensive way to resolve the issue?

A. Deploy custom HIPS signatures to detect and block the attacks.
B. Validate and deploy the appropriate patch.
C. Run the application in terminal services to reduce the threat landscape.
D. Deploy custom NIPS signatures to detect and block the attacks.

Answer: B

NEW QUESTION 116
A security administrator notices a recent increase in workstations becoming compromised by malware. Often, the malware is delivered via drive-by downloads, from malware hosting websites, and is not being detected by the corporate antivirus. Which of the following solutions would provide the BEST protection for the company?

A. Increase the frequency of antivirus downloads and install updates to all workstations.
B. Deploy a cloud-based content filter and enable the appropriate category to prevent further infections.
C. Deploy a WAF to inspect and block all web traffic which may contain malware and exploits.
D. Deploy a web based gateway antivirus server to intercept viruses before they enter the network.

Answer: B

NEW QUESTION 121
A security firm is writing a response to an RFP from a customer that is building a new network based software product. The firm's expertise is in penetration testing corporate networks. The RFP explicitly calls for all possible behaviors of the product to be tested, however, it does not specify any particular method to achieve this goal. Which of the following should be used to ensure the security and functionality of the product? (Select TWO).

A. Code review
B. Penetration testing
C. Grey box testing
D. Code signing
E. White box testing

Answer: AE

NEW QUESTION 124
Due to compliance regulations, a company requires a yearly penetration test. The Chief Information Security Officer (CISO) has asked that it be done under a black box methodology.
Which of the following would be the advantage of conducting this kind of penetration test?

A. The risk of unplanned server outages is reduced.
B. Using documentation provided to them, the pen-test organization can quickly determine areas to focus on.
C. The results will show an in-depth view of the network and should help pin-point areas of internal weakness.

D. The results should reflect what attackers may be able to learn about the company.

Answer: D

NEW QUESTION 127
The senior security administrator wants to redesign the company DMZ to minimize the risks associated with both external and internal threats. The DMZ design must support security in depth, change management and configuration processes, and support incident reconstruction. Which of the following designs BEST supports the given requirements?

A. A dual firewall DMZ with remote logging where each firewall is managed by a separate administrator.
B. A single firewall DMZ where each firewall interface is managed by a separate administrator and logging to the cloud.
C. A SaaS based firewall which logs to the company's local storage via SSL, and is managed by the change control team.
D. A virtualized firewall, where each virtual instance is managed by a separate administrator and logging to the same hardware.

Answer: A

NEW QUESTION 128
A security policy states that all applications on the network must have a password length of eight characters. There are three legacy applications on the network that cannot meet this
policy. One system will be upgraded in six months, and two are not expected to be upgraded or removed from the network. Which of the following processes should be followed?

A. Establish a risk matrix
B. Inherit the risk for six months
C. Provide a business justification to avoid the risk
D. Provide a business justification for a risk exception

Answer: D

NEW QUESTION 132
A company sales manager received a memo from the company's financial department which stated that the company would not be putting its software products through the same security testing as previous years to reduce the research and development cost by 20 percent for the upcoming year. The memo also stated that the marketing material and service level agreement for each product would remain unchanged. The sales manager has reviewed the sales goals for the upcoming year and identified an increased target across the software products that will be affected by the financial department's change. All software products will continue to go through new development in the coming year. Which of the following should the sales manager do to ensure the company stays out of trouble?

A. Discuss the issue with the software product's user groups
B. Consult the company's legal department on practices and law
C. Contact senior finance management and provide background information
D. Seek industry outreach for software practices and law

Answer: B

NEW QUESTION 135
A small retail company recently deployed a new point of sale (POS) system to all 67 stores. The core of the POS is an extranet site, accessible only from retail stores and the corporate office over a split-tunnel VPN. An additional split-tunnel VPN provides bi-directional connectivity back to the main office, which provides voice connectivity for store VoIP phones. Each store offers guest wireless functionality, as well as employee wireless. Only the staff wireless network has access to the POS VPN. Recently, stores are reporting poor response times when accessing the POS application from store computers as well as degraded voice quality when making phone calls. Upon investigation, it is determined that three store PCs are hosting malware, which is generating excessive network traffic. After malware removal, the information security department is asked to review the configuration and suggest changes to prevent this from happening again. Which of the following denotes the BEST way to mitigate future malware risk?

A. Deploy new perimeter firewalls at all stores with UTM functionality.
B. Change antivirus vendors at the store and the corporate office.
C. Move to a VDI solution that runs offsite from the same data center that hosts the new POS solution.
D. Deploy a proxy server with content filtering at the corporate office and route all traffic through it.

Answer: A

NEW QUESTION 136
Which of the following BEST constitutes the basis for protecting VMs from attacks from other VMs hosted on the same physical platform?

A. Aggressive patch management on the host and guest OSs.
B. Host based IDS sensors on all guest OSs.
C. Different antivirus solutions between the host and guest OSs.
D. Unique Network Interface Card (NIC) assignment per guest OS.

Answer: A

NEW QUESTION 140
Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?

A. Integer overflow
B. Click-jacking
C. Race condition

D. SQL injection
E. Use after free
F. Input validation

Answer: E

NEW QUESTION 141

A new web based application has been developed and deployed in production. A security engineer decides to use an HTTP interceptor for testing the application. Which of the following problems would MOST likely be uncovered by this tool?

A. The tool could show that input validation was only enabled on the client side
B. The tool could enumerate backend SQL database table and column names
C. The tool could force HTTP methods such as DELETE that the server has denied
D. The tool could fuzz the application to determine where memory leaks occur

Answer: A

NEW QUESTION 144

Company XYZ has purchased and is now deploying a new HTML5 application. The company wants to hire a penetration tester to evaluate the security of the client and server components of the proprietary web application before launch. Which of the following is the
penetration tester MOST likely to use while performing black box testing of the security of the company's purchased application? (Select TWO).

A. Code review
B. Sandbox
C. Local proxy
D. Fuzzer
E. Port scanner

Answer: CD

NEW QUESTION 146

A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model
B. Incremental model
C. Waterfall model
D. Agile model

Answer: C

NEW QUESTION 149

Three companies want to allow their employees to seamlessly connect to each other's wireless corporate networks while keeping one consistent wireless client configuration. Each company wants to maintain its own authentication infrastructure and wants to ensure that an employee who is visiting the other two companies is authenticated by the home office when connecting to the other companies' wireless network. All three companies have agreed to standardize on 802.1x EAP-PEAP-MSCHAPv2 for client configuration. Which of the following should the three companies implement?

A. The three companies should agree on a single SSID and configure a hierarchical RADIUS system which implements trust delegation.
B. The three companies should implement federated authentication through Shibboleth connected to an LDAP backend and agree on a single SSID.
C. The three companies should implement a central portal-based single sign-on and agree to use the same CA when issuing client certificates.
D. All three companies should use the same wireless vendor to facilitate the use of a shared cloud based wireless controller.

Answer: A

**Explanation:** Topic 2, Volume B

NEW QUESTION 154

DRAG DROP
Company A has experienced external attacks on their network and wants to minimize the attacks from reoccurring. Modify the network diagram to prevent SQL injections, XSS attacks, smurf attacks, e-mail spam, downloaded malware, viruses and ping attacks. The company can spend a MAXIMUM of $50,000 USD. A cost list for each item is listed below:
1. Anti-Virus Server - $10,000
2. Firewall-$15,000
3. Load Balanced Server - $10,000 4. NIDS/NIPS-$10,000
5. Packet Analyzer - $5,000
6. Patch Server-$15,000
7. Proxy Server-$20,000
8. Router-$10,000
9. Spam Filter-$5,000
10. Traffic Shaper - $20,000
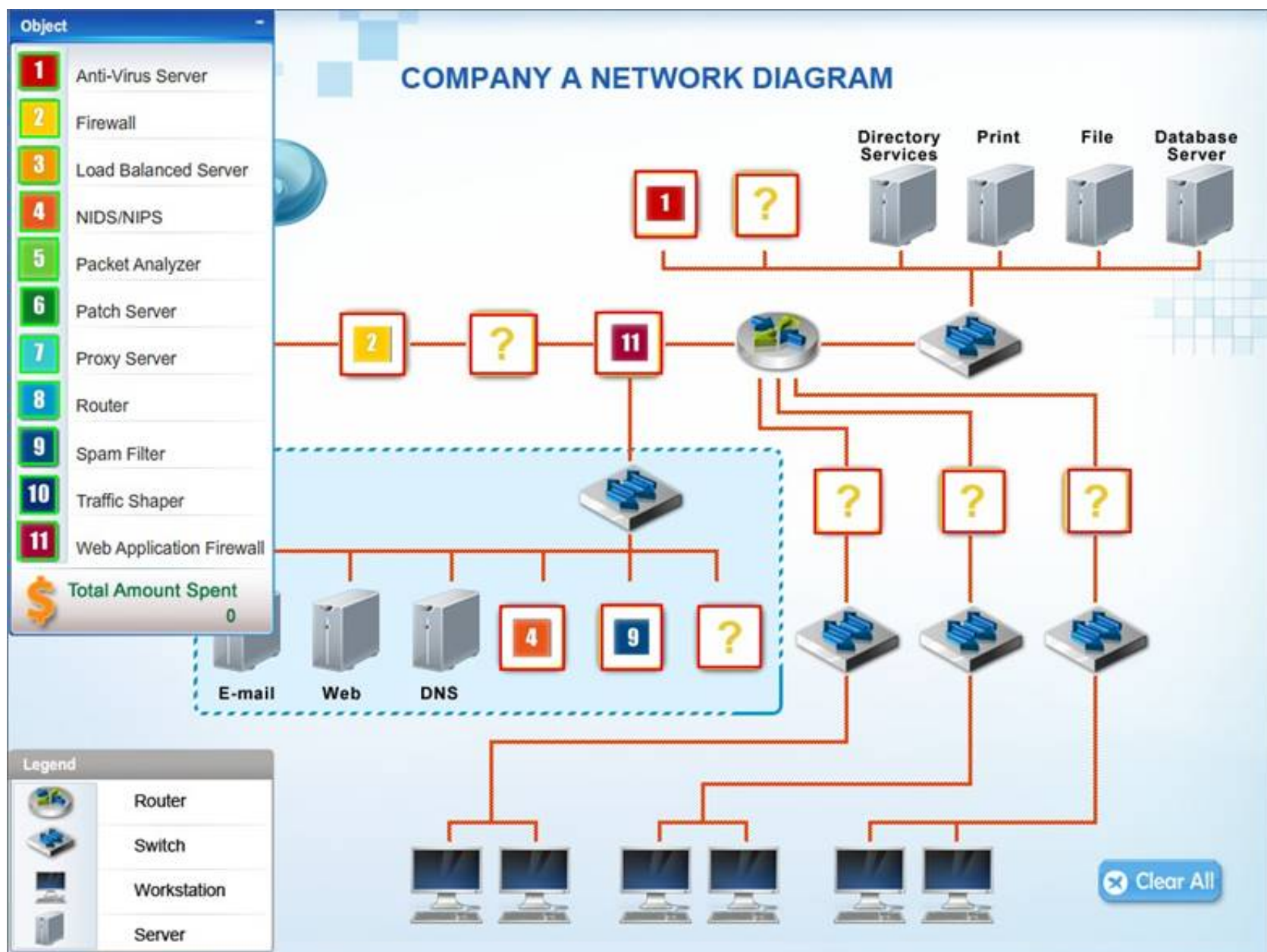11. Web Application Firewall - $10,000
Instructions: Not all placeholders in the diagram need to be filled and items can only be used once. If you place an object on the network diagram, you can remove it by clicking the
(x) in the upper right-hand of the object.
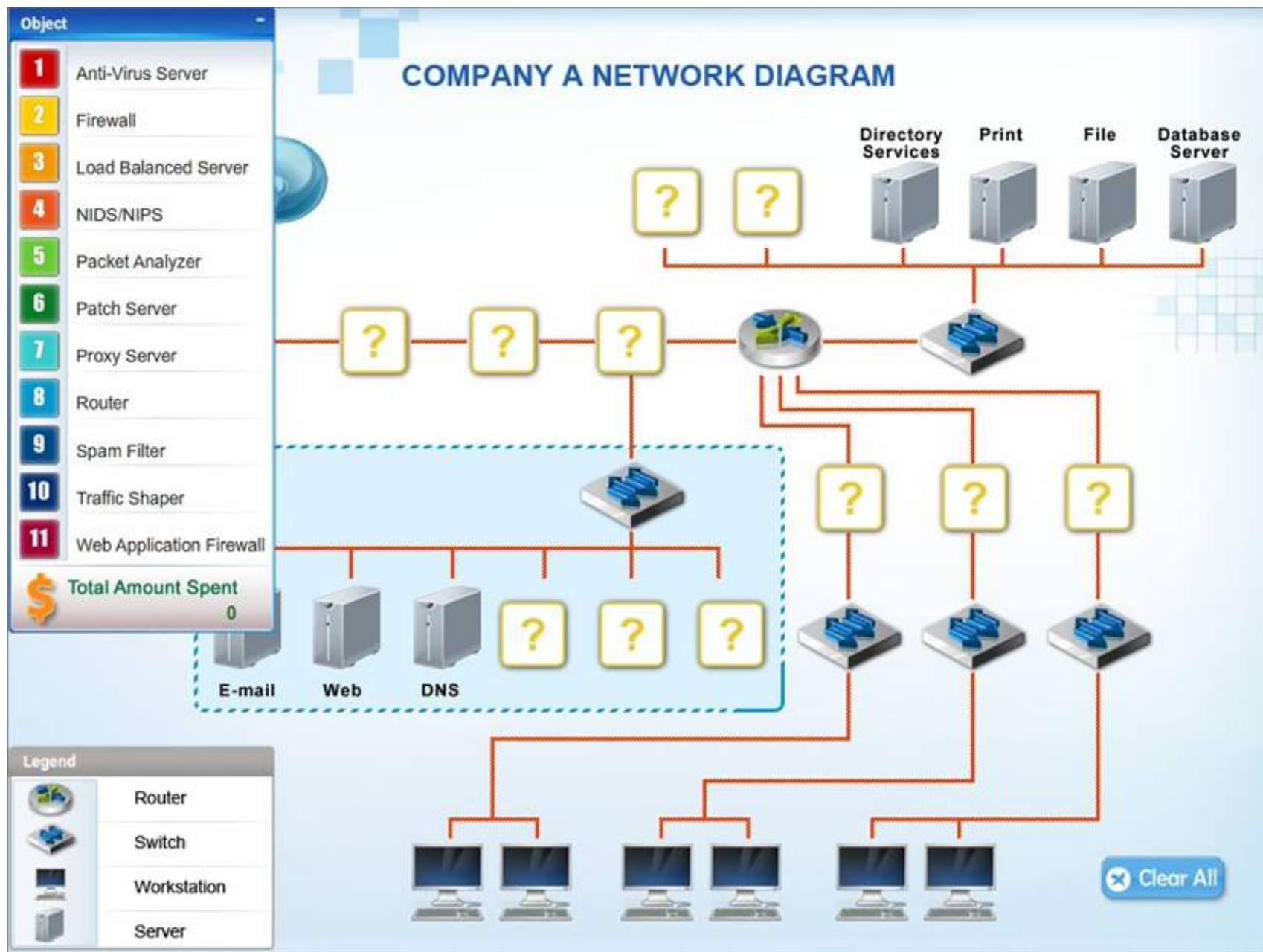
Answer:

Explanation:

NEW QUESTION 155
Which of the following represents important technical controls for securing a SAN storage infrastructure? (Select TWO).

A. Synchronous copy of data
B. RAID configuration
C. Data de-duplication
D. Storage pool space allocation
E. Port scanning
F. LUN masking/mapping
G. Port mapping

Answer: FG

NEW QUESTION 156
A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.
To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?

A. Residual Risk calculation
B. A cost/benefit analysis
C. Quantitative Risk Analysis
D. Qualitative Risk Analysis

Answer: C

NEW QUESTION 160
A pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the
shortest time period?

A. Online password testing
B. Rainbow tables attack
C. Dictionary attack
D. Brute force attack

Answer: B

NEW QUESTION 161
A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems
B. Implement an application layer firewall to protect the payroll system interface
C. Monitor the system's security log for unauthorized access to the payroll application
D. Perform reconciliation of all payroll transactions on a daily basis

Answer: A

NEW QUESTION 165
The DLP solution has been showing some unidentified encrypted data being sent using FTP to a remote server. A vulnerability scan found a collection of Linux servers that are missing OS level patches. Upon further investigation, a technician notices that there are a few unidentified processes running on a number of the servers. What would be a key FIRST step for the data security team to undertake at this point?

A. Capture process ID data and submit to anti-virus vendor for review.
B. Reboot the Linux servers, check running processes, and install needed patches.
C. Remove a single Linux server from production and place in quarantine.
D. Notify upper management of a security breach.
E. Conduct a bit level image, including RAM, of one or more of the Linux servers.

Answer: E

NEW QUESTION 170
A new IT company has hired a security consultant to implement a remote access system, which will enable employees to telecommute from home using both company issued as well as personal computing devices, including mobile devices. The company wants a flexible system to provide confidentiality and integrity for data in transit to the company's internally developed application GUI. Company policy prohibits employees from having administrative rights to company issued devices. Which of the following remote access solutions has the lowest technical complexity?

A. RDP server
B. Client-based VPN
C. IPSec
D. Jump box
E. SSL VPN

Answer: A

NEW QUESTION 172
During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for

compliance to regulations. The audit discovers that 40 percent of the desktops do not meet requirements. Which of the following is the MOST likely cause of the noncompliance?

A. The devices are being modified and settings are being overridden in production.
B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
C. The desktop applications were configured with the default username and password.
D. 40 percent of the devices use full disk encryption.

Answer: A

NEW QUESTION 175
VPN users cannot access the active FTP server through the router but can access any
server in the data center.
Additional network information:
DMZ network – 192.168.5.0/24 (FTP server is 192.168.5.11) VPN network – 192.168.1.0/24
Datacenter – 192.168.2.0/24 User network - 192.168.3.0/24 HR network – 192.168.4.0/24\
Traffic shaper configuration: VLAN Bandwidth Limit (Mbps) VPN50
User175 HR250
Finance250 Guest0
Router ACL: ActionSourceDestination Permit192.168.1.0/24192.168.2.0/24 Permit192.168.1.0/24192.168.3.0/24 Permit192.168.1.0/24192.168.5.0/24
Permit192.168.2.0/24192.168.1.0/24 Permit192.168.3.0/24192.168.1.0/24 Permit192.168.5.1/32192.168.1.0/24 Deny192.168.4.0/24192.168.1.0/24
Deny192.168.1.0/24192.168.4.0/24
Denyanyany
Which of the following solutions would allow the users to access the active FTP server?

A. Add a permit statement to allow traffic from 192.168.5.0/24 to the VPN network
B. Add a permit statement to allow traffic to 192.168.5.1 from the VPN network
C. IPS is blocking traffic and needs to be reconfigured
D. Configure the traffic shaper to limit DMZ traffic
E. Increase bandwidth limit on the VPN network

Answer: A

NEW QUESTION 176
An information security assessor for an organization finished an assessment that identified critical issues with the human resource new employee management software application. The assessor submitted the report to senior management but nothing has happened. Which of the following would be a logical next step?

A. Meet the two key VPs and request a signature on the original assessment.
B. Include specific case studies from other organizations in an updated report.
C. Schedule a meeting with key human resource application stakeholders.
D. Craft an RFP to begin finding a new human resource application.

Answer: C

NEW QUESTION 178
A security administrator is performing VDI traffic data collection on a virtual server which migrates from one host to another. While reviewing the data collected by the protocol analyzer, the security administrator notices that sensitive data is present in the packet capture. Which of the following should the security administrator recommend to ensure the confidentiality of sensitive information during live VM migration, while minimizing latency issues?

A. A separate physical interface placed on a private VLAN should be configured for live host operations.
B. Database record encryption should be used when storing sensitive information on virtual servers.
C. Full disk encryption should be enabled across the enterprise to ensure the confidentiality of sensitive data.
D. Sensitive data should be stored on a backend SAN which uses an isolated fiber channel network.

Answer: A

NEW QUESTION 183
A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).

A. LUN masking
B. Snapshots
C. vSAN
D. Dynamic disk pools
E. Multipath
F. Deduplication

Answer: DE

NEW QUESTION 186
Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential product
B. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirement
C. Test the product and make a product recommendation.
D. Evaluate relevant RFC and ISO standards to choose an appropriate vendor produc

E. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.
F. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.
G. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provide
H. Give access to internal security employees so that they can inspect the application payload data.
I. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Answer: A

NEW QUESTION 189
A company has adopted a BYOD program. The company would like to protect confidential information. However, it has been decided that when an employee leaves, the company will not completely wipe the personal device. Which of the following would MOST likely help the company maintain security when employees leave?

A. Require cloud storage on corporate servers and disable access upon termination
B. Whitelist access to only non-confidential information
C. Utilize an MDM solution with containerization
D. Require that devices not have local storage

Answer: C

NEW QUESTION 191
An investigator wants to collect the most volatile data first in an incident to preserve the data that runs the highest risk of being lost. After memory, which of the following BEST represents the remaining order of volatility that the investigator should follow?

A. File system information, swap files, network processes, system processes and raw disk blocks.
B. Raw disk blocks, network processes, system processes, swap files and file system information.
C. System processes, network processes, file system information, swap files and raw disk blocks.
D. Raw disk blocks, swap files, network processes, system processes, and file system information.

Answer: C

NEW QUESTION 192
An administrator is implementing a new network-based storage device. In selecting a storage protocol, the administrator would like the data in transit's integrity to be the most important concern. Which of the following protocols meets these needs by implementing either AES-CMAC or HMAC-SHA256 to sign data?

A. SMB
B. NFS
C. FCoE
D. iSCSI

Answer: A

NEW QUESTION 194
Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:
Delivered-To: customer@example.com Received: by 10.14.120.205
Mon, 1 Nov 2010 11:15:24 -0700 (PDT)
Received: by 10.231.31.193
Mon, 01 Nov 2010 11:15:23 -0700 (PDT)
Return-Path: <IT@company.com>
Received: from 127.0.0.1 for <customer@example.com>; Mon, 1 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)
Received: by smtpex.example.com (SMTP READY)
with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500
Received: from 172.18.45.122 by 192.168.2.55; Mon, 1 Nov 2010 13:15:14 -0500
From: Company <IT@Company.com>
To: "customer@example.com" <customer@example.com> Date: Mon, 1 Nov 2010 13:15:11 -0500
Subject: New Insurance Application Thread-Topic: New Insurance Application
Please download and install software from the site below to maintain full access to your account.
www.examplesite.com
_____Additional information: The authorized mail servers IPs are 192.168.2.10 and 192.168.2.11. The network's subnet is 192.168.2.0/25.
Which of the following are the MOST appropriate courses of action a security administrator could take to eliminate this risk? (Select TWO).

A. Identify the origination point for malicious activity on the unauthorized mail server.
B. Block port 25 on the firewall for all unauthorized mail servers.
C. Disable open relay functionality.
D. Shut down the SMTP service on the unauthorized mail server.
E. Enable STARTTLS on the spam filter.

Answer: BD

NEW QUESTION 197
The IT director has charged the company helpdesk with sanitizing fixed and removable media. The helpdesk manager has written a new procedure to be followed by the helpdesk staff. This procedure includes the current standard to be used for data sanitization, as well as the location of physical degaussing tools. In which of the following cases should the helpdesk staff use the new procedure? (Select THREE).

A. During asset disposal

B. While reviewing the risk assessment
C. While deploying new assets
D. Before asset repurposing
E. After the media has been disposed of
F. During the data classification process
G. When installing new printers
H. When media fails or is unusable

Answer: ADH

NEW QUESTION 198
An administrator wishes to replace a legacy clinical software product as it has become a security risk. The legacy product generates $10,000 in revenue a month. The new software product has an initial cost of $180,000 and a yearly maintenance of $2,000 after the first year. However, it will generate $15,000 in revenue per month and be more secure. How many years until there is a return on investment for this new package?

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

Answer: D

NEW QUESTION 201
The telecommunications manager wants to improve the process for assigning company- owned mobile devices and ensuring data is properly removed when no longer needed. Additionally, the manager wants to onboard and offboard personally owned mobile devices that will be used in the BYOD initiative. Which of the following should be implemented to ensure these processes can be automated? (Select THREE).

A. SIM's PIN
B. Remote wiping
C. Chargeback system
D. MDM software
E. Presence software
F. Email profiles
G. Identity attestation
H. GPS tracking

Answer: BDG

NEW QUESTION 206
After reviewing a company's NAS configuration and file system access logs, the auditor is advising the security administrator to implement additional security controls on the NFS export. The security administrator decides to remove the no_root_squash directive from the export and add the nosuid directive. Which of the following is true about the security controls implemented by the security administrator?

A. The newly implemented security controls are in place to ensure that NFS encryption can only be controlled by the root user.
B. Removing the no_root_squash directive grants the root user remote NFS read/write access to important files owned by root on the NAS.
C. Users with root access on remote NFS client computers can always use the SU command to modify other user's files on the NAS.
D. Adding the nosuid directive disables regular users from accessing files owned by the root user over NFS even after using the SU command.

Answer: C

NEW QUESTION 208
ODBC access to a database on a network-connected host is required. The host does not have a security mechanism to authenticate the incoming ODBC connection, and the application requires that the connection have read/write permissions. In order to further secure the data, a nonstandard configuration would need to be implemented. The information in the database is not sensitive, but was not readily accessible prior to the implementation of the ODBC connection. Which of the following actions should be taken by the security analyst?

A. Accept the risk in order to keep the system within the company's standard security configuration.
B. Explain the risks to the data owner and aid in the decision to accept the risk versus choosing a nonstandard solution.
C. Secure the data despite the need to use a security control or solution that is not within company standards.
D. Do not allow the connection to be made to avoid unnecessary risk and avoid deviating from the standard security configuration.

Answer: B

NEW QUESTION 212
A company has a difficult time communicating between the security engineers, application developers, and sales staff. The sales staff tends to overpromise the application deliverables. The security engineers and application developers are falling behind schedule. Which of the following should be done to solve this?

A. Allow the sales staff to shadow the developers and engineers to see how their sales impact the deliverables.
B. Allow the security engineering team to do application development so they understand why it takes so long.
C. Allow the application developers to attend a sales conference so they understand how business is done.
D. Allow the sales staff to learn application programming and security engineering so they understand the whole lifecycle.

Answer: A

NEW QUESTION 215
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

Answer: D

NEW QUESTION 217
A company provides on-demand cloud computing resources for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two- factor authentication for customer access to the administrative website. The security administrator at the company has uncovered a breach in data confidentiality. Sensitive data from customer A was found on a hidden directory within the VM of company B. Company B is not in the same industry as company A and the two are not competitors. Which of the following has MOST likely occurred?

A. Both VMs were left unsecured and an attacker was able to exploit network vulnerabilities to access each and move the data.
B. A stolen two factor token was used to move data from one virtual guest to another host on the same network segment.
C. A hypervisor server was left un-patched and an attacker was able to use a resource exhaustion attack to gain unauthorized access.
D. An employee with administrative access to the virtual guests was able to dump the guest memory onto a mapped disk.

Answer: A

NEW QUESTION 220
A security administrator was recently hired in a start-up company to represent the interest of security and to assist the network team in improving security in the company. The programmers are not on good terms with the security team and do not want to be distracted with security issues while they are working on a major project. Which of the following is the BEST time to make them address security issues in the project?
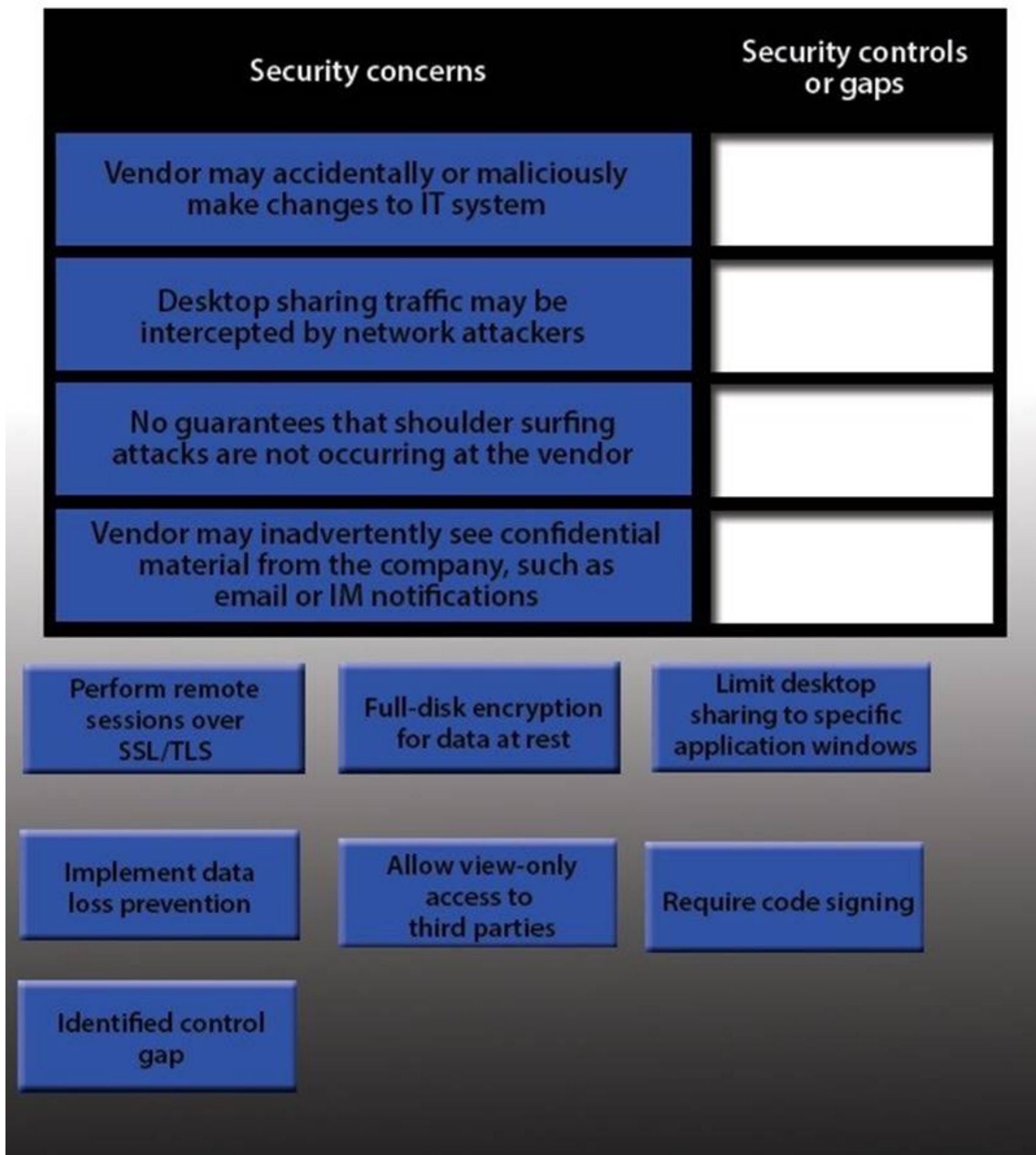
A. In the middle of the project
B. At the end of the project
C. At the inception of the project
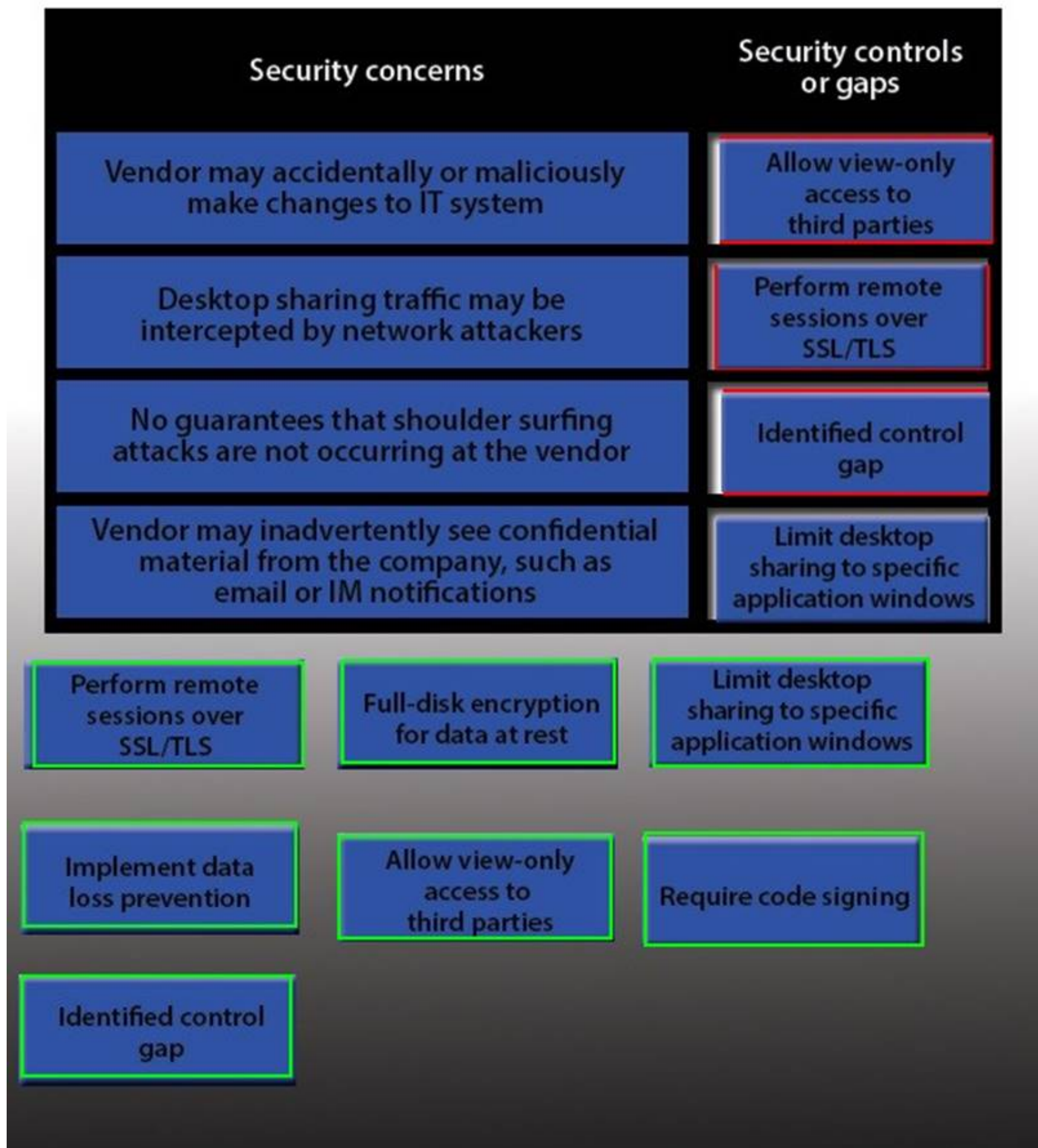D. At the time they request

Answer: C

NEW QUESTION 221
DRAG DROP
IT staff within a company often conduct remote desktop sharing sessions with vendors to troubleshoot vendor product-related issues. Drag and drop the following security controls to match the associated security concern. Options may be used once or not at all.

Security concerns

Security concerns
Vendor may accidentally or maliciously make changes to IT system
Desktop sharing traffic may be intercepted by network attackers
No guarantees that shoulder surfing attacks are not occurring at the vendor
Vendor may inadvertently see confidential material from the company, such as email or IM notifications

Security controls or gaps

- Perform remote sessions over SSL/TLS
- Full-disk encryption for data at rest
- Limit desktop sharing to specific application windows
- Implement data loss prevention
- Allow view-only access to third parties
- Require code signing
- Identified control gap

Answer:

Explanation:

NEW QUESTION 226
A bank is in the process of developing a new mobile application. The mobile client renders content and communicates back to the company servers via REST/JSON calls. The bank wants to ensure that the communication is stateless between the mobile application and the web services gateway. Which of the following controls MUST be implemented to enable stateless communication?

A. Generate a one-time key as part of the device registration process.
B. Require SSL between the mobile application and the web services gateway.
C. The jsession cookie should be stored securely after authentication.
D. Authentication assertion should be stored securely on the client.

Answer: D

NEW QUESTION 229
After the install process, a software application executed an online activation process. After a few months, the system experienced a hardware failure. A backup image of the system was restored on a newer revision of the same brand and model device. After the restore, the specialized application no longer works. Which of the following is the MOST likely cause of the problem?

A. The binary files used by the application have been modified by malware.
B. The application is unable to perform remote attestation due to blocked ports.
C. The restored image backup was encrypted with the wrong key.
D. The hash key summary of hardware and installed software no longer match.

Answer: D

NEW QUESTION 230
The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000
B. $24,000
C. $30,000
D. $96,000

Answer: A

NEW QUESTION 231
ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP
B. PAP
C. CHAP
D. HOTP

Answer: D

NEW QUESTION 232
Company policy requires that all company laptops meet the following baseline requirements:
Software requirements:
Antivirus Anti-malware Anti-spyware
Log monitoring
Full-disk encryption
Terminal services enabled for RDP Administrative access for local users
Hardware restrictions: Bluetooth disabled FireWire disabled WiFi adapter disabled
Ann, a web developer, reports performance issues with her laptop and is not able to access any network resources. After further investigation, a bootkit was discovered and it was trying to access external websites. Which of the following hardening techniques should be applied to mitigate this specific issue from reoccurring? (Select TWO).

A. Group policy to limit web access
B. Restrict VPN access for all mobile users
C. Remove full-disk encryption
D. Remove administrative access to local users
E. Restrict/disable TELNET access to network resources
F. Perform vulnerability scanning on a daily basis
G. Restrict/disable USB access

Answer: DG

NEW QUESTION 237
A port in a fibre channel switch failed, causing a costly downtime on the company's primary website. Which of the following is the MOST likely cause of the downtime?

A. The web server iSCSI initiator was down.
B. The web server was not multipathed.
C. The SAN snapshots were not up-to-date.
D. The SAN replication to the backup site failed.

Answer: B

NEW QUESTION 239
Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).

A. Jailbroken mobile device
B. Reconnaissance tools
C. Network enumerator
D. HTTP interceptor
E. Vulnerability scanner
F. Password cracker

Answer: DE

NEW QUESTION 244
A firm's Chief Executive Officer (CEO) is concerned that IT staff lacks the knowledge to identify complex vulnerabilities that may exist in a payment system being internally developed. The payment system being developed will be sold to a number of organizations and is in direct competition with another leading product. The CEO highlighted that code base confidentiality is of critical importance to allow the company to exceed the competition in terms of the product's reliability, stability, and performance. Which of the following would provide the MOST thorough testing and satisfy the CEO's requirements?

A. Sign a MOU with a marketing firm to preserve the company reputation and use in-house resources for random testing.
B. Sign a BPA with a small software consulting firm and use the firm to perform Black box testing and address all findings.
C. Sign a NDA with a large security consulting firm and use the firm to perform Grey box testing and address all findings.
D. Use the most qualified and senior developers on the project to perform a variety of White box testing and code reviews.

Answer: C

NEW QUESTION 247
A security administrator has noticed that an increased number of employees' workstations are becoming infected with malware. The company deploys an enterprise antivirus system as well as a web content filter, which blocks access to malicious web sites where malware files can be downloaded. Additionally, the company implements technical measures to disable external storage. Which of the following is a technical control that the security administrator should implement next to reduce malware infection?

A. Implement an Acceptable Use Policy which addresses malware downloads.
B. Deploy a network access control system with a persistent agent.
C. Enforce mandatory security awareness training for all employees and contractors.
D. Block cloud-based storage software on the company network.

Answer: D

NEW QUESTION 250
A system administrator has just installed a new Linux distribution. The distribution is configured to be "secure out of the box". The system administrator cannot make updates to certain system files and services. Each time changes are attempted, they are denied and a system error is generated. Which of the following troubleshooting steps should the security administrator suggest?

A. Review settings in the SELinux configuration files
B. Reset root permissions on systemd files
C. Perform all administrative actions while logged in as root
D. Disable any firewall software before making changes

Answer: A

NEW QUESTION 254
It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?

A. Update the blog page to HTTPS
B. Filter metacharacters
C. Install HIDS on the server
D. Patch the web application
E. Perform client side input validation

Answer: B

NEW QUESTION 255
A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user's ongoing communication be retained in the user's account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user's communicatio
B. Next, place a legal hold on the user's email account.
C. Perform an e-discover using the applicable search term
D. Next, back up the user's email for a future investigation.
E. Place a legal hold on the user's email accoun
F. Next, perform e-discovery searches to collect applicable emails.
G. Perform a back up of the user's email accoun
H. Next, export the applicable emails that match the search terms.

Answer: C

NEW QUESTION 256
A facilities manager has observed varying electric use on the company's metered service lines. The facility management rarely interacts with the IT department unless new equipment is being delivered. However, the facility manager thinks that there is a correlation between spikes in electric use and IT department activity. Which of the following business processes and/or practices would provide better management of organizational resources with the IT department's needs? (Select TWO).

A. Deploying a radio frequency identification tagging asset management system
B. Designing a business resource monitoring system
C. Hiring a property custodian
D. Purchasing software asset management software
E. Facility management participation on a change control board
F. Rewriting the change board charter
G. Implementation of change management best practices

Answer: EG

NEW QUESTION 260
A large company is preparing to merge with a smaller company. The smaller company has been very profitable, but the smaller company's main applications were created in-house. Which of the following actions should the large company's security administrator take in preparation for the merger?

A. A review of the mitigations implemented from the most recent audit findings of the smaller company should be performed.
B. An ROI calculation should be performed to determine which company's application should be used.
C. A security assessment should be performed to establish the risks of integration or co- existence.
D. A regression test should be performed on the in-house software to determine security risks associated with the software.

Answer: C

NEW QUESTION 263
A company with 2000 workstations is considering purchasing a HIPS to minimize the impact of a system compromise from malware. Currently, the company projects a total cost of $50,000 for the next three years responding to and eradicating workstation malware. The Information Security Officer (ISO) has received three quotes from different companies that provide HIPS.
Which solution should the company select if the contract is only valid for three years?

A. First quote
B. Second quote
C. Third quote
D. Accept the risk

Answer: B

NEW QUESTION 268
An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is $25,000 and the ALE after implementing the web filter is $15,000. The web filtering solution will cost the organization
$10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

A. $0
B. $7,500
C. $10,000
D. $12,500
E. $15,000

Answer: B

NEW QUESTION 273
A security solutions architect has argued consistently to implement the most secure method of encrypting corporate messages. The solution has been derided as not being cost effective by other members of the IT department. The proposed solution uses symmetric keys to encrypt all messages and is very resistant to unauthorized decryption. The method also requires special handling and security for all key material that goes above and beyond most encryption systems. Which of the following is the solutions architect MOST likely trying to implement?

A. One time pads
B. PKI
C. Quantum cryptography
D. Digital rights management

Answer: A

NEW QUESTION 276
A security manager looked at various logs while investigating a recent security breach in the data center from an external source. Each log below was collected from various security devices compiled from a report through the company's security information and event management server.
Logs: Log 1:
Feb 5 23:55:37.743: %SEC-6-IPACCESSLOGS: list 10 denied 10.2.5.81 3 packets
Log 2: HTTP://www.company.com/index.php?user=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Log 3:
Security Error Alert
Event ID 50: The RDP protocol component X.224 detected an error in the protocol stream and has disconnected the client
Log 4:
Encoder oe = new OracleEncoder ();
String query = "Select user_id FROM user_data WHERE user_name = ' "
+ oe.encode (req.getParameter("userID")) + " ' and user_password = ' "
+ oe.encode (req.getParameter("pwd")) +" ' ";
Vulnerabilities Buffer overflow SQL injection ACL
XSS
Which of the following logs and vulnerabilities would MOST likely be related to the security breach? (Select TWO).

A. Log 1
B. Log 2
C. Log 3
D. Log 4
E. Buffer overflow
F. ACL
G. XSS
H. SQL injection

Answer: BE

NEW QUESTION 278
Using SSL, an administrator wishes to secure public facing server farms in three subdomains: dc1.east.company.com, dc2.central.company.com, and dc3.west.company.com. Which of the following is the number of wildcard SSL certificates that should be purchased?

A. 1
B. 3
C. 6

Answer: C

NEW QUESTION 279
A security manager is looking into the following vendor proposal for a cloud-based SIEM solution. The intention is that the cost of the SIEM solution will be justified by having reduced the number of incidents and therefore saving on the amount spent investigating incidents.
Proposal:
External cloud-based software as a service subscription costing $5,000 per month. Expected to reduce the number of current incidents per annum by 50%.
The company currently has ten security incidents per annum at an average cost of $10,000 per incident. Which of the following is the ROI for this proposal after three years?

A. -$30,000
B. $120,000
C. $150,000
D. $180,000

Answer: A

NEW QUESTION 282
A senior network security engineer has been tasked to decrease the attack surface of the corporate network. Which of the following actions would protect the external network interfaces from external attackers performing network scanning?

A. Remove contact details from the domain name registrar to prevent social engineering attacks.
B. Test external interfaces to see how they function when they process fragmented IP packets.
C. Enable a honeynet to capture and facilitate future analysis of malicious attack vectors.
D. Filter all internal ICMP message traffic, forcing attackers to use full-blown TCP port
E. scans against external network interfaces.

Answer: B

NEW QUESTION 285
An IT Manager is concerned about errors made during the deployment process for a new model of tablet. Which of the following would suggest best practices and configuration parameters that technicians could follow during the deployment process?

A. Automated workflow
B. Procedure
C. Corporate standard
D. Guideline
E. Policy

Answer: D

NEW QUESTION 290
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: CD

NEW QUESTION 294
During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company's database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non- volatile storage, implement chain of custody, and analyze original media.
B. Take inventory, secure the scene, capture RAM, capture had drive, implement chain of custody, document, and analyze the data.
C. Implement chain of custody, take inventory, secure the scene, capture volatile and non- volatile storage, and document the findings.
D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Answer: D

NEW QUESTION 296

A small company is developing a new Internet-facing web application. The security requirements are:

1. Users of the web application must be uniquely identified and authenticated.
2. Users of the web application will not be added to the company's directory services.
3. Passwords must not be stored in the code. Which of the following meets these requirements?

A. Use OpenID and allow a third party to authenticate users.
B. Use TLS with a shared client certificate for all users.
C. Use SAML with federated directory services.
D. Use Kerberos and browsers that support SAML.

Answer: A

NEW QUESTION 297

The network administrator at an enterprise reported a large data leak. One compromised server was used to aggregate data from several critical application servers and send it out
to the Internet using HTTPS. Upon investigation, there have been no user logins over the previous week and the endpoint protection software is not reporting any issues. Which of the following BEST provides insight into where the compromised server collected the information?

A. Review the flow data against each server's baseline communications profile.
B. Configure the server logs to collect unusual activity including failed logins and restarted services.
C. Correlate data loss prevention logs for anomalous communications from the server.
D. Setup a packet capture on the firewall to collect all of the server communications.

Answer: A

NEW QUESTION 299

A trucking company delivers products all over the country. The executives at the company would like to have better insight into the location of their drivers to ensure the shipments are following secure routes. Which of the following would BEST help the executives meet this goal?

A. Install GSM tracking on each product for end-to-end delivery visibility.
B. Implement geo-fencing to track products.
C. Require drivers to geo-tag documentation at each delivery location.
D. Equip each truck with an RFID tag for location services.

Answer: B

NEW QUESTION 304

A security services company is scoping a proposal with a client. They want to perform a general security audit of their environment within a two week period and consequently have the following requirements:
Requirement 1 – Ensure their server infrastructure operating systems are at their latest patch levels
Requirement 2 – Test the behavior between the application and database Requirement 3 – Ensure that customer data can not be exfiltrated
Which of the following is the BEST solution to meet the above requirements?

A. Penetration test, perform social engineering and run a vulnerability scanner
B. Perform dynamic code analysis, penetration test and run a vulnerability scanner
C. Conduct network analysis, dynamic code analysis, and static code analysis
D. Run a protocol analyzer perform static code analysis and vulnerability assessment

Answer: B

NEW QUESTION 306

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:
Bundled offering expected to be $100,000 per year.
Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.
Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following
options is MOST accurate?

A. Based on cost alone, having an outsourced solution appears cheaper.
B. Based on cost alone, having an outsourced solution appears to be more expensive.
C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.
D. Based on cost alone, having a purchased product solution appears cheaper.

Answer: A

NEW QUESTION 309

A storage as a service company implements both encryption at rest as well as encryption in transit of customers' data. The security administrator is concerned with the overall security of the encrypted customer data stored by the company servers and wants the development team to implement a solution that will strengthen the customer's encryption key. Which of the following, if implemented, will MOST increase the time an offline password attack against the customers' data would take?

A. key = NULL ; for (int i=0; i<5000; i++) { key = sha(key + password) }
B. password = NULL ; for (int i=0; i<10000; i++) { password = sha256(key) }
C. password = password + sha(password+salt) + aes256(password+salt)
D. key = aes128(sha256(password), password))

Answer: A

NEW QUESTION 313
An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?

A. Intermediate Root Certificate
B. Wildcard Certificate
C. EV x509 Certificate
D. Subject Alternative Names Certificate

Answer: D

NEW QUESTION 314
An organization has implemented an Agile development process for front end web application development. A new security architect has just joined the company and wants to integrate security activities into the SDLC.
Which of the following activities MUST be mandated to ensure code quality from a security perspective? (Select TWO).

A. Static and dynamic analysis is run as part of integration
B. Security standards and training is performed as part of the project
C. Daily stand-up meetings are held to ensure security requirements are understood
D. For each major iteration penetration testing is performed
E. Security requirements are story boarded and make it into the build
F. A security design is performed at the end of the requirements phase

Answer: AD

NEW QUESTION 317
The IT Security Analyst for a small organization is working on a customer's system and identifies a possible intrusion in a database that contains PII. Since PII is involved, the analyst wants to get the issue addressed as soon as possible. Which of the following is the FIRST step the analyst should take in mitigating the impact of the potential intrusion?

A. Contact the local authorities so an investigation can be started as quickly as possible.
B. Shut down the production network interfaces on the server and change all of the DBMS account passwords.
C. Disable the front-end web server and notify the customer by email to determine how the customer would like to proceed.
D. Refer the issue to management for handling according to the incident response process.

Answer: D

NEW QUESTION 321
An enterprise must ensure that all devices that connect to its networks have been previously approved. The solution must support dual factor mutual authentication with strong identity assurance. In order to reduce costs and administrative overhead, the security architect wants to outsource identity proofing and second factor digital delivery to the third party. Which of the following solutions will address the enterprise requirements?

A. Implementing federated network access with the third party.
B. Using a HSM at the network perimeter to handle network device access.
C. Using a VPN concentrator which supports dual factor via hardware tokens.
D. Implementing 802.1x with EAP-TTLS across the infrastructure.

Answer: D

NEW QUESTION 322
An internal development team has migrated away from Waterfall development to use Agile development. Overall, this has been viewed as a successful initiative by the stakeholders as it has improved time-to-market. However, some staff within the security team have
contended that Agile development is not secure. Which of the following is the MOST accurate statement?

A. Agile and Waterfall approaches have the same effective level of security postur
B. They both need similar amounts of security effort at the same phases of development.
C. Agile development is fundamentally less secure than Waterfall due to the lack of formal up-front design and inability to perform security reviews.
D. Agile development is more secure than Waterfall as it is a more modern methodology which has the advantage of having been able to incorporate security best practices of recent years.
E. Agile development has different phases and timings compared to Waterfal
F. Security activities need to be adapted and performed within relevant Agile phases.

Answer: D

NEW QUESTION 324
A security auditor suspects two employees of having devised a scheme to steal money from the company. While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?

A. Background checks
B. Job rotation
C. Least privilege
D. Employee termination procedures

Answer: B

NEW QUESTION 327
A finance manager says that the company needs to ensure that the new system can "replay" data, up to the minute, for every exchange being tracked by the investment departments. The finance manager also states that the company's transactions need to be tracked against this data for a period of five years for compliance. How would a security engineer BEST interpret the finance manager's needs?

A. Compliance standards
B. User requirements
C. Data elements
D. Data storage
E. Acceptance testing
F. Information digest
G. System requirements

Answer: B

NEW QUESTION 330
The finance department for an online shopping website has discovered that a number of customers were able to purchase goods and services without any payments. Further analysis conducted by the security investigations team indicated that the website allowed customers to update a payment amount for shipping. A specially crafted value could be entered and cause a roll over, resulting in the shipping cost being subtracted from the balance and in some instances resulted in a negative balance. As a result, the system processed the negative balance as zero dollars. Which of the following BEST describes the application issue?

A. Race condition
B. Click-jacking
C. Integer overflow
D. Use after free
E. SQL injection

Answer: C

NEW QUESTION 335
A recently hired security administrator is advising developers about the secure integration of a legacy in-house application with a new cloud based processing system. The systems must exchange large amounts of fixed format data such as names, addresses, and phone numbers, as well as occasional chunks of data in unpredictable formats. The developers want to construct a new data format and create custom tools to parse and process the data. The security administrator instead suggests that the developers:

A. Create a custom standard to define the data.
B. Use well formed standard compliant XML and strict schemas.
C. Only document the data format in the parsing application code.
D. Implement a de facto corporate standard for all analyzed data.

Answer: B

NEW QUESTION 340
A company decides to purchase commercially available software packages. This can introduce new security risks to the network. Which of the following is the BEST description of why this is true?

A. Commercially available software packages are typically well known and widely availabl
B. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
C. Commercially available software packages are often widely availabl
D. Information concerning vulnerabilities is often kept internal to the company that developed the software.
E. Commercially available software packages are not widespread and are only available in limited area
F. Information concerning vulnerabilities is often ignored by business managers.
G. Commercially available software packages are well known and widely availabl
H. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

Answer: B

NEW QUESTION 341
An educational institution would like to make computer labs available to remote students. The labs are used for various IT networking, security, and programming courses. The requirements are:
1. Each lab must be on a separate network segment.
2. Labs must have access to the Internet, but not other lab networks.
3. Student devices must have network access, not simple access to hosts on the lab networks.
4. Students must have a private certificate installed before gaining access.
5. Servers must have a private certificate installed locally to provide assurance to the students.
6. All students must use the same VPN connection profile.
Which of the following components should be used to achieve the design in conjunction with directory services?

A. L2TP VPN over TLS for remote connectivity, SAML for federated authentication, firewalls between each lab segment
B. SSL VPN for remote connectivity, directory services groups for each lab group, ACLs on routing equipment
C. IPSec VPN with mutual authentication for remote connectivity, RADIUS for authentication, ACLs on network equipment
D. Cloud service remote access tool for remote connectivity, OAuth for authentication, ACL on routing equipment

Answer: C

NEW QUESTION 346

The helpdesk is receiving multiple calls about slow and intermittent Internet access from the finance department. The following information is compiled:
Caller 1, IP 172.16.35.217, NETMASK 255.255.254.0
Caller 2, IP 172.16.35.53, NETMASK 255.255.254.0
Caller 3, IP 172.16.35.173, NETMASK 255.255.254.0
All callers are connected to the same switch and are routed by a router with five built-in interfaces. The upstream router interface's MAC is 00-01-42-32-ab-1a
A packet capture shows the following:
09:05:15.934840 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:06:16.124850 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:07:25.439811 arp reply 172.16.34.1 is-at 00:01:42:32:ab:1a (00:01:42:32:ab:1a)
09:08:10.937590 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2305, seq 1,
length 65534
09:08:10.937591 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2306, seq 2,
length 65534
09:08:10.937592 IP 172.16.35.1 > 172.16.35.255: ICMP echo request, id 2307, seq 3,
length 65534
Which of the following is occurring on the network?

A. A man-in-the-middle attack is underway on the network.
B. An ARP flood attack is targeting at the router.
C. The default gateway is being spoofed on the network.
D. A denial of service attack is targeting at the router.

Answer: D

NEW QUESTION 348

A project manager working for a large city government is required to plan and build a WAN, which will be required to host official business and public access. It is also anticipated that the city's emergency and first response communication systems will be required to operate across the same network. The project manager has experience with enterprise IT projects, but feels this project has an increased complexity as a result of the mixed business / public use and the critical infrastructure it will provide. Which of the following should the project manager release to the public, academia, and private industry to ensure the city provides due care in considering all project factors prior to building its new WAN?

A. NDA
B. RFI
C. RFP
D. RFQ

Answer: B

NEW QUESTION 353

A penetration tester is inspecting traffic on a new mobile banking application and sends the following web request:
POST http://www.example.com/resources/NewBankAccount HTTP/1.1 Content-type: application/json
{
"account": [
{ "creditAccount":"Credit Card Rewards account"} { "salesLeadRef":"www.example.com/badcontent/exploitme.exe"}
],
"customer": [
{ "name":"Joe Citizen"} { "custRef":"3153151"}
]
}
The banking website responds with: HTTP/1.1 200 OK
{
"newAccountDetails": [
{ "cardNumber":"1234123412341234"} { "cardExpiry":"2020-12-31"}
{ "cardCVV":"909"}
],
"marketingCookieTracker":"JSESSIONID=000000001" "returnCode":"Account added successfully"
}
Which of the following are security weaknesses in this example? (Select TWO).

A. Missing input validation on some fields
B. Vulnerable to SQL injection
C. Sensitive details communicated in clear-text
D. Vulnerable to XSS
E. Vulnerable to malware file uploads
F. JSON/REST is not as secure as XML

Answer: AC

NEW QUESTION 358

In a situation where data is to be recovered from an attacker's location, which of the following are the FIRST things to capture? (Select TWO).

A. Removable media
B. Passwords written on scrap paper
C. Snapshots of data on the monitor
D. Documents on the printer
E. Volatile system memory
F. System hard drive

Answer: CE

NEW QUESTION 359
The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year's growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.
B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.
C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.
D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Answer: B

NEW QUESTION 361
An organization recently upgraded its wireless infrastructure to support 802.1x and requires all clients to use this method. After the upgrade, several critical wireless clients fail to
connect because they are only pre-shared key compliant. For the foreseeable future, none of the affected clients have an upgrade path to put them into compliance with the 802.1x requirement. Which of the following provides the MOST secure method of integrating the non-compliant clients into the network?

A. Create a separate SSID and require the use of dynamic encryption keys.
B. Create a separate SSID with a pre-shared key to support the legacy clients and rotate the key at random intervals.
C. Create a separate SSID and pre-shared WPA2 key on a new network segment and only allow required communication paths.
D. Create a separate SSID and require the legacy clients to connect to the wireless network using certificate-based 802.1x.
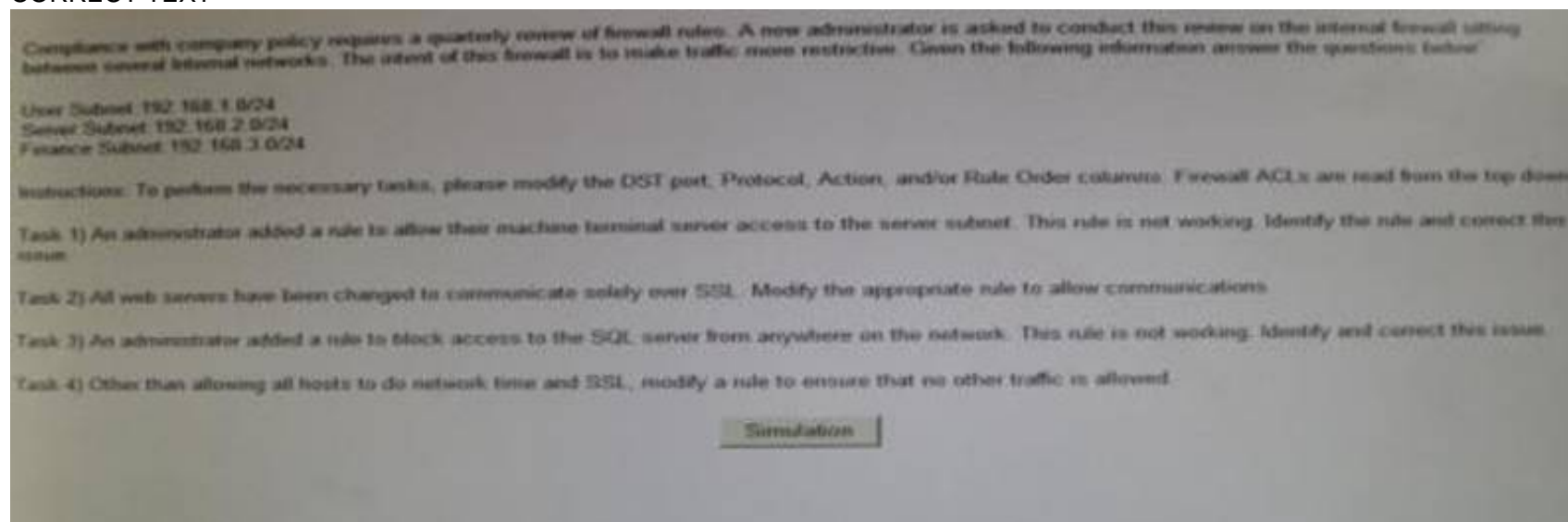
Answer: B

NEW QUESTION 363
A security administrator must implement a SCADA style network overlay to ensure secure remote management of all network management and infrastructure devices. Which of the following BEST describes the rationale behind this architecture?

A. A physically isolated network that allows for secure metric collection.
B. A physically isolated network with inband management that uses two factor authentication.
C. A logically isolated network with inband management that uses secure two factor authentication.
D. An isolated network that provides secure out-of-band remote management.

Answer: D

NEW QUESTION 366
CORRECT TEXT
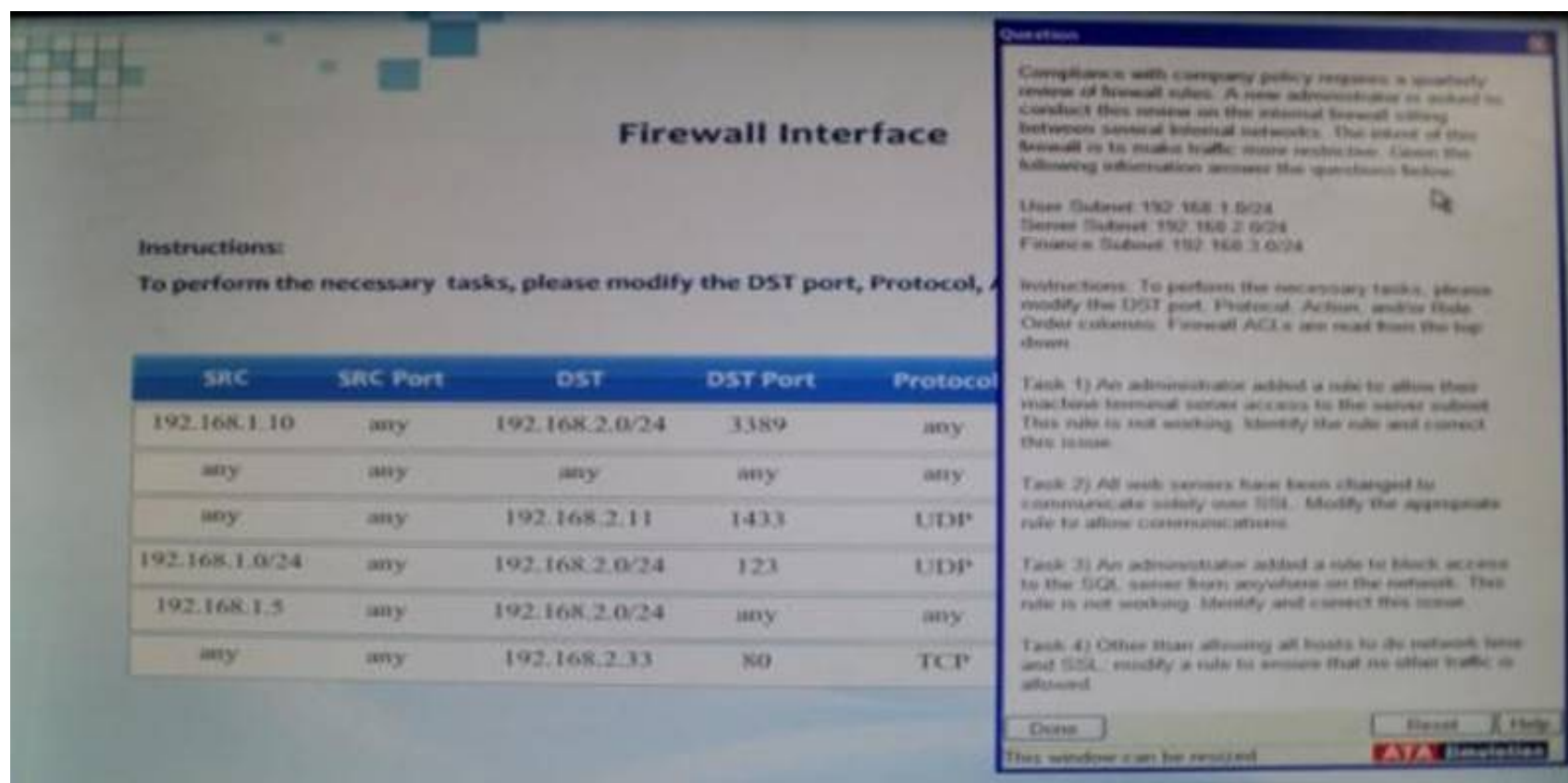
Answer:

NEW QUESTION 368
A security administrator at a Lab Company is required to implement a solution which will provide the highest level of confidentiality possible to all data on the lab network.
The current infrastructure design includes:
The network is protected with a firewall implementing ACLs, a NIPS device, and secured wireless access points.
Which of the following cryptographic improvements should be made to the current architecture to achieve the stated goals?

A. PKI based authorization
B. Transport encryption
C. Data at rest encryption
D. Code signing

Answer: B

NEW QUESTION 369
A security consultant is hired by a company to determine if an internally developed web application is vulnerable to attacks. The consultant spent two weeks testing the application, and determines that no vulnerabilities are present. Based on the results of the tools and tests available, which of the following statements BEST reflects the security status of the application?

A. The company's software lifecycle management improved the security of the application.
B. There are no vulnerabilities in the application.
C. The company should deploy a web application firewall to ensure extra security.
D. There are no known vulnerabilities at this time.

Answer: D

NEW QUESTION 373
An administrator receives reports that the network is running slow for users connected to a certain switch. Viewing the network traffic, the administrator reviews the following:
18:51:59.042108 IP linuxwksta.55467 > dns.company.com.domain: 39462+ PTR? 222.17.4.10.in-addr.arpa. (42)
18:51:59.055732 IP dns.company.com.domain > linuxwksta.55467: 39462 NXDomain 0/0/0 (42)
18:51:59.055842 IP linuxwksta.48287 > dns.company.com.domain: 46767+ PTR? 255.19.4.10.in-addr.arpa. (42)
18:51:59.069816 IP dns.company.com.domain > linuxwksta.48287: 46767 NXDomain 0/0/0 (42)
18:51:59.159060 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [P.], seq 1989625106:1989625154, ack 2067334822, win 1525, options [nop,nop,TS val 16021424
ecr 215646227], length 48
18:51:59.159145 IP linuxwksta.48854 > dns.company.com.domain: 3834+ PTR? 72.17.4.10.in-addr.arpa. (41)
18:51:59.159314 IP 10.4.17.72.iscsi-target > linuxwksta.42491: Flags [P.], seq 1:49, ack 48, win 124, options [nop,nop,TS val 215647479 ecr 16021424], length 48
18:51:59.159330 IP linuxwksta.42491 > 10.4.17.72.iscsi-target: Flags [.], ack 49, win 1525, options [nop,nop,TS val 16021424 ecr 215647479], length 0
18:51:59.165342 IP dns.company.com.domain > linuxwksta.48854: 3834 NXDomain 0/0/0 (41)
18:51:59.397461 ARP, Request who-has 10.4.16.58 tell 10.4.16.1, length 46 18:51:59.397597 IP linuxwksta.37684 > dns.company.com.domain: 15022+ PTR?
58.16.4.10.in-addr.arpa. (41)
Given the traffic report, which of the following is MOST likely causing the slow traffic?

A. DNS poisoning
B. Improper network zoning
C. ARP poisoning
D. Improper LUN masking

Answer: B

NEW QUESTION 377
CORRECT TEXT
An administrator wants to install a patch to an application. Given the scenario, download, verify and install the patch in the most secure manner. Instructions The last install that is completed will be the final submission
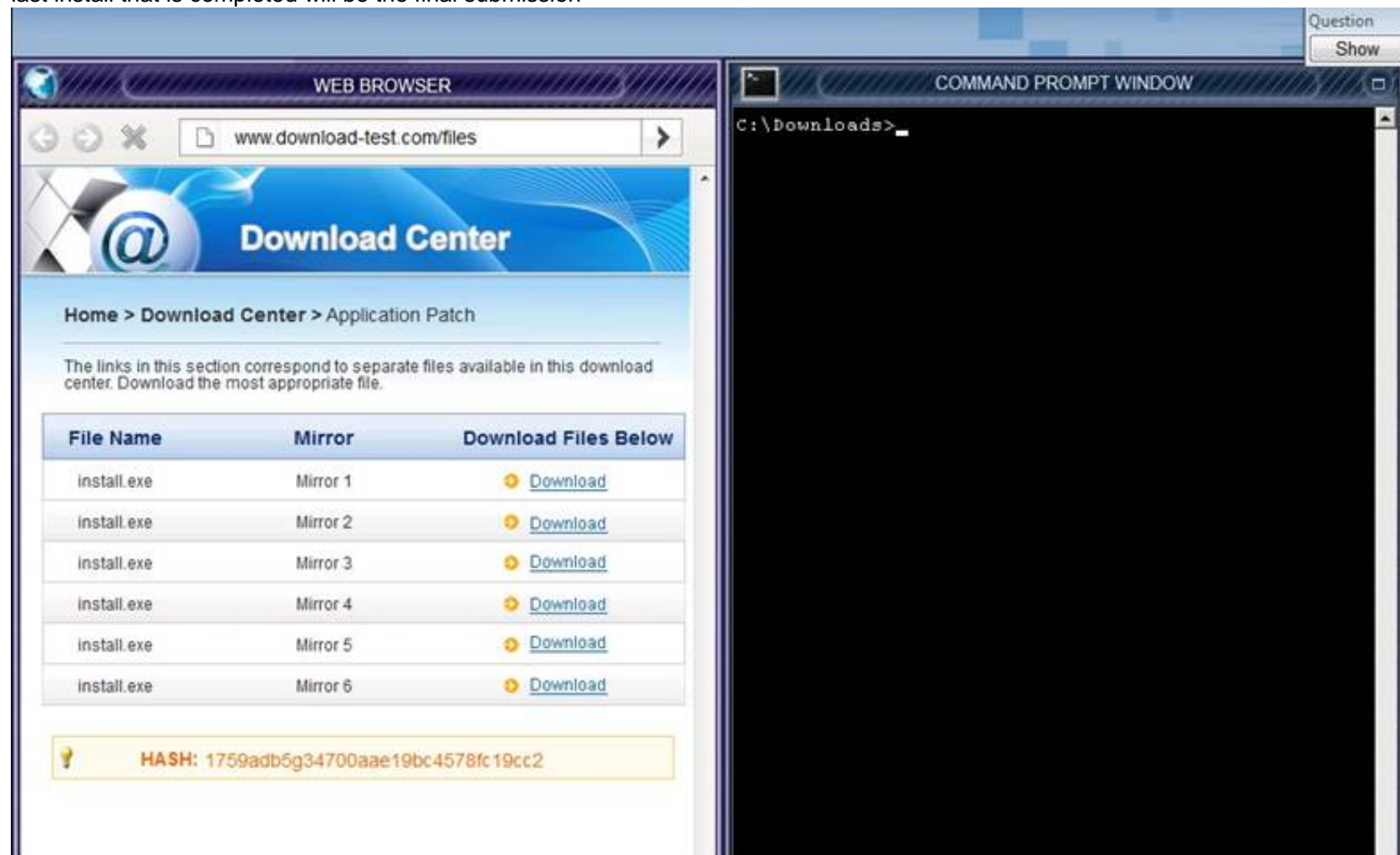
Answer:

NEW QUESTION 382
The marketing department at Company A regularly sends out emails signed by the company's Chief Executive Officer (CEO) with announcements about the company. The CEO sends company and personal emails from a different email account. During legal proceedings against the company, the Chief Information Officer (CIO) must prove which emails came from the CEO and which came from the marketing department. The email server allows emails to be digitally signed and the corporate PKI provisioning allows for one certificate per user. The CEO did not share their password with anyone. Which of the following will allow the CIO to state which emails the CEO sent and which the marketing department sent?

A. Identity proofing
B. Non-repudiation
C. Key escrow
D. Digital rights management

Answer: B

NEW QUESTION 386
A manager who was attending an all-day training session was overdue entering bonus and payroll information for subordinates. The manager felt the best way to get the changes entered while in training was to log into the payroll system, and then activate desktop sharing with a trusted subordinate. The manager granted the subordinate control of the desktop thereby giving the subordinate full access to the payroll system. The subordinate did not have authorization to be in the payroll system. Another employee reported the incident to the security team. Which of the following would be the MOST appropriate method for dealing with this issue going forward?

A. Provide targeted security awareness training and impose termination for repeat violators.
B. Block desktop sharing and web conferencing applications and enable use only with approval.
C. Actively monitor the data traffic for each employee using desktop sharing or web conferencing applications.
D. Permanently block desktop sharing and web conferencing applications and do not allow its use at the company.

Answer: A

NEW QUESTION 388
The Chief Technology Officer (CTO) has decided that servers in the company datacenter should be virtualized to conserve physical space. The risk assurance officer is concerned that the project team in charge of virtualizing servers plans to co-mingle many guest operating systems with different security requirements to speed up the rollout and reduce the number of host operating systems or hypervisors required.
Which of the following BEST describes the risk assurance officer's concerns?

A. Co-mingling guest operating system with different security requirements allows guest OS privilege elevation to occur within the guest OS via shared memory allocation with the host OS.
B. Co-mingling of guest operating systems with different security requirements increases the risk of data loss if the hypervisor fails.
C. A weakly protected guest OS combined with a host OS exploit increases the chance of a successful VMEscape attack being executed, compromising the hypervisor and other guest OS.
D. A weakly protected host OS will allow the hypervisor to become corrupted resulting in
E. data throughput performance issues.

Answer: C

NEW QUESTION 393
......

Thank You for Trying Our Product

* 100% Pass or Money Back

     All our products come with a 90-day Money Back Guarantee.

* One year free update

     You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

     We currently serve more than 30,000,000 customers.

* Shop Securely

     All transactions are protected by VeriSign!

100% Pass Your CAS-002 Exam with Our Prep Materials Via below:

https://www.certleader.com/CAS-002-dumps.html