Vendor: CompTIA

Exam Code:CA1-001

Exam Name: CompTIA Advanced Security Practitioner (CASP) Beta Exam

Version: Demo

QUESTION 1

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. What are the essential elements required for continuous monitoring?

Each correct answer represents a complete solution. Choose all that apply.

A. Ongoing assessment of system security controls

B. Security tools definition

C. Security status monitoring and reporting

D. Security impact analyses

E. Configuration management and change control

Correct Answer: ACDE

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Following are the four essential elements required for continuous monitoring:

Configuration management and change control

Security impact analyses

Ongoing assessment of system security controls

Security status monitoring and reporting

QUESTION 2

In which of the following phases of the system development life cycle (SDLC) is the primary implementation of the configuration management process performed?

A. Implementation

B. Operation/maintenance

C. Initiation

D. Acquisition/development

Correct Answer: B

The primary implementation of the configuration management process is performed during the operation/maintenance phase of the SDLC. The operation/maintenance phase describes that the system should be modified on a regular basis through the addition of hardware and software. Answer options C, D, and A are incorrect. The other phases are too early for this process to take place.

QUESTION 3

The help desk is flooded with calls from users who receive an e-mail warning about a new virus. The e-mail instructs them to search and delete a number of files from their systems. Many of them attempt to reboot the systems after deleting the specified files and find that the systems are not rebooting properly, which of the following types of attacks has occurred?

A. Hoax

B. Phishing

C. Spam

D. Pharming

Correct Answer: A

Hoax messages may warn of emerging threats that do not exist. These messages instruct users to delete certain files in order to ensure their security against a new virus, while actually only rendering the system more susceptible to later viral agents.

Answer option D is incorrect. Pharming is an attack made by a hacker in which the traffic of a Website is redirected to another bogus Website.

Answer option B is incorrect. Phishing is an attempt to obtain sensitive information by masquerading as a trustworthy entity using an electronic communication, such as e-mail. Answer option C is incorrect. Spam is an unwanted e-mail communication.

QUESTION 4

Fred is a network administrator for an insurance company. Lately there has been an issue with the antivirus software not updating. What is the first thing Fred should do to solve the problem?

A. Devise a plan to solve the problem

B. Clearly define the problem

C. Try reasonable alternatives

D. Consider probable causes

Correct Answer: B

The first step in problem solving is always to clearly define the problem. You have to fist be able to clearly define the problem before any other problem solving steps can be taken.

Answer option C is incorrect. You cannot try reasonable alternatives until you define the problem.

Answer option D is incorrect. Considering probable causes is an excellent idea, once you have defined the problem.

Answer option A is incorrect. You must first define the problem, then devise a plan before you have any chance of solving the problem.

QUESTION 5

Which of the following is a flexible set of design principles used during tine phases of systems development and integration?

A. Service-oriented modeling framework (SOMF)

B. Sherwood Applied Business Security Architecture (SABSA)

C. Service-oriented modeling and architecture (SOMA)

D. Service-oriented architecture (SOA)

Correct Answer: D

A service-oriented architecture (SOA) is a flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely integrated suite of services that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications- to be aware of available SOA-based services.

Answer option C is incorrect. The service-oriented modeling and architecture (SOMA) includes an analysis and design method that extends traditional object-oriented and component-based analysis and design methods to include concerns relevant to and supporting SOA. Answer option A is incorrect. The service-oriented modeling framework (SOMF) has been proposed by author Michael 8ell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems.

The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a service development scheme.

Answer option B is incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

QUESTION 6

Which of the following is the capability to correct flows in the existing functionality without affecting other components of the system?

A. Manageability

B. Reliability

C. Maintainability

D. Availability

Correct Answer: C

Availability: It is used to make certain that a service/resource is always accessible.

Manageability: It is the capability to manage the system for ensuring the constant health of the system with respect to scalability, reliability, availability, performance, and security.

Maintainability: It is the capability to correct flows in the existing functionality without affecting other components of the system.

Answer option B is incorrect. It is not a valid option.

QUESTION 7

Which of the following steps are involved in a generic cost-benefit analysis process: Each correct answer represents a complete solution. Choose three.

A. Compile a list of key players

B. Assess potential risks that may impact the solution

C. Select measurement and collect all cost and benefits elements

D. Establish alternative projects/programs

Correct Answer: ACD

The following steps are involved in a generic cost-benefit analysis process:

Establish alternative projects /programs

Compile a list of key players

Select measurement and collect all cost and benefits elements

Predict outcome of cost and benefits over the duration of the project

Put all effects of costs and benefits in dollars

Apply discount rate

Calculate net present value of project options

Sensitivity analysis

Recommendation

Answer option B is incorrect. It is not a valid step.

QUESTION 8

Your manager has approached you regarding her desire to outsource certain functions to an external firm. The manager would like for you to create a document for sending to three vendors asking them for solutions for these functions that your organization is to outsource. Which type of a procurement document will you create and send to the vendors to accomplish the task?

A. Request for Information

B. Invitation for Bid

C. Request for Proposal

D. Request for Quote

Correct Answer: C

According to the scenario, you will create and send the Request for Proposal procurement document.

QUESTION 9

Which of the following is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to?

A. NDA

B. SLA

C. OLA

D. SA

Correct Answer: A

A non-discloser agreement is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to.

QUESTION 10

Which of the following is an XML-based framework developed by OASIS and used to exchange user, resource and service provisioning information between cooperating organizations?

A. SOAP

B. SAML

C. SPML

D. XACML

Correct Answer: C

Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS (Organization for the Advancement of Structured Information Standards). It is used to exchange user, resource and service provisioning information between cooperating organizations.

SPML is the open standard for the integration and interoperation of service provisioning requests. It has a goal to allow organizations to securely and quickly set up user interfaces for Web applications and services, by letting enterprise platforms such as Web portals, application servers, and service centers produce provisioning requests within and across organizations. Answer option A is incorrect. SOAP, defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on extensible Markup Language as its message format, and usually relies on other Application Layer protocols for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Answer option D is incorrect. XACML stands for extensible Access Control Markup Language. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies.

Latest version 2.0 was ratified by OASIS standards organization on 1 February 2005. The planned version 3.0 will add generic attribute categories for the evaluation context and policy delegation profile (administrative policy profile).

Answer option B is incorrect. Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

QUESTION 11

Which of the following statements are true about distributed computing? Each correct answer represents a complete solution. Choose all that apply.

A. In distributed computing, the computers interact with each other in order to achieve a common goal

B. A distributed system consists of multiple autonomous computers that communicate through a computer network.

C. In distributed computing, a problem is divided into many tasks, each of which is solved by a programmer.

D. Distributed computing refers to the use of distributed systems to solve computational problems.

Correct Answer: ABD

Distributed computing is a field of computer science that studies distributed systems. In distributed computing, a problem is divided into many tasks, each of which is solved by one computer. A distributed system consists of multiple autonomous computers that communicate through a computer network. It also refers to the use of distributed systems to solve computational problems. The computers interact with each other in order to achieve a common goal.

QUESTION 12

Derrick works as a Security Administrator for a police station. He wants to determine the minimum CIA levels for his organization. Which of the following best represents the minimum CIA levels for a police departments data systems?

A. Confidentiality = high, Integrity = high, Availability = high

B. Confidentiality = moderate. Integrity = moderate, Availability = high

C. Confidentiality = low. Integrity = low. Availability = low

D. Confidentiality = high, Integrity = moderate, Availability = moderate

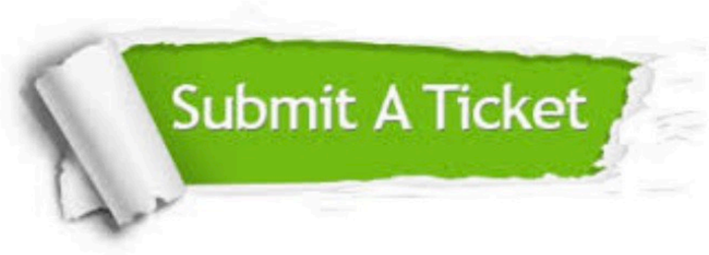
Correct Answer: D

For any law enforcement agency, confidentiality of data is absolutely critical. Breach of confidentiality could have catastrophic consequences. However, integrity and availability issues are standard/moderate.

Answer option A is incorrect. While a law enforcement agency needs high confidentiality, the integrity and availability needs are not high.

Answer option C is incorrect. Certainly all low is not appropriate. And the Confidentiality must be high.

Answer option B is incorrect. This setup is exactly the opposite of what is required.


Submit A Ticket

100%