Vendor: CompTIA

Exam Code:CAS-003

Exam Name: CompTIA Advanced Security Practitioner (CASP+)

Version: Demo

QUESTION 1

An application development company implements object reuse to reduce life-cycle costs for the company and its clients Despite the overall cost savings, which of the following BEST describes a security risk to customers inherent within this model?

A. Configurations of applications will affect multiple products.

B. Reverse engineering of applications will lead to intellectual property loss

C. Software patch deployment will occur less often

D. Homogeneous vulnerabilities will occur across multiple products

Correct Answer: D

QUESTION 2

The Chief Information Officer (CIO) has been asked to develop a security dashboard with the relevant metrics. The board of directors will use the dashboard to monitor and track the overall security posture of the organization. The CIO produces a basic report containing both KPI and KRI data in two separate sections for the board to review.

Which of the following BEST meets the needs of the board?

A. KRI:- Compliance with regulations- Backlog of unresolved security investigations- Severity of threats and vulnerabilities reported by sensors- Time to patch critical issues on a monthly basisKPI:- Time to resolve open security items- % of suppliers with approved security control frameworks- EDR coverage across the fleet- Threat landscape rating

B. KRI:- EDR coverage across the fleet- Backlog of unresolved security investigations- Time to patch critical issues on a monthly basis- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors

C. KRI:- EDR coverage across the fleet- % of suppliers with approved security control framework- Backlog of unresolved security investigations- Threat landscape ratingKPI:- Time to resolve open security items- Compliance with regulations-Time to patch critical issues on a monthly basis- Severity of threats and vulnerabilities reported by sensors

D. KPI:- Compliance with regulations- % of suppliers with approved security control frameworks- Severity of threats and vulnerabilities reported by sensors- Threat landscape ratingKRI:- Time to resolve open security items- Backlog of unresolved security investigations- EDR coverage across the fleet- Time to patch critical issues on a monthly basis

Correct Answer: A

QUESTION 3

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

Correct Answer: D

QUESTION 4

While attending a meeting with the human resources department, an organization\\'s information security officer sees an employee using a username and password written on a memo pad to log into a specific service. When the information security officer inquires further as to why passwords are being written down, the response is that there are too many passwords to remember for all the different services the human resources department is required to use.

Additionally, each password has specific complexity requirements and different expiration time frames. Which of the following would be the BEST solution for the information security officer to recommend?

A. Utilizing MFA

B. Implementing SSO

C. Deploying 802.1X

D. Pushing SAML adoption

E. Implementing TACACS

Correct Answer: B

QUESTION 5

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

Correct Answer: BD

QUESTION 6

A large, multinational company currently has two separate databases One is used for ERP while the second is used for CRM To consolidate services and infrastructure, it is proposed to combine the databases The company\\'s compliance manager is asked to review the proposal and is concerned about this integration Which of the following would pose the MOST concern to the compliance manager?

A. The attack surface of the combined database is lower than the previous separate systems, so there likely are wasted resources on additional security controls that will not be needed

B. There are specific regulatory requirements the company might be violating by combining these two types of services into one shared platform.

C. By consolidating services in this manner, there is an increased risk posed to the organization due to the number of resources required to manage the larger data pool.

D. Auditing the combined database structure will require more short-term resources, as the new system will need to be learned by the auditing team to ensure all security controls are in

Correct Answer: B

QUESTION 7

An organization relies heavily on third-party mobile applications for official use within a BYOD deployment scheme. An excerpt from an approved text-based-chat client application AndroidManifest.xml is as follows:

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="a.company.irocli
        ...
        <uses-permission android:name="android.permission.RECORD_AUDIO" />
        <uses-permission android:name="android.permission.SEND_SMS" />
        ...
</manifest>
```

Which of the following would restrict application permissions while minimizing the impact to normal device operations?

A. Add the application to the enterprise mobile whitelist.

B. Use the MDM to disable the devices\\' recording microphones and SMS

C. Wrap the application before deployment

D. Install the application outside of the corporate container

Correct Answer: A

QUESTION 8

Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the

requirements that it be easy to manage and provide capacity for growth.

The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth Utilization
St.Louis	18	50Mbps	20Mbps
Des Moines	12	25Mbps	19Mbps
Chicago	27	100Mbps	41Mbps
Rapid City	6	10Mbps	8Mbps
Indianapolis	7	12Mbps	8Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	150Mbps	Y	Y
B	60	400Mbps	N	Y
C	25	200Mbps	N	N
D	25	100Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO?

Which of the following would be the BEST option to recommend to the CIO?

A. Vendor C for small remote sites, and Vendor B for large sites.

B. Vendor B for all remote sites

C. Vendor C for all remote sites

D. Vendor A for all remote sites

E. Vendor D for all remote sites

Correct Answer: D

QUESTION 9

SIMULATION

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit.

This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print.

The command window will be provided along with root access. You are connected via a secure shell with root access.

You may query help for a list of commands.

Instructions:

You need to disable and turn off unrelated services and processes.

It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Correct Answer: Check the answer in explanation.

See the explanation below In Order to deactivate web services, database services and print service, we can do following things 1) deactivate its services /etc/init.d/apache2 stop /etc/init.d/mysqld stop 2) close ports for these services Web Server

iptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables save Print Server iptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables save

Database Server iptables -I INPUT -p tcp -m tcp --dport -j REJECTservice iptables save 3) Kill the process any running for the same ps -aef|grep mysql kill -9

QUESTION 10

A pharmacy gives its clients online access to their records and the ability to review bills and make payments. A new SSL vulnerability on a specific platform was discovered, allowing an attacker to capture the data between the end user and the web server providing these services. After the new vulnerability, it was determined that web services provided are being impacted by this new threat. Which of the following data types MOST likely at risk of exposure based on this new threat? (Select Two)

A. Cardholder data

B. Intellectual property

C. Personal health information

D. Employee records

E. Corporate financial data

Correct Answer: AC

QUESTION 11

A security analyst works for a defense contractor that produces classified research on drones. The contractor faces nearly constant attacks from sophisticated nation-state actors and other APIs. Which of the following would help protect the confidentiality of the research data?

A. Use diverse components in layers throughout the architecture

B. Implement non-heterogeneous components at the network perimeter

C. Purge all data remnants from client devices\\' volatile memory at regularly scheduled intervals

D. Use only in-house developed applications that adhere to strict SDLC security requirements

Correct Answer: A

QUESTION 12

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

Correct Answer: B

The Lessons Learned phase is the final step in the Incident Response process, when everyone involved reviews what happened and why.