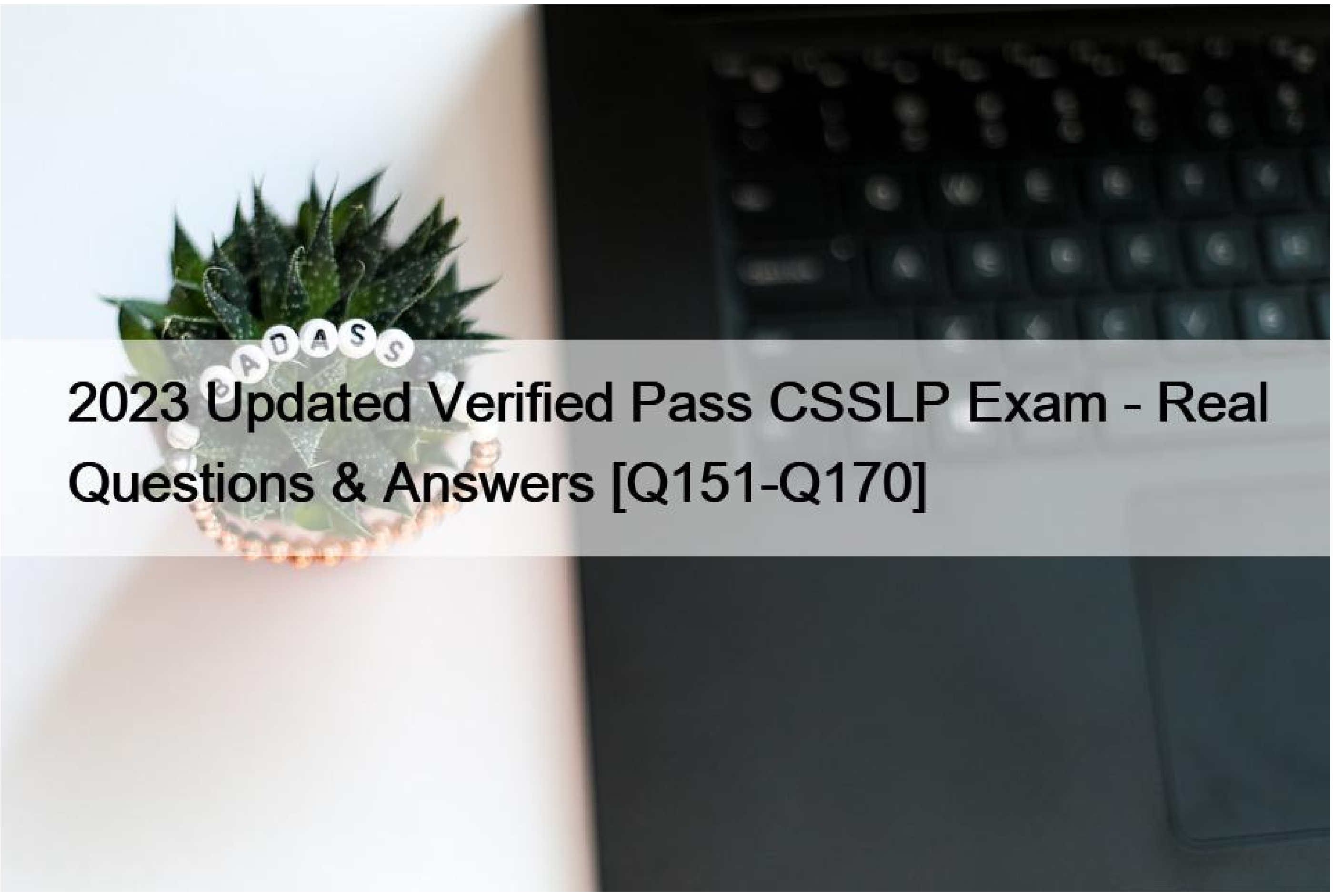
2023 Updated Verified Pass CSSLP Exam - Real Questions & Answers [Q151-Q170


2023 Updated Verified Pass CSSLP Exam - Real Questions & Answers [Q151-Q170]

2023 Updated Verified Pass CSSLP Exam - Real Questions and Answers
Dumps Moneyack Guarantee - CSSLP Dumps Approved Dumps

NEW QUESTION 151

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?
* Discretionary Access Control
* Mandatory Access Control
* Policy Access Control
* Role-Based Access Control
* Explanation:

Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources. This situation can also be handled using the RBAC model.

is incorrect. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as &#8220;secret&#8221;, he cannot grant permission to other users to see this object unless they have the appropriate permission. Answer A is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data. This model is commonly used in PC environment. The basis of this model is the use of Access Control List (ACL). Answer C is incorrect. There is no such access control model as Policy Access Control.

NEW QUESTION 152

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?
* Phase 3, Validation
* Phase 1, Definition
* Phase 2, Verification
* Phase 4, Post Accreditation Phase
Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle. Answer B is incorrect. Phase 1, Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort necessary to achieve accreditation. Answer C is incorrect. Phase 2, Verification, verifies the evolving or modified system&#8217;s compliance with the information agreed on in the System Security Authorization Agreement (SSAA). Answer A is incorrect. Phase 3 validates the compliance of a fully integrated system with the information stated in the SSAA.

NEW QUESTION 153

You work as an analyst for Tech Perfect Inc. You want to prevent information flow that may cause a conflict of interest in your organization representing competing clients. Which of the following security models will you use?
* Bell-LaPadula model
* Chinese Wall model
* Clark-Wilson model
* Biba model
The Chinese Wall Model is the basic security model developed by Brewer and Nash. This model prevents information flow that may cause a conflict of interest in an organization representing competing clients. The Chinese Wall Model provides both privacy and integrity for data. Answer D is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. Answer C is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model&#8217;s enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. Answer A is incorrect. The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,&#8221;Top Secret&#8221;), down to the least sensitive (e.g., &#8220;Unclassified&#8221; or &#8220;Public&#8221;). The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.

NEW QUESTION 154

Which of the following are the principle duties performed by the BIOS during POST (power-on-self-test)?

Each correct answer represents a part of the solution. Choose all that apply.
* It provides a user interface for system&#8217;s configuration.
* It identifies, organizes, and selects boot devices.
* It delegates control to other BIOS, if it is required.
* It discovers size and verifies system memory.
* It verifies the integrity of the BIOS code itself.
* It interrupts the execution of all running programs.
Explanation/Reference:

Explanation: The principle duties performed by the BIOS during POST (power-on-self-test) are as follows:

It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system&#8217;s configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. AnswerF is incorrect. The BIOS does not interrupt the execution of all running programs.

NEW QUESTION 155

Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?
* Emulator
* Hypervisor
* Grid computing
* CP/CMS
A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their execution process. It provides isolation to the host&#8217;s resources. The hypervisor is installed on server hardware. Answer A is incorrect. Emulator duplicates the functions of one system using a different system, so that the second system behaves like the first system. Answer D is incorrect. CP/CMS is a time-sharing operating system of the late 60s and early 70s, and it is known for its excellent performance and advanced features. Answer C is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

NEW QUESTION 156

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?
* Superscan
* NBTscan
* Nmap
* P0f
According to the scenario, you have searched all open ports of the we-are-secure server. Now you want to perform the next information-gathering step, i.e., passive OS fingerprinting. For this, you will use the P0f tool to accomplish the task. P0f is a passive OS fingerprinting tool that is used to identify the operating system of a target host simply by examining captured packets even when the device is behind a packet firewall. It does not generate any additional direct or indirect network traffic. P0f can also be used to gather various information, such as firewall presence, NAT use (for policy enforcement), existence of a load balancer setup, the distance to the remote system and its uptime, etc. Answer C is incorrect. Nmap is used for active OS fingerprinting. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a &#8220;map&#8221; of the network. Just like many simple port scanners, Nmap is capable of discovering

passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc. Answer A is incorrect. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system.The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified &#8220;helper&#8221; applications. It has the transmission speed control utility. Answer B is incorrect. NBTscan is a scanner that scans IP networks for NetBIOS name information. It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. It displays IP address, NetBIOS computer name, logged-in user name and MAC address of each responded host. NBTscan works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

NEW QUESTION 157

Which of the following process areas does the SSE-CMM define in the &#8216;Project and Organizational Practices&#8217; category? Each correct answer represents a complete solution. Choose all that apply.
* Provide Ongoing Skills and Knowledge
* Verify and Validate Security
* Manage Project Risk
* Improve Organization&#8217;s System Engineering Process
Project and Organizational Practices include the following process areas: PA12: Ensure Quality PA13: Manage Configuration PA14: Manage Project Risk PA15: Monitor and Control Technical Effort PA16: Plan Technical Effort PA17: Define Organization&#8217;s System Engineering Process PA18: Improve Organization&#8217;s System Engineering Process PA19: Manage Product Line Evolution PA20: Manage Systems Engineering Support Environment PA21: Provide Ongoing Skills and Knowledge PA22: Coordinate with Suppliers

NEW QUESTION 158

Security is a state of well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security? Each correct answer represents a complete solution. Choose all that apply.
* Integrity
* Authenticity
* Confidentiality
* Availability
The elements of security are as follows: 1.Confidentiality: It is the concealment of information or resources. 2.Authenticity: It is the identification and assurance of the origin of information. 3.Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes. 4.Availability: It refers to the ability to use the information or resources as desired.

NEW QUESTION 159

Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.
* HTML
* PHP
* .NET
* Perl
Explanation/Reference:

Explanation: Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS- Windows, provide an API so that programmers can write applications consistent with the operating environment. Answer: A is incorrect. HTML stands for Hypertext Markup Language. It is a set of markup symbols or codes used to create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

NEW QUESTION 160

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.
* Certification analysis
* Assessment of the Analysis Results
* Configuring refinement of the SSAA
* System development
* Registration

Explanation/Reference:

Explanation: The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows:

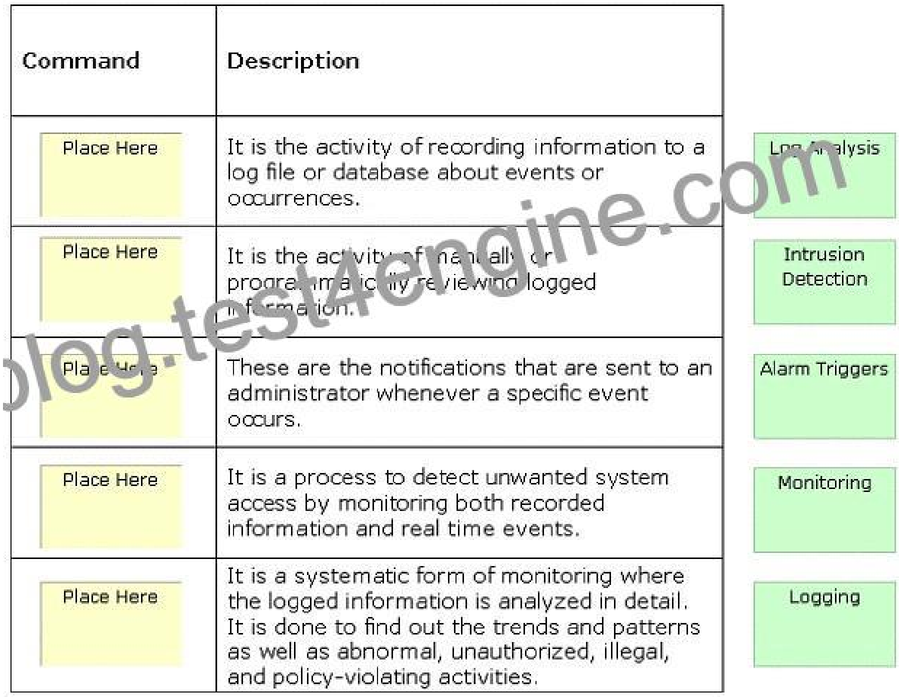
Configuring refinement of the SSAA System development Certification analysis Assessment of the Analysis Results AnswerE is incorrect. Registration is a Phase 1 activity.

NEW QUESTION 161

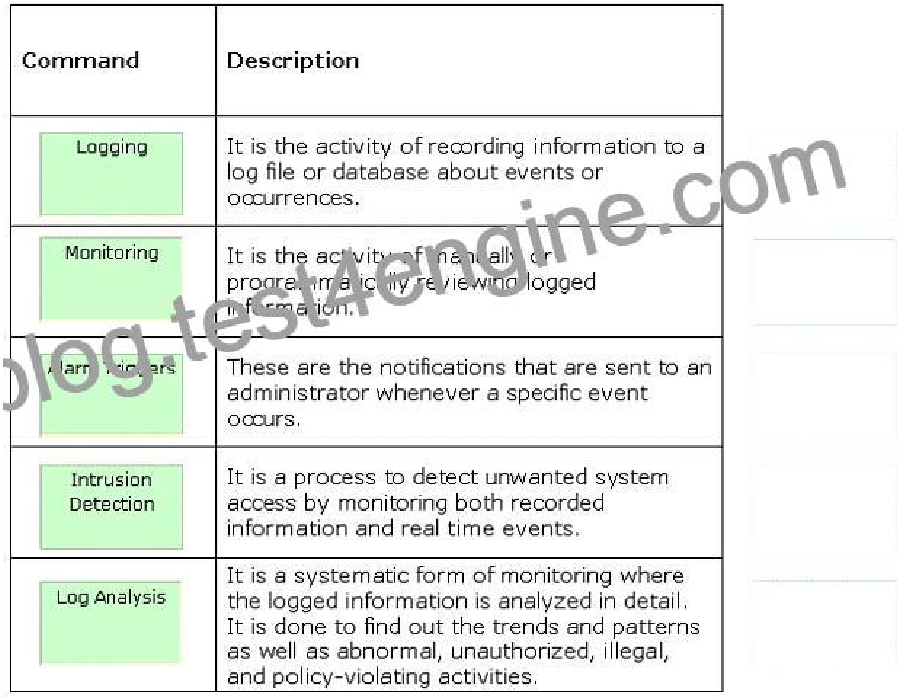
DRAG DROP

Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, and many more vulnerabilities to enhance the security of the network. It encompasses a wide variety of activities. Place the different auditing activities in front of their descriptions.

Select and Place:



Command	Description	
Place Here	It is the activity of recording information to a log file or database about events or occurrences.	Log Analysis
Place Here	It is the activity of manually or programmatically reviewing logged information.	Intrusion Detection
Place Here	These are the notifications that are sent to an administrator whenever a specific event occurs.	Alarm Triggers
Place Here	It is a process to detect unwanted system access by monitoring both recorded information and real time events.	Monitoring
Place Here	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.	Logging



Command	Description
Logging	It is the activity of recording information to a log file or database about events or occurrences.
Monitoring	It is the activity of manually or programmatically reviewing logged information.
Alarm Triggers	These are the notifications that are sent to an administrator whenever a specific event occurs.
Intrusion Detection	It is a process to detect unwanted system access by monitoring both recorded information and real time events.
Log Analysis	It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

Explanation/Reference:

Explanation: Auditing encompasses a wide variety of activities as follows: Logging: It is the activity of recording information to a log file or database about events or occurrences. Log Analysis: It is a systematic form of monitoring where the logged information is analyzed in detail. It is done to find out the trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Intrusion Detection: It is a process to detect unwanted system access by monitoring both recorded information and real time events.

Alarm Triggers: These are the notifications that are sent to an administrator whenever a specific event occurs. Monitoring: It is the activity of manually or programmatically reviewing logged information.

NEW QUESTION 162

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the pre-attack phase to check the security of the We-are-secure network: Gathering information Determining the network range Identifying active systems Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?
* ARIN
* APNIC
* RIPE
* SuperScan
* Explanation:

In such a situation, John will use the SuperScan tool to find the open ports and applications on the We-are-secure network. SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a given range of IP addresses and resolve the host name of the remote system. The features of SuperScan are as follows: It scans any port range from a built-in list or any given range. It performs ping scans and port scans using any IP range. It modifies the port list and port descriptions using the built in editor. It connects to any discovered open port using user-specified &#8220;helper&#8221; applications. It has the transmission speed control utility.
A, and B are incorrect. RIPE, ARIN, and APNIC are the Regional Internet Registries (RIR) that manage, distribute, and register public IP addresses within their respective regions. These can be used as passive tools by an attacker to determine the network range.

NEW QUESTION 163

The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.
* Testing
* Implementation
* Operation/maintenance
* Development/acquisition
* Disposal
* Initiation

The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/maintenance 5.Disposal

NEW QUESTION 164

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.
* Kernel flaws
* Information system architectures
* Race conditions
* File and directory permissions

* Buffer overflows
* Trojan horses
* Social engineering
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

NEW QUESTION 165

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?
* Level 2
* Level 3
* Level 5
* Level 1
* Level 4
Explanation/Reference:

Explanation: The following are the five levels of FITSAF based on SEI&#8217;s Capability Maturity Model (CMM):

Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

NEW QUESTION 166

SIMULATION

Fill in the blank with an appropriate phrase The is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity.
Biba model

Explanation/Reference:

Explanation: The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

NEW QUESTION 167

Which of the following are the benefits of information classification for an organization? Each correct answer represents a complete solution. Choose two.
* It helps reduce the Total Cost of Ownership (TCO).

* It helps identify which protections apply to which information.
* It helps identify which information is the most sensitive or vital to an organization.
* It ensures that modifications are not made to data by unauthorized personnel or processes.

Following are the benefits of information classification for an organization: It helps identify which protections apply to which information. It helps identify which information is the most sensitive or vital to an organization. It supports the tenets of confidentiality, integrity, and availability as it pertains to data. Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes. Answer A is incorrect. Information classification cannot reduce the Total Cost of Ownership (TCO).

NEW QUESTION 168

Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?
* Non-repudiation
* Integrity
* Authentication
* Confidentiality

Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer A is incorrect. Non-repudiation is a mechanism to prove that the sender really sent this message. Answer C is incorrect. Authentication is the process of verifying the identity of a person or network host.

NEW QUESTION 169

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies? Each correct answer represents a complete solution. Choose all that apply.
* Advisory
* Systematic
* Informative
* Regulatory

Following are the different types of policies: Regulatory: This type of policy ensures that the organization is following standards set by specific industry regulations. This policy type is very detailed and specific to a type of industry. This is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Advisory: This type of policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical information, handle financial transactions, or process confidential information. Informative: This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company&#8217;s goals and mission, and a general reporting structure in different situations. Answer B is incorrect. No such type of policy exists.

NEW QUESTION 170

Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program? Each correct answer represents a complete solution. Choose all that apply.
* Security education
* Security organization
* System classification
* Information classification

Explanation/Reference:

Explanation: The first action of a management program to implement information security is to have a security program in place. The objectives of a security program are as follows: Protect the company and its assets Manage risks by identifying assets, discovering threats, and estimating the risk Provide direction for security activities by framing of information security policies, procedures, standards, guidelines and baselines Information classification Security organization Security education AnswerC is incorrect.

System classification is not one of the objectives of a security program.

Certification Path

The Certified Secure Software Lifecycle Professional (CSSLP) certification path includes only one CSSLP certification exam.

How to book CSSLP Exam

Register for Certified Secure Software Lifecycle Professional (CSSLP) Certification Exam on Pearson VUE

Updated PDF (New 2023) Actual ISC CSSLP Exam Questions:
https://www.test4engine.com/CSSLP_exam-latest-braindumps.html]