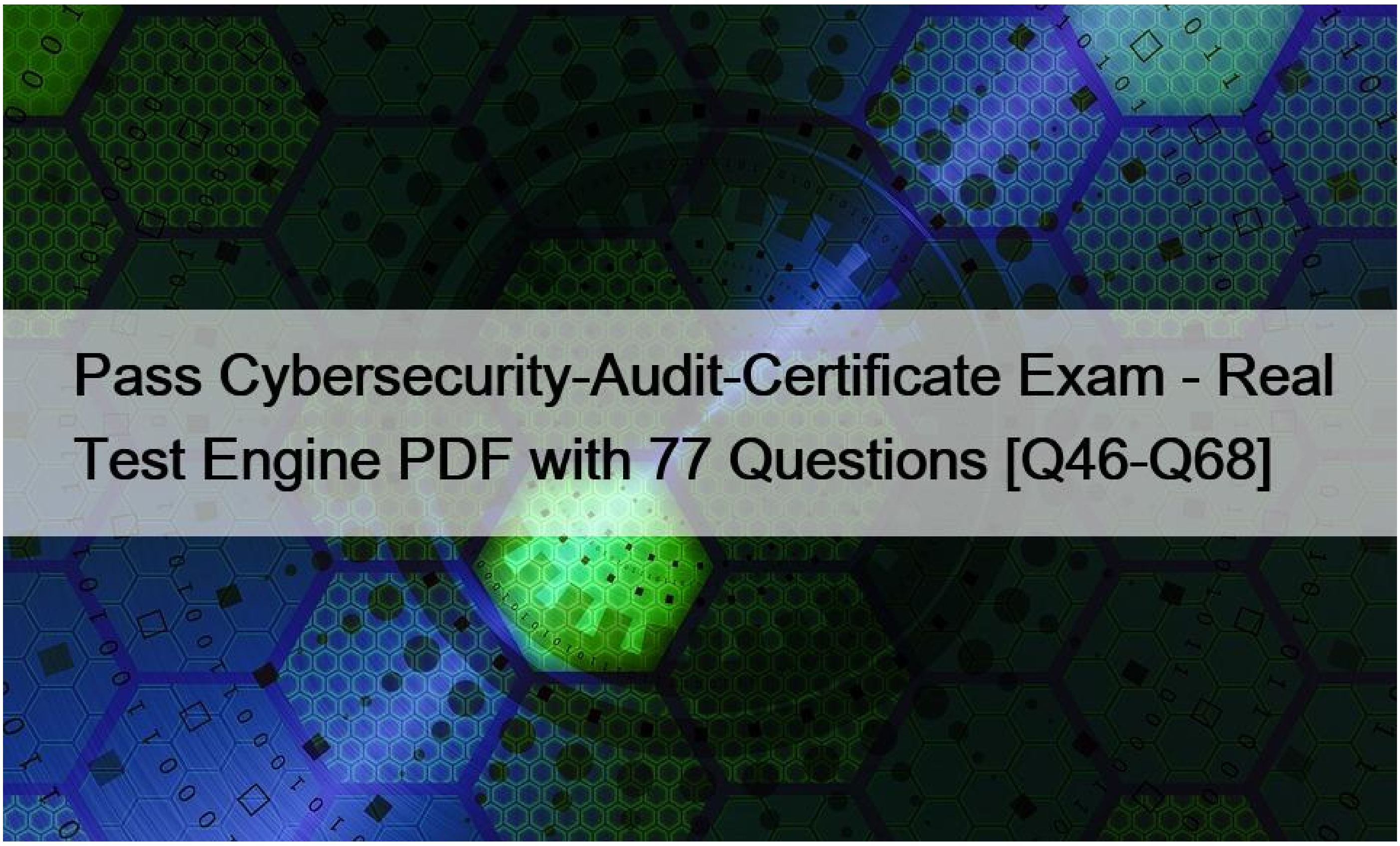
Pass Cybersecurity-Audit-Certificate Exam - Real Test Engine PDF with 77 Questions [Q46-Q68



Pass Cybersecurity-Audit-Certificate Exam - Real Test Engine PDF with 77 Questions
Get New Cybersecurity-Audit-Certificate Certification Practice Test Questions Exam Dumps

NEW QUESTION 46

Which of the following are politically motivated hackers who target specific individuals or organizations to achieve various ideological ends?
* Malware researchers
* Hacktivists
* Cybercriminals
* Script kiddies
Explanation

Hacktivists are politically motivated hackers who target specific individuals or organizations to achieve various ideological ends. They may use various methods such as defacing websites, launching denial-of-service attacks, leaking confidential information, or spreading propaganda to advance their causes or protest against perceived injustices.

NEW QUESTION 47

Which of the following is the BEST method of maintaining the confidentiality of digital information?

* Use of access controls, file permissions, and encryption
* Use of backups and business continuity planning
* Use of logging digital signatures, and write protection
* Use of the awareness tracing programs and related end-user testing

Explanation

The BEST method of maintaining the confidentiality of digital information is using access controls, file permissions, and encryption. This is because these techniques help to prevent unauthorized access, disclosure, or modification of digital information, by restricting who can access the information, what they can do with it, and how they can access it. The other options are not as effective as using access controls, file permissions, and encryption, because they either relate to protecting availability (B), integrity C, or awareness (D).

NEW QUESTION 48

Which of the following is a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon?

* VPN
* IPsec
* SSH
* SFTP

Explanation

The correct answer is C. SSH.

SSH stands for Secure Shell, a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. SSH allows users to remotely access and execute commands on a server without exposing their credentials or data to eavesdropping, tampering or replay attacks. SSH also supports secure file transfer protocols such as SFTP and SCP1.

VPN stands for Virtual Private Network, a technology that creates a secure, encrypted tunnel between two or more devices over a public network such as the Internet. VPN allows users to access resources on a remote network as if they were physically connected to it, while protecting their privacy and identity2.

IPsec stands for Internet Protocol Security, a set of protocols that provides security at the network layer of the Internet. IPsec supports two modes: transport mode and tunnel mode. Transport mode encrypts only the payload of each packet, while tunnel mode encrypts the entire packet, including the header. IPsec can be used to secure VPN connections, as well as other applications that require data confidentiality, integrity and authentication3.

SFTP stands for Secure File Transfer Protocol, a protocol that uses SSH to securely transfer files between a client and a server over a network. SFTP provides encryption, authentication and compression features to ensure the security and reliability of file transfers.

1: SSH (Secure Shell) 2: What is a VPN? How It Works, Types of VPN | Kaspersky 3: IPsec &#8211; Wikipedia :

[SFTP &#8211; Wikipedia]

NEW QUESTION 49

A cloud service provider is used to perform analytics on an organization&#8217;s sensitive data. A data leakage incident occurs in the service providers network from a regulatory perspective, who is responsible for the data breach?

* The service provider

* Dependent upon the nature of breath
* Dependent upon specific regulatory requirements
* The organization

Explanation

A cloud service provider is used to perform analytics on an organization&#8217;s sensitive data. A data leakage incident occurs in the service provider&#8217;s network. From a regulatory perspective, the organization is responsible for the data breach. This is because the organization is the data owner and has the ultimate accountability and liability for the security and privacy of its data, regardless of where it is stored or processed.

The organization cannot transfer or delegate its responsibility to the service provider, even if there is a contractual agreement or service level agreement that specifies the security obligations of the service provider.

The other options are not correct, because they either imply that the service provider is responsible (A), or that the responsibility depends on the nature of breach (B) or specific regulatory requirements C, which are not relevant factors.

NEW QUESTION 50

Cyber threat intelligence aims to research and analyze trends and technical developments in which of the following areas?

* Industry-specific security regulator
* Cybercrime, hacktism. and espionage
* Cybersecurity risk scenarios
* Cybersecurity operations management

Explanation

Cyber threat intelligence aims to research and analyze trends and technical developments in the areas of cybercrime, hacktivism, and espionage. These are the main sources of malicious cyber activities that pose risks to organizations and individuals. Cyber threat intelligence helps to understand the motivations, capabilities, tactics, techniques, and procedures of various threat actors and groups.

NEW QUESTION 51

The protection of information from unauthorized access or disclosure is known as:

* access control.
* cryptograph
* media protect on.
* confidentiality.

Explanation

The protection of information from unauthorized access or disclosure is known as confidentiality. This is because confidentiality is one of the three main objectives of information security, along with integrity and availability. Confidentiality ensures that information is accessible and readable only by those who are authorized and intended to do so, and prevents unauthorized or accidental exposure of information to unauthorized parties. The other options are not the protection of information from unauthorized access or disclosure, but rather different concepts or techniques that are related to information security, such as access control (A), cryptography (B), or media protection C.

NEW QUESTION 52

The GREATEST advantage of using a common vulnerability scoring system is that it helps with:

* risk aggregation.
* risk prioritization.

* risk elimination.
* risk quantification

Explanation

The GREATEST advantage of using a common vulnerability scoring system is that it helps with risk prioritization. This is because a common vulnerability scoring system provides a standardized and consistent way of measuring and comparing the severity of vulnerabilities, based on their impact and exploitability. This allows organizations to prioritize the remediation of the most critical vulnerabilities and allocate resources accordingly. The other options are not as advantageous as using a common vulnerability scoring system, because they either involve aggregating (A), eliminating C, or quantifying (D) risk, which are not directly related to the scoring system.

NEW QUESTION 53

While risk is measured by potential activity, which of the following describes the actual occurrence of a threat?

* Attack
* Payload
* Vulnerability
* Target

Explanation

An attack is the actual occurrence of a threat, which is a potential activity that could harm an asset. An attack is the result of a threat actor exploiting a vulnerability in a system or network to achieve a malicious objective.

For example, a denial-of-service attack is the occurrence of a threat that aims to disrupt the availability of a service.

NEW QUESTION 54

Which of the following is the MOST important consideration when choosing between different types of cloud services?

* Emerging risk and infrastructure scalability
* Security features available on demand
* Overall risk and benefits
* Reputation of the cloud providers

Explanation

The MOST important consideration when choosing between different types of cloud services is the overall risk and benefits. This is because choosing between different types of cloud services involves weighing the trade-offs between the risk and benefits of each type of cloud service, such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS). For example, SaaS may offer more benefits in terms of cost savings, scalability, and usability, but also more risks in terms of security, privacy, and compliance. On the other hand, IaaS may offer more benefits in terms of flexibility, customization, and control, but also more risks in terms of complexity, management, and maintenance. The other options are not the most important consideration when choosing between different types of cloud services, but rather different aspects or factors that affect the choice of cloud services, such as emerging risk and infrastructure scalability (A), security features available on demand (B), or reputation of the cloud providers (D).

NEW QUESTION 55

In cloud computing, which type of hosting is MOST appropriate for a large organization that wants greater control over the environment?

* Private hosting
* Public hosting

* Shared hosting
* Hybrid hosting
Explanation

In cloud computing, the type of hosting that is MOST appropriate for a large organization that wants greater control over the environment is private hosting. Private hosting is a type of cloud service model where the cloud infrastructure is dedicated to a single organization and hosted either on-premise or off-premise by a third-party provider. Private hosting offers more control over the security, performance, customization, and compliance of the cloud environment than other types of hosting.

NEW QUESTION 56

Which of the following is MOST critical to guiding and managing security activities throughout an organization to ensure objectives are met?
* Allocating a significant amount of budget to security investments
* Adopting industry security standards and frameworks
* Establishing metrics to measure and monitor security performance
* Conducting annual security awareness training for all employees
Explanation

The MOST critical thing to guiding and managing security activities throughout an organization to ensure objectives are met is establishing metrics to measure and monitor security performance. This is because metrics provide quantifiable and objective data that can be used to evaluate the effectiveness and efficiency of security activities, as well as identify gaps and areas for improvement. Metrics also enable communication and reporting of security performance to stakeholders, such as senior management, board members, auditors, regulators, customers, etc. The other options are not as critical as establishing metrics, because they either involve spending money without knowing the return on investment (A), adopting standards without customizing them to fit the organization&#8217;s context and needs (B), or conducting training without assessing its impact on behavior change (D).

NEW QUESTION 57

Which intrusion detection system component is responsible for collecting data in the form of network packets, log files, or system call traces?
* Packet filters
* Analyzers
* Administration modules
* Sensors
Explanation

The intrusion detection system component that is responsible for collecting data in the form of network packets, log files, or system call traces is sensors. This is because sensors are components of an intrusion detection system that are deployed on various locations or points of the network or system, such as routers, switches, servers, etc., and that capture and collect data from the network traffic or system activities. Sensors then forward the collected data to another component of the intrusion detection system, such as analyzers, for further processing and analysis. The other options are not components of an intrusion detection system that are responsible for collecting data in the form of network packets, log files, or system call traces, but rather different components or techniques that are related to intrusion detection or prevention, such as packet filters (A), analyzers (B), or administration modules C.

NEW QUESTION 58

Which of the following is the GREATEST advantage of using a virtual private network (VPN) over dedicated circuits and dial-in

servers?
* It is more secure
* It is more reliable
* It is higher speed.
* It is more cost effective.
Explanation

The GREATEST advantage of using a virtual private network (VPN) over dedicated circuits and dial-in servers is that it is more cost effective. This is because a VPN is a technology that creates a secure and encrypted connection between a client and a server over an existing public network, such as the Internet. A VPN reduces the cost of establishing and maintaining a secure communication channel, as it does not require any additional hardware, software, or infrastructure, unlike dedicated circuits and dial-in servers, which require dedicated lines, modems, routers, switches, etc. The other options are not the greatest advantage of using a VPN over dedicated circuits and dial-in servers, because they either involve security (A), reliability (B), or speed C aspects that may not be significantly different or better than dedicated circuits and dial-in servers.

NEW QUESTION 59

A healthcare organization recently acquired another firm that outsources its patient information processing to a third-party Software as a Service (SaaS) provider. From a regulatory perspective, which of the following is MOST important for the healthcare organization to determine?
* Cybersecurity risk assessment methodology
* Encryption algorithms used to encrypt the data
* Incident escalation procedures
* Physical location of the data
Explanation

From a regulatory perspective, the MOST important thing for the healthcare organization to determine when outsourcing its patient information processing to a third-party Software as a Service (SaaS) provider is the incident escalation procedures. This is because incident escalation procedures define how security incidents involving patient information are reported, communicated, escalated, and resolved between the healthcare organization and the SaaS provider. This is essential for complying with regulatory requirements such as HIPAA, which mandate timely notification and response to breaches of protected health information. The other options are not as important as incident escalation procedures from a regulatory perspective, because they either relate to technical aspects that may not affect compliance (A, B), or operational aspects that may not affect patient information security (D).

NEW QUESTION 60

Which of the following is an objective of public key infrastructure (PKI)?
* Creating the private-public key pair for secure communications
* Independently authenticating the validity of the sender&#8217;s public key
* Securely distributing secret keys to the communicating parties
* Approving the algorithm to be used during data transmission
Explanation

An objective of public key infrastructure (PKI) is to independently authenticate the validity of the sender&#8217;s public key. PKI is a system that uses cryptographic keys to secure communications and transactions. PKI involves a trusted third party called a certificate authority (CA) that issues digital certificates that link a public key with an identity. The recipient can use the CA&#8217;s public key to verify the sender&#8217;s certificate and public key.

NEW QUESTION 61

In public key cryptography, digital signatures are primarily used to;
* ensure message integrity.
* ensure message accuracy.
* prove sender authenticity.
* maintain confidentiality.
Explanation

In public key cryptography, digital signatures are primarily used to prove sender authenticity. A digital signature is a cryptographic technique that allows the sender of a message to sign it with their private key, which can only be decrypted by their public key. The recipient can verify that the message was sent by the sender and not tampered with by using the sender&#8217;s public key.

NEW QUESTION 62

Which of the following BIST enables continuous identification and mitigation of security threats to an organization?
* demit/ and access management (1AM)
* Security operations center (SOC)
* Security training and awareness
* Security information and event management (SEM)
Explanation

A security operations center (SOC) is a centralized unit that monitors, detects, analyzes, and responds to cyber threats and incidents in real time. A SOC enables continuous identification and mitigation of security threats to an organization by using various tools, processes, and expertise.

NEW QUESTION 63

Which of the following is a feature of an intrusion detection system (IDS)?
* Intrusion prevention
* Automated response
* Interface with firewalls
* Back doors into applications
Explanation

A feature of an intrusion detection system (IDS) is automated response. This is because an IDS is a system that monitors network or system activities for malicious or anomalous behavior, and alerts or reports on any detected incidents. An IDS can also perform automated response actions, such as blocking traffic, terminating sessions, or sending notifications, to contain or mitigate the incidents. The other options are not features of an IDS, but rather different concepts or techniques that are related to intrusion detection or prevention, such as intrusion prevention (A), interface with firewalls C, or back doors into applications (D).

NEW QUESTION 64

Which of the following devices is at GREATEST risk from activity monitoring and data retrieval?
* Mobile devices
* Cloud storage devices
* Desktop workstation
* Printing devices
Explanation

The device that is at GREATEST risk from activity monitoring and data retrieval is mobile devices. This is because mobile devices are devices that are portable, wireless, and connected to the Internet or other networks, such as smartphones, tablets, laptops, etc.

Mobile devices are at greatest risk from activity monitoring and data retrieval, because they can be easily lost, stolen, or compromised by attackers who can access or extract the data stored or transmitted on the devices. Mobile devices can also be subject to activity monitoring and data retrieval by third-party applications or services that may collect or share the user&#8217;s personal or sensitive information without their consent or knowledge. The other options are not devices that are at greatest risk from activity monitoring and data retrieval, but rather different types of devices that may have different levels of risk or protection from activity monitoring and data retrieval, such as cloud storage devices (B), desktop workstations C, or printing devices (D).

NEW QUESTION 65

Which process converts extracted information to a format understood by investigators?
* Reporting
* Ingestion
* imaging
* Filtering
Explanation

The process that converts extracted information to a format understood by investigators is reporting. This is because reporting is a technique that involves presenting and communicating the results and findings of an investigation in a clear, concise, and accurate manner, using appropriate formats, such as tables, charts, graphs, etc. Reporting helps to convey the meaning and significance of the extracted information to the investigators, as well as other stakeholders, such as management, auditors, regulators, etc. The other options are not processes that convert extracted information to a format understood by investigators, but rather different techniques that are related to information extraction or analysis, such as ingestion (B), imaging C, or filtering (D).

NEW QUESTION 66

Within the NIST core cybersecurity framework, which function is associated with using organizational understanding to minimize risk to systems, assets, and data?
* Detect
* Identify
* Recover
* Respond
Explanation

Within the NIST core cybersecurity framework, the identify function is associated with using organizational understanding to minimize risk to systems, assets, and data. This is because the identify function helps organizations to develop an organizational understanding of their cybersecurity risk management posture, as well as the threats, vulnerabilities, and impacts that could affect their business objectives. The other functions are not directly related to using organizational understanding, but rather focus on detecting (A), recovering C, or responding (D) to cybersecurity events.

NEW QUESTION 67

What would be an IS auditor&#8217;s BEST response to an IT managers statement that the risk associated with the use of mobile devices in an organizational setting is the same as for any other device?
* Replication of privileged access and the greater likelihood of physical loss increases risk levels.
* The risk associated with mobile devices is less than that of other devices and systems.
* The risk associated with mobile devices cannot be mitigated with similar controls for workstations.
* The ability to wipe mobile devices and disable connectivity adequately mitigates additional
Explanation

The BEST response to an IT manager&#8217;s statement that the risk associated with the use of mobile devices in an organizational setting is the same as for any other device is that replication of privileged access and the greater likelihood of physical loss increases risk levels. Mobile devices pose unique risks to an organization due to their portability, connectivity, and functionality. Mobile devices may store or access sensitive data or systems that require privileged access, which can be compromised if the device is lost, stolen, or hacked. Mobile devices also have a higher chance of being misplaced or taken by unauthorized parties than other devices.

NEW QUESTION 68

Which of the following is a feature of a stateful inspection firewall?
* It tracks the destination IP address of each packet that leaves the organization&#8217;s internal network.
* It is capable of detecting and blocking sophisticated attacks
* It prevents any attack initiated and originated by an insider.
* It translates the MAC address to the destination IP address of each packet that enters the organization&#8217;s internal network.
Explanation

A feature of a stateful inspection firewall is that it is capable of detecting and blocking sophisticated attacks. A stateful inspection firewall is a type of firewall that monitors and analyzes the state and context of network traffic. It keeps track of the source, destination, protocol, port, and session information of each packet and compares it with a set of predefined rules. A stateful inspection firewall can detect and block attacks that exploit the logic or behavior of network protocols or applications, such as fragmentation attacks, session hijacking, or application-layer attacks.

Cybersecurity-Audit-Certificate Exam Dumps - PDF Questions and Testing Engine:
https://www.validexam.com/Cybersecurity-Audit-Certificate-latest-dumps.html]