ExamCost

Try before you buy

Download a free sample of any of our exam questions and answers

Download Demo

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Quality and Value

ExamCost Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

Tested and Approved

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our ExamCost testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

ExamCost offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

http://www.examcost.com

ExamCost provides valid exam collection and save exam cost

Exam : **CAS-002**

Title : CompTIA Advanced Security Practitioner (CASP)

Vendor : CompTIA

Version : DEMO

NO.1 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

NO.2 An Association is preparing to upgrade their firewalls at five locations around the United States. Each of the three vendor's RFP responses is in-line with the security and other requirements. Which of the following should the security administrator do to ensure the firewall platform is appropriate for the Association?

A. Correlate current industry research with the RFP responses to ensure validity.

B. Create a lab environment to evaluate each of the three firewall platforms.

C. Benchmark each firewall platform's capabilities and experiences with similar sized companies.

D. Develop criteria and rate each firewall platform based on information in the RFP responses.

Answer: B

NO.3 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

NO.4 A corporation has expanded for the first time by integrating several newly acquired businesses. Which of the following are the FIRST tasks that the security team should undertake? (Select TWO).

A. Re-image all end user computers to a standard image.

B. Remove acquired companies Internet access.

C. Install firewalls between the businesses.

D. Conduct a risk analysis of each acquired company's networks.
E. Develop interconnection policy.
F. Federate identity management systems.
Answer: D,E

NO.5 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

NO.6 Every year, the accounts payable employee, Ann, takes a week off work for a vacation.
She typically completes her responsibilities remotely during this week. Which of the following policies, when implemented, would allow the company to audit this employee's work and potentially discover improprieties?
A. Job rotation
B. Mandatory vacations
C. Least privilege
D. Separation of duties
Answer: A

NO.7 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

NO.8 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

NO.9 -- Exhibit --

	Client	Protocol	File Exchange	Emoticons	Group Chat	Video Chat
Product A	Proprietary Windows/Mac/Linux	IRC over TLS	Yes FTP	65	Up to 5	2 Party Flash video
Product B	Open Source Windows/Mac/Linux	Jabber	No	55	Up to 5	3 Party Flash video
Product C	Proprietary Windows/Linux	XMPP over TLS	Yes SCP	120	Up to 10	2 Party using H.323 over TLS
Product D	Open Source Windows/Mac	SIP	Yes RCP	25	Up to 5	2 Party H.323

-- Exhibit --

Company management has indicated that instant messengers (IM) add to employee productivity. Management would like to implement an IM solution, but does not have a budget for the project. The security engineer creates a feature matrix to help decide the most secure product. Click on the Exhibit button.

Which of the following would the security engineer MOST likely recommend based on the table?

A. Product A

B. Product B

C. Product C

D. Product D

Answer: C

NO.10 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

9 0.76.165.40 - - [08/Mar/2014:10:54:05] "GET ../../../root/.bash_history HTTP/1.1" 200 5 724

90.76.165.40 - - [08/Mar/2014:10:54:04] "GET index.php?user=<script>Create</script> HTTP/1.1" 20 0 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

NO.11 A new company requirement mandates the implementation of multi-factor authentication to access network resources. The security administrator was asked to research and implement the most cost-effective solution that would allow for the authentication of both hardware and users. The company wants to leverage the PKI infrastructure which is already well established. Which of the following solutions should the security administrator implement?

A. Issue individual private/public key pairs to each user, install the private key on the central authentication system, and protect the private key with the user's credentials.
Require each user to install the public key on their computer.

B. Deploy USB fingerprint scanners on all desktops, and enable the fingerprint scanner on all laptops. Require all network users to register their fingerprint using the reader and store the information in the central authentication system.

C. Issue each user one hardware token. Configure the token serial number in the user properties of the central authentication system for each user and require token authentication with PIN for network logon.

D. Issue individual private/public key pairs to each user, install the public key on the central authentication system, and require each user to install the private key on their computer and protect it with a password.

Answer: D

NO.12 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

NO.13 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

NO.14 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

NO.15 A security researcher is about to evaluate a new secure VoIP routing appliance. The appliance manufacturer claims the new device is hardened against all known attacks and several un-disclosed zero day exploits. The code base used for the device is a combination of compiled C and TC/TKL scripts. Which of the following methods should the security research use to enumerate the ports and protocols in use by the appliance?
A. Device fingerprinting
B. Switchport analyzer
C. Grey box testing
D. Penetration testing
Answer: A

NO.16 A large bank deployed a DLP solution to detect and block customer and credit card data from leaving the organization via email. A disgruntled employee was able to successfully exfiltrate data through the corporate email gateway by embedding a word processing document containing sensitive data as an object in a CAD file. Which of the following BEST explains why it was not detected and blocked by the DLP solution? (Select TWO).
A. The embedding of objects in other documents enables document encryption by default.
B. The process of embedding an object obfuscates the data.
C. The mail client used to send the email is not compatible with the DLP product.
D. The DLP product cannot scan multiple email attachments at the same time.
Answer: A,C

NO.17 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

NO.18 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

NO.19 In an effort to reduce internal email administration costs, a company is determining whether to outsource its email to a managed service provider that provides email, spam, and malware protection. The security manager is asked to provide input regarding any security implications of this change.
Which of the following BEST addresses risks associated with disclosure of intellectual property?
A. Require the managed service provider to implement additional data separation.
B. Require encrypted communications when accessing email.
C. Enable data loss protection to minimize emailing PII and confidential data.
D. Establish an acceptable use policy and incident response policy.
Answer: C

NO.20 A company is preparing to upgrade its NIPS at five locations around the world. The three platforms the team plans to test, claims to have the most advanced features and lucrative pricing. Assuming all platforms meet the functionality requirements, which of the following methods should be used to select the BEST platform?
A. Establish return on investment as the main criteria for selection.
B. Run a cost/benefit analysis based on the data received from the RFP.
C. Evaluate each platform based on the total cost of ownership.
D. Develop a service level agreement to ensure the selected NIPS meets all performance requirements.
Answer: C

NO.21 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.

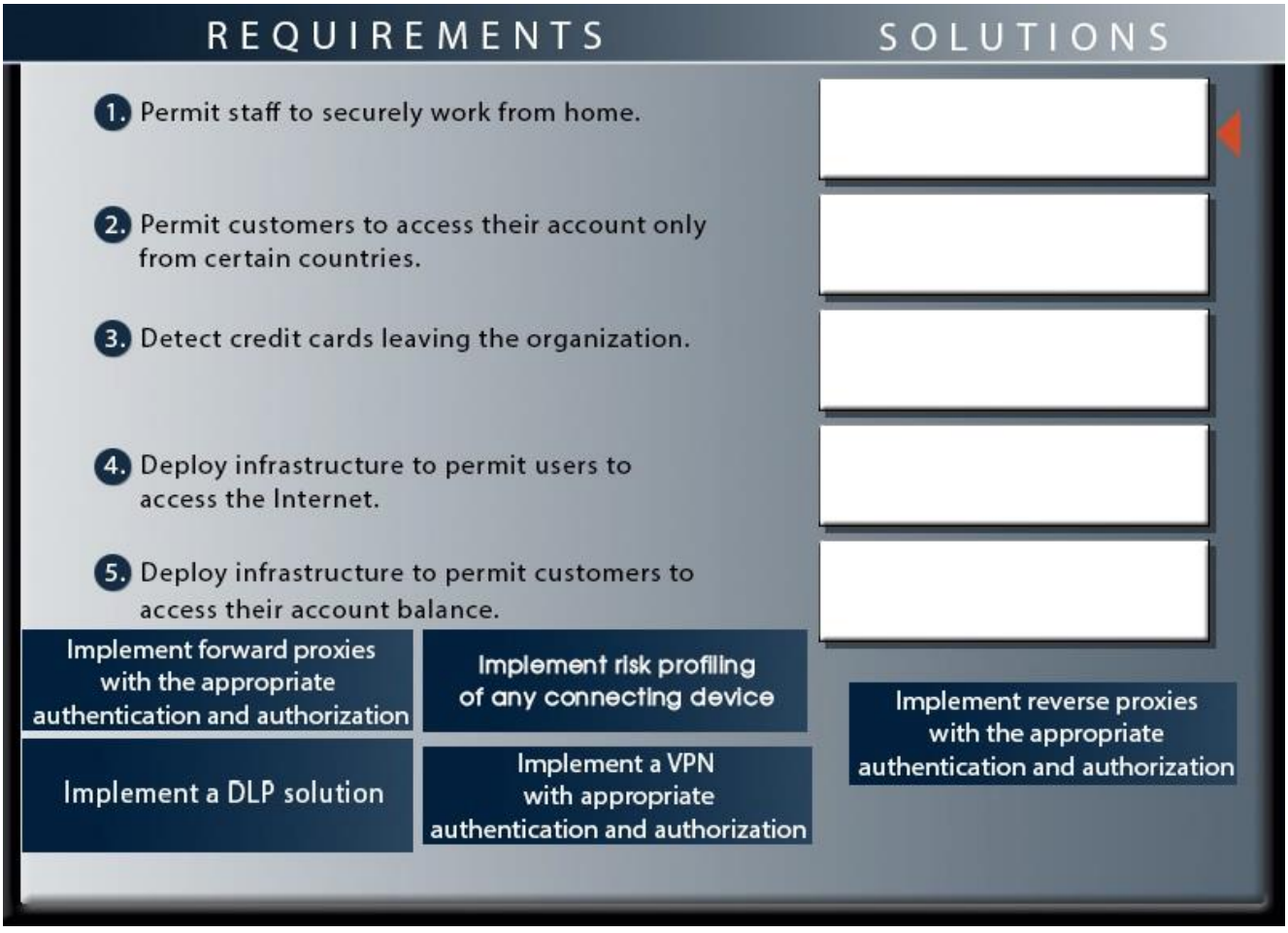
C. The companies should federate, with the parent becoming the IdP, and the subsidiaries becoming an SP.

D. The companies should federate, with the parent becoming the ASP, and the subsidiaries becoming an IdP.

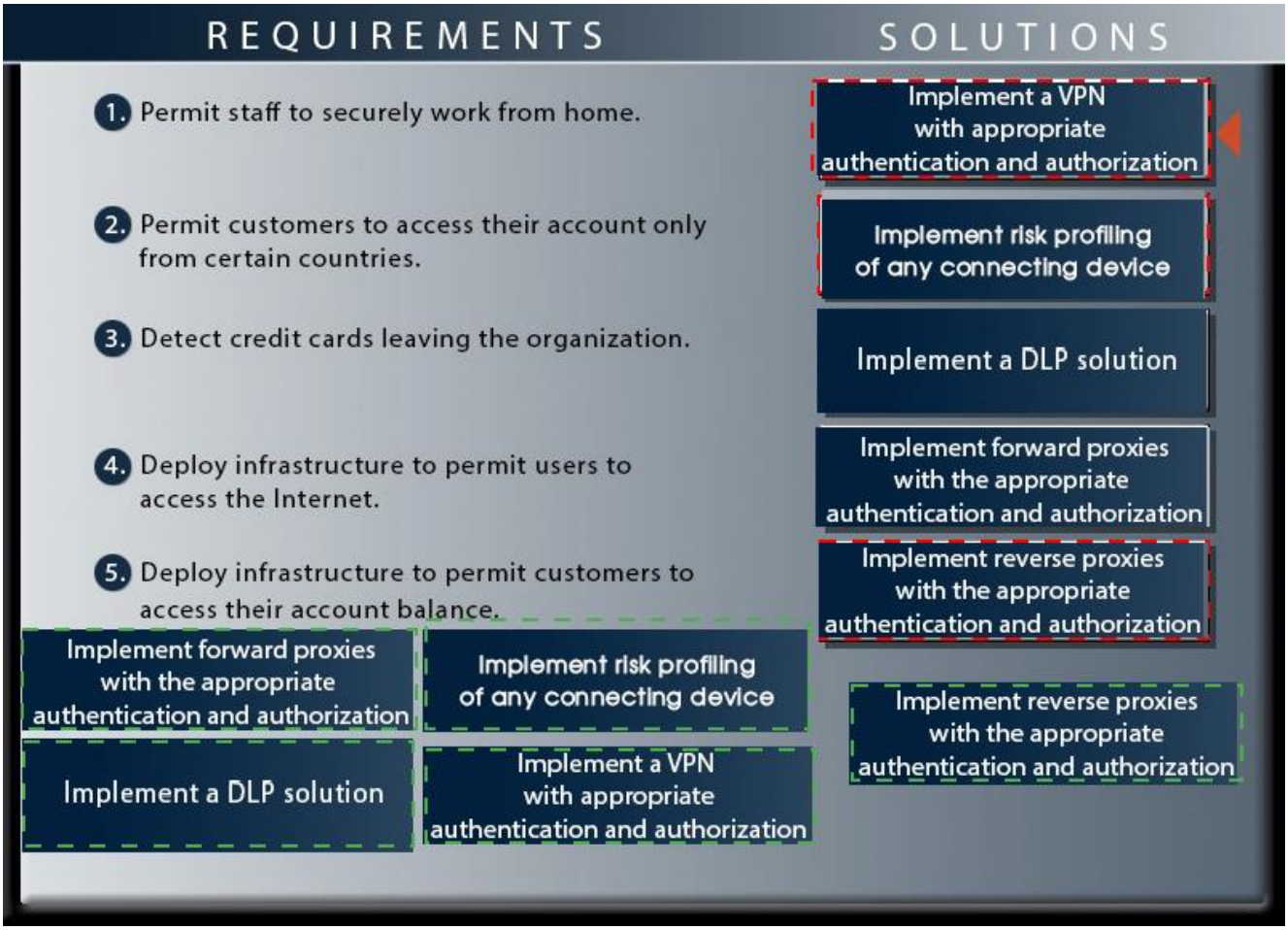
Answer: C

NO.22 DRAG DROP

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:


REQUIREMENTS
SOLUTIONS
1. Permit staff to securely work from home.
2. Permit customers to access their account only from certain countries.
3. Detect credit cards leaving the organization.
4. Deploy infrastructure to permit users to access the Internet.
5. Deploy infrastructure to permit customers to access their account balance.
Implement a VPN with appropriate authentication and authorization
Implement risk profiling of any connecting device
Implement a DLP solution
Implement forward proxies with the appropriate authentication and authorization
Implement reverse proxies with the appropriate authentication and authorization
Implement forward proxies with the appropriate authentication and authorization
Implement risk profiling of any connecting device
Implement a DLP solution
Implement a VPN with appropriate authentication and authorization
Implement reverse proxies with the appropriate authentication and authorization