CAS-002$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner Exam

Pass CompTIA CAS-002 Exam with 100% Guarantee

QUESTION 1

A WAF without customization will protect the infrastructure from which of the following attack combinations?

A. DDoS, DNS poisoning, Boink, Teardrop

B. Reflective XSS, HTTP exhaustion, Teardrop

C. SQL Injection, DOM based XSS, HTTP exhaustion

D. SQL Injection, CSRF, Clickjacking

Correct Answer: C

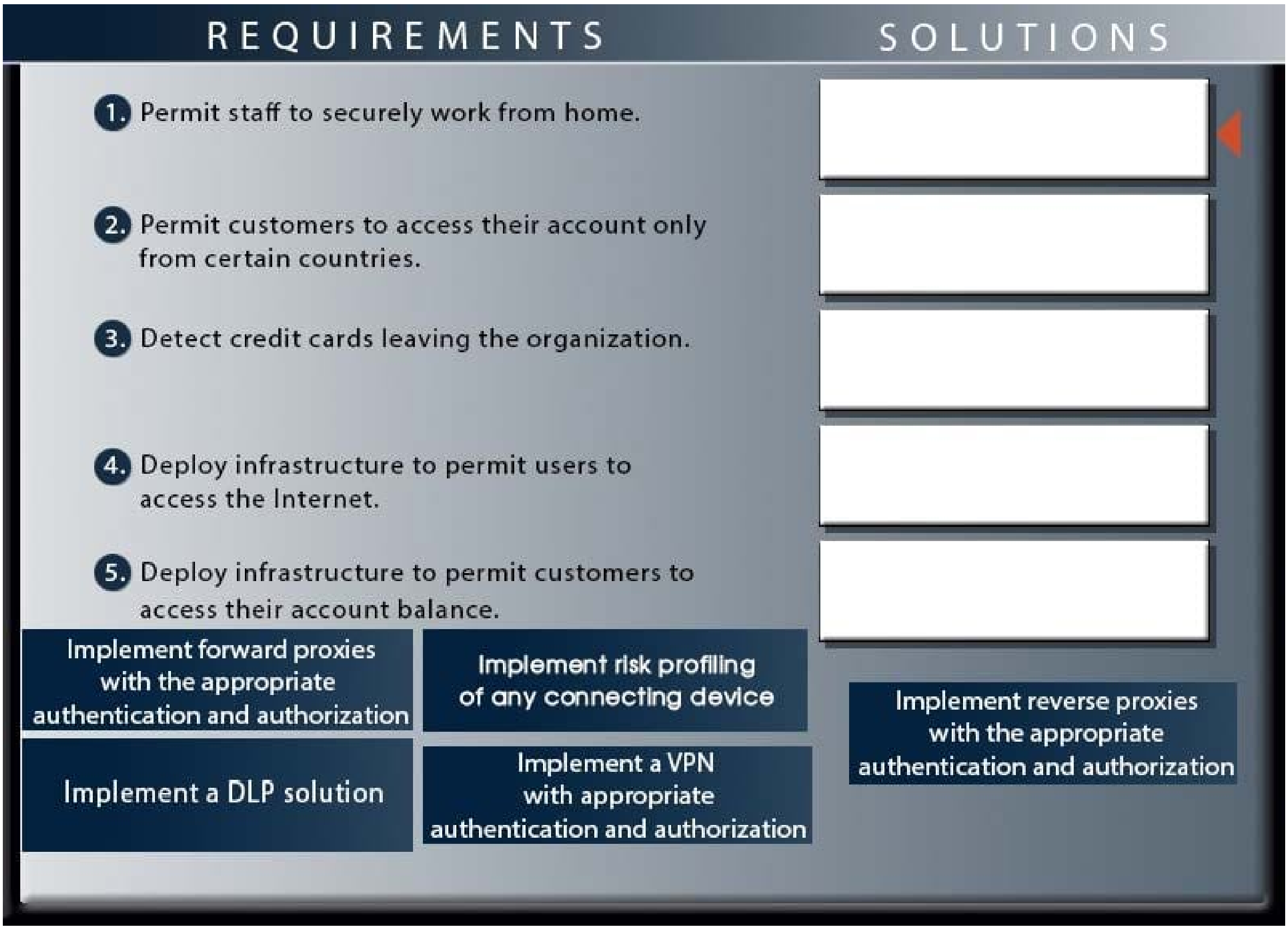
QUESTION 2

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.

Select and Place:



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 forward proxies with the appropriate authentication and authorization

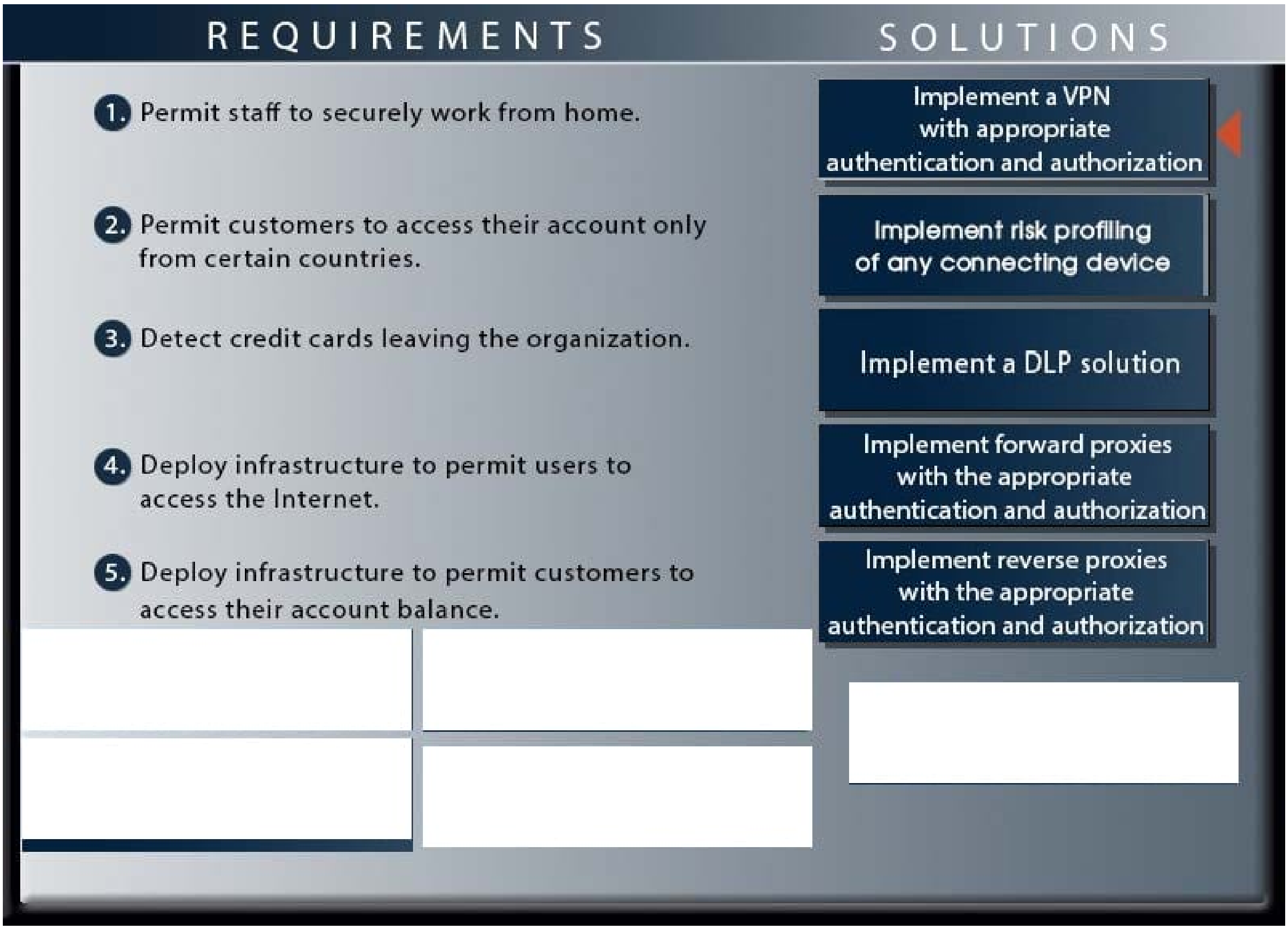
Implement risk profiling of any connecting device

Implement reverse proxies with the appropriate authentication and authorization

Implement a DLP solution

Implement a VPN with appropriate authentication and authorization

Correct Answer:



REQUIREMENTS

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.

SOLUTIONS

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

QUESTION 3

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. Web vulnerability scanner

Correct Answer: CD

QUESTION 4

A security auditor is conducting an audit of a corporation where 95% of the users travel or work from non- corporate locations a majority of the time. While the employees are away from the corporate offices, they retain full access to the corporate network and use of corporate laptops. The auditor knows that the corporation processes PII and other sensitive data with applications requiring local caches of any data being manipulated. Which of the following security controls should the auditor check for and recommend to be implemented if missing from the laptops?

A. Trusted operating systems

B. Full disk encryption

C. Host-based firewalls

D. Command shell restrictions

Correct Answer: B

QUESTION 5

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

Correct Answer: DE

QUESTION 6

A security audit has uncovered that some of the encryption keys used to secure the company B2B financial transactions with its partners may be too weak. The security administrator needs to implement a process to ensure that financial transactions will not be compromised if a weak encryption key is found. Which of the following should the security administrator implement?

A. Entropy should be enabled on all SSLv2 transactions.

B. AES256-CBC should be implemented for all encrypted data.

C. PFS should be implemented on all VPN tunnels.

D. PFS should be implemented on all SSH connections.

Correct Answer: C

QUESTION 7

A company has migrated its data and application hosting to a cloud service provider (CSP). To meet its future needs, the company considers an IdP. Why might the company want to select an IdP that is separate from its CSP? (Select TWO).

A. A circle of trust can be formed with all domains authorized to delegate trust to an IdP

B. Identity verification can occur outside the circle of trust if specified or delegated

C. Replication of data occurs between the CSP and IdP before a verification occurs

D. Greater security can be provided if the circle of trust is formed within multiple CSP domains

E. Faster connections can occur between the CSP and IdP without the use of SAML

Correct Answer: AD

QUESTION 8

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.

Correct Answer: CD

QUESTION 9

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

Correct Answer: B

QUESTION 10

An intrusion detection system logged an attack attempt from a remote IP address. One week later, the attacker successfully compromised the network. Which of the following MOST likely occurred?

A. The IDS generated too many false negatives.

B. The attack occurred after hours.

C. The IDS generated too many false positives.

D. No one was reviewing the IDS event logs.

Correct Answer: D

QUESTION 11

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

Correct Answer: DG

QUESTION 12

Several business units have requested the ability to use collaborative web-based meeting places with third party vendors. Generally these require user registration, installation of client-based ActiveX or Java applets, and also the ability for the user to share their desktop in read-only or read-write mode. In order to ensure that information security is not compromised, which of the following controls is BEST suited to this situation?

A. Disallow the use of web-based meetings as this could lead to vulnerable client-side components being installed, or a malicious third party gaining read-write control over an internal workstation.

B. Hire an outside consultant firm to perform both a quantitative and a qualitative risk- based assessment. Based on the outcomes, if any risks are identified then do not allow web-based meetings. If no risks are identified then go forward and allow for these meetings to occur.

C. Allow the use of web-based meetings, but put controls in place to ensure that the use of these meetings is logged and tracked.

D. Evaluate several meeting providers. Ensure that client-side components do not introduce undue security risks. Ensure that the read-write desktop mode can either be prevented or strongly audited.

Correct Answer: D

QUESTION 13

A Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:

Vendor A: product-based solution which can be purchased by the pharmaceutical company. Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year. Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company\\'s needs.

Bundled offering expected to be $100,000 per year.

Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.

Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?

A. Based on cost alone, having an outsourced solution appears cheaper.

B. Based on cost alone, having an outsourced solution appears to be more expensive.

C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.

D. Based on cost alone, having a purchased product solution appears cheaper.

Correct Answer: A

QUESTION 14

Company ABC has entered into a marketing agreement with Company XYZ, whereby ABC will share some of its customer information with XYZ. However, XYZ can only contact ABC customers who explicitly agreed to being contacted by third parties. Which of the following documents would contain the details of this marketing agreement?

A. BPA

B. ISA

C. NDA

D. SLA

Correct Answer: A

QUESTION 15

A manufacturing company is having issues with unauthorized access and modification of the controls operating the production equipment. A communication requirement is to allow the free flow of data between all network segments at the site. Which of the following BEST remediates the issue?

A. Implement SCADA security measures.

B. Implement NIPS to prevent the unauthorized activity.

C. Implement an AAA solution.

D. Implement a firewall to restrict access to only a single management station.

Correct Answer: C

Latest CAS-002 Dumps   CAS-002 Study Guide   CAS-002 Exam Questions