CERTSWARRIOR

Comptia

CAS-003
CompTIA Advanced Security Practitioner

Questions & Answers PDF

For More Information:

https://www.certswarrior.com/

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Question: 1

An organization is improving its web services to enable better customer engagement and self-service. The organization has a native mobile application and a rewards portal provided by a third party. The business wants to provide customers with the ability to log in once and have SSO between each of the applications. The integrity of the identity is important so it can be propagated through to back-end systems to maintain a consistent audit trail. Which of the following authentication and authorization types BEST meet the requirements? (Choose two.)

A. SAML
B. Social login
C. OpenID connect
D. XACML
E. SPML
F. OAuth

Answer: B,C

Question: 2

After the departure of a developer under unpleasant circumstances, the company is concerned about the security of the software to which the developer has access. Which of the following is the BEST way to ensure security of the code following the incident?

A. Hire an external red tem to conduct black box testing
B. Conduct a peer review and cross reference the SRTM
C. Perform white-box testing on all impacted finished products
D. Perform regression testing and search for suspicious code

Answer: A

Question: 3

A software company is releasing a new mobile application to a broad set of external customers. Because the software company is rapidly releasing new features, it has built in an over-the-air software update process that can automatically update the application at launch time. Which of the following security controls should be recommended by the company's security architect to protect the integrity of the update process? (Choose two.)

A. Validate cryptographic signatures applied to software updates
B. Perform certificate pinning of the associated code signing key
C. Require HTTPS connections for downloads of software updates

D. Ensure there are multiple download mirrors for availability
E. Enforce a click-through process with user opt-in for new features

Answer: A,B

Question: 4

A Chief Information Security Officer (CISO) is developing a new BIA for the organization. The CISO wants to gather requirements to determine the appropriate RTO and RPO for the organization's ERP. Which of the following should the CISO interview as MOST qualified to provide RTO/RPO metrics?

A. Data custodian
B. Data owner
C. Security analyst
D. Business unit director
E. Chief Executive Officer (CEO)

Answer: D

Question: 5

A Chief Information Security Officer (CISO) requests the following external hosted services be scanned for malware, unsecured PII, and healthcare data:
Corporate intranet site
Online storage application
Email and collaboration suite
Security policy also is updated to allow the security team to scan and detect any bulk downloads of corporate data from the company's intranet and online storage site. Which of the following is needed to comply with the corporate security policy and the CISO's request?

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

Answer: B

Question: 6

Several recent ransomware outbreaks at a company have cost a significant amount of lost revenue. The security team needs to find a technical control mechanism that will meet the following requirements and aid in preventing these outbreaks:
Stop malicious software that does not match a signature
Report on instances of suspicious behavior
Protect from previously unknown threats
Augment existing security capabilities
Which of the following tools would BEST meet these requirements?

A. Host-based firewall
B. EDR
C. HIPS
D. Patch management

Answer: C

Question: 7

A company that has been breached multiple times is looking to protect cardholder data. The previous undetected attacks all mimicked normal administrative-type behavior. The company must deploy a host solution to meet the following requirements:
Detect administrative actions
Block unwanted MD5 hashes
Provide alerts
Stop exfiltration of cardholder data
Which of the following solutions would BEST meet these requirements? (Choose two.)

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

Answer: B,E

Question: 8

A security engineer is employed by a hospital that was recently purchased by a corporation. Throughout the acquisition process, all data on the virtualized file servers must be shared by departments within both organizations. The security engineer considers data ownership to determine:

A. the amount of data to be moved.
B. the frequency of data backups.

C. which users will have access to which data
D. when the file server will be decommissioned

Answer: C

Question: 9

A security analyst is reviewing the following packet capture of communication between a host and a company's router:

```
1 192.168.1.10 -> 10.5.10.1 icmp echo request 33 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZ
2 10.5.10.1 -> 192.168.1.10 icmp echo reply 34 bytes sent ABCDEFGHIJKLMNOPQRSTUVWXYZA%MDKF8
```

Which of the following actions should the security analyst take to remove this vulnerability?

A. Update the router code
B. Implement a router ACL
C. Disconnect the host from the network
D. Install the latest antivirus definitions
E. Deploy a network-based IPS

Answer: B

Question: 10

An information security manager conducted a gap analysis, which revealed a 75% implementation of security controls for high-risk vulnerabilities, 90% for medium vulnerabilities, and 10% for low-risk vulnerabilities. To create a road map to close the identified gaps, the assurance team reviewed the likelihood of exploitation of each vulnerability and the business impact of each associated control. To determine which controls to implement, which of the following is the MOST important to consider?

A. KPI
B. KRI
C. GRC
D. BIA

Answer: C

Question: 11

A development team is testing an in-house-developed application for bugs. During the test, the application crashes several times due to null pointer exceptions. Which of the following tools, if integrated into an IDE during coding, would identify these bugs routinely?

A. Issue tracker
B. Static code analyzer
C. Source code repository
D. Fuzzing utility

Answer: D

Question: 12

A legacy web application, which is being used by a hospital, cannot be upgraded for 12 months. A new vulnerability is found in the legacy application, and the networking team is tasked with mitigation. Middleware for mitigation will cost $100,000 per year. Which of the following must be calculated to determine ROI? (Choose two.)

A. ALE
B. RTO
C. MTBF
D. ARO
E. RPO

Answer: A,D

Question: 13

A security engineer is assisting a developer with input validation, and they are studying the following code block:

```
string accountIdRegexp = "TODO, help!";
private static final Pattern accountIdPattern = Pattern.compile
("accountIdRegexp");
String accountId = request.getParameter("accountNumber");
if (!accountIdPattern.matcher(accountId).matches() {
      System.out.println("account ID format incorrect");
} else {
      // continue
}
```

The security engineer wants to ensure strong input validation is in place for customer-provided account identifiers. These identifiers are ten-digit numbers. The developer wants to ensure input validation is fast because a large number of people use the system.
Which of the following would be the BEST advice for the security engineer to give to the developer?

A. Replace code with Java-based type checks
B. Parse input into an array
C. Use regular expressions

D. Canonicalize input into string objects before validation

Answer: C

Question: 14

A project manager is working with a software development group to collect and evaluate user stories related to the organization's internally designed CRM tool. After defining requirements, the project manager would like to validate the developer's interpretation and understanding of the user's request. Which of the following would BEST support this objective?

A. Peer review
B. Design review
C. Scrum
D. User acceptance testing
E. Unit testing

Answer: C

Question: 15

A network printer needs Internet access to function. Corporate policy states all devices allowed on the network must be authenticated. Which of the following is the MOST secure method to allow the printer on the network without violating policy?

A. Request an exception to the corporate policy from the risk management committee
B. Require anyone trying to use the printer to enter their username and password
C. Have a help desk employee sign in to the printer every morning
D. Issue a certificate to the printer and use certificate-based authentication

Answer: D

Question: 16

The Chief Information Security Officer (CISO) of an established security department, identifies a customer who has been using a fraudulent credit card. The CISO calls the local authorities, and when they arrive on-site, the authorities ask a security engineer to create a point-in-time copy of the running database in their presence. This is an example of:

A. creating a forensic image
B. deploying fraud monitoring
C. following a chain of custody

D. analyzing the order of volatility

Answer: C

Question: 17

A technician is configuring security options on the mobile device manager for users who often utilize public Internet connections while travelling. After ensuring that full disk encryption is enabled, which of the following security measures should the technician take? (Choose two.)

A. Require all mobile device backups to be encrypted
B. Ensure all mobile devices back up using USB OTG
C. Issue a remote wipe of corporate and personal partitions
D. Restrict devices from making long-distance calls during business hours
E. Implement an always-on VPN

Answer: C,E

Question: 18

A systems administrator receives an advisory email that a recently discovered exploit is being used in another country and the financial institutions have ceased operations while they find a way to respond to the attack. Which of the following BEST describes where the administrator should look to find information on the attack to determine if a response must be prepared for the systems? (Choose two.)

A. Bug bounty websites
B. Hacker forums
C. Antivirus vendor websites
D. Trade industry association websites
E. CVE database
F. Company's legal department

Answer: E,F

Question: 19

A security assessor is working with an organization to review the policies and procedures associated with managing the organization's virtual infrastructure. During a review of the virtual environment, the assessor determines the organization is using servers to provide more than one primary function, which violates a regulatory requirement. The assessor reviews hardening guides and determines policy allows for this configuration. It would be MOST appropriate for the assessor to advise the organization to:

A. segment dual-purpose systems on a hardened network segment with no external access
B. assess the risks associated with accepting non-compliance with regulatory requirements
C. update system implementation procedures to comply with regulations
D. review regulatory requirements and implement new policies on any newly provisioned servers

Answer: A

Question: 20

While conducting a BIA for a proposed acquisition, the IT integration team found that both companies outsource CRM services to competing and incompatible third-party cloud services. The decision has been made to bring the CRM service in-house, and the IT team has chosen a future solution. With which of the following should the Chief Information Security Officer (CISO) be MOST concerned? (Choose two.)

A. Data remnants
B. Sovereignty
C. Compatible services
D. Storage encryption
E. Data migration
F. Chain of custody

Answer: C,E

Question: 21

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

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

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

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

Answer: E

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

20% Discount Coupon Code: 20off2019