ISC.CC.v2026-08-08.q343

Exam Code:	CC
Exam Name:	Certified in Cybersecurity (CC)
Certification Provider:	ISC
Free Question Number:	343
Version:	v2026-08-08
# of views:	103
# of Questions views:	3798
https://www.dumpsfiles.com/files/ISC/CC/ISC.CC.v2026-08-08.q343	

NEW QUESTION: 1
Which of these is WEAKEST form of authentication we can implement?
A. Something you have
B. Something you know
C. Biometric authentications
D. Something you are
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
Port forwarding is also known as
A. Port mapping
B. ALL
C. Tunneling
D. Punch through
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
What is an IP address
A. An address that denotes the vendor or manufacturer of the physical network interface
B. A Logical address associated with a unique network interface within the network
C. A physical address used to connect multiple devices in a network
D. An Address that represents the network interface within the network
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

Tina is an (ISC)² member and is invited to join an online group of IT security enthusiasts. After attending a few online sessions, Tina learns that some participants in the group are sharing malware with each other, in order to use it against other organizations online. What should Tina do?

A. Stop participating in the group

B. Report the group to law enforcement

C. Report the group to (ISC)2

D. Nothing

Answer: (SHOW ANSWER)

NEW QUESTION: 5

Which of these is an example of a physical access control mechanism?

A. Software-based firewall at the perimeter of the network

B. Network switches that filter according to MAC addresses

C. A lock on a door

D. A process that requires two people to act at the same time to perform a function

Answer: C (LEAVE A REPLY)

NEW QUESTION: 6

Which uses encrypted, machine-generated codes to verify a user's identity.

A. Token Based Authentication

B. AII

C. Basic Authentication

D. Form Based Authentication

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

To avoid bodily injury claims, a company decides not to offer high-risk services. This is an example of:

A. Risk Acceptance

B. Risk Assessment

C. Risk Avoidance

D. Risk Control

Answer: (SHOW ANSWER)

Risk Avoidanceeliminates risk by discontinuing activities that expose the organization to unacceptable threats.

NEW QUESTION: 8

The Bell-LaPadula access control model is a form of:

A. RBAC

B. MAC

C. DAC

D. ABAC

Answer: B (LEAVE A REPLY)

Bell-LaPadula is a Mandatory Access Control (MAC) model focused on confidentiality. It uses security labels and clearances to enforce access rules such as "no read up, no write down."

NEW QUESTION: 9
Which maintains that a user or entity should only have access to the spec data, resources and applications needed to complete a required task.
A. AII
B. Zero Trust
C. Least Privileges
D. Defence in Depth
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
What is privacy in the context of Information Security?
A. Protecting data from unauthorized access
B. Ensuring data is accurate and unchanged
C. Making sure data is always accessible when needed
D. Disclosed without their consent
Answer: A (LEAVE A REPLY)
In information security, privacy refers to protecting personal and sensitive information from unauthorized access, use, or disclosure. Privacy focuses specifically on data related to individuals, such as PII, and ensuring it is handled according to legal, ethical, and regulatory requirements.
While privacy is closely related to confidentiality, it places greater emphasis on individual rights and consent. Ensuring privacy means limiting access to personal data and preventing misuse.
Integrity and availability address different aspects of the CIA triad, while option D is incomplete and incorrect.
Security frameworks treat privacy as a critical objective, especially in environments handling personal data.

NEW QUESTION: 11
Which OSI layer associates MAC addresses with network devices?
A. Physical layer
B. Network layer
C. Data Link layer
D. Transport layer
Answer: C (LEAVE A REPLY)
The Data Link layer (Layer 2) handles MAC addressing and frame delivery within local networks.

NEW QUESTION: 12
A _____ is a record of something that has occurred.
A. Firewall
B. Log
C. Law

D. Biometric
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
Within the organization, who can identify risk?
A. Anyone
B. Any security team member
C. Senior management
D. The security manager
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What is the importance of non-repudiation in today's world of e-commerce?
A. Ensures people are not held responsible for transactions they did not conduct
B. Ensures people are held responsible for transactions they conducted
C. Ensures transactions are not conducted online
D. Ensures transactions are conducted online
Answer: B (LEAVE A REPLY)
In e-commerce,non-repudiationensures accountability by preventing buyers or sellers from denying transactions they actually performed. This is essential for trust, legal enforcement, and dispute resolution in digital commerce.
By using digital signatures, certificates, and secure transaction logs, organizations can prove that a specific user authorized a transaction. This protects merchants from fraudulent chargebacks and customers from transaction tampering.
Without non-repudiation, online commerce would lack trust and legal enforceability, undermining digital economies.

NEW QUESTION: 15
What is the main purpose of using digital signatures in communication security?
A. To verify the identity of the sender and ensure the integrity of the message (Correct)
B. To compress data to reduce bandwidth usage
C. To encrypt sensitive data during transmission
D. To prevent unauthorized access to a network
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
Access control used in in high-security situations such as military and government organizations.
A. DAC
B. ABAC
C. MAC
D. RBAC

Answer: C (LEAVE A REPLY)

NEW QUESTION: 17
Which plan is activated when both the Incident response and BCP fails
A. Risk Management
B. DRP
C. None
D. BIA
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which one of the following groups is NOT normally part of an organization's cybersecurity incident response team?
A. Technical subject matter experts
B. Cybersecurity experts
C. Management
D. Law enforcement
Answer: (SHOW ANSWER)
Law enforcement is not typically part of an organization's internal incident response team. Incident response teams usually consist of cybersecurity professionals, technical subject matter experts, IT staff, legal advisors, and management representatives.
Law enforcement may become involved after an incident, especially in cases involving criminal activity, regulatory requirements, or large-scale breaches. However, they are external stakeholders, not internal team members.
Management plays a key role in decision-making and communication, while technical and cybersecurity experts handle detection, containment, eradication, and recovery.
NIST incident response guidance emphasizes coordination with external entities but clearly distinguishes internal response teams from external authorities such as law enforcement.

NEW QUESTION: 19
Which is NOT a function of an Intrusion Prevention System (IPS)?
A. Encrypt network traffic
B. Monitor network traffic

C. Filter network traffic
D. Detect and prevent attacks
Answer: (SHOW ANSWER)
An IPS monitors traffic, detects malicious activity, and actively blocks attacks. Encryption is handled by protocols such as TLS or IPSec, not IPS devices.

NEW QUESTION: 20
Data _____ is data left behind on systems/media after normal deletion procedures have been attempted.
A. Packets
B. Remanence
C. Residue
D. Fragments
Answer: B (LEAVE A REPLY)

NEW QUESTION: 21
Which protocol would be most suitable to fulfill the secure communication requirements between clients and the server for a company deploying a new application?
A. FTP
B. HTTP
C. HTTPS
D. SMTP
Answer: (SHOW ANSWER)
HTTPS (Hypertext Transfer Protocol Secure) is the most suitable protocol for secure communication between clients and servers. HTTPS uses TLS to encrypt data in transit, ensuring confidentiality, integrity, and authentication. This prevents attackers from eavesdropping, tampering, or impersonating servers.
HTTP and FTP transmit data in clear text, making them vulnerable to interception. SMTP is used for email delivery, not client-server web communication. Modern security standards mandate HTTPS for all production web applications.

NEW QUESTION: 22
(ISC)² publishes a Common Body of Knowledge (CBK) that IT security practitioners should be familiar with; this is recognized throughout the industry as a set of material that is useful for practitioners to refer to. Certifications can be issued for demonstrating expertise in this Common Body of Knowledge. What kind of document is the Common Body of Knowledge?
A. Procedure
B. Policy
C. Standard
D. Law
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23

Aphrodite is a member of (ISC)² and a data analyst for Triffid Corporation. While Aphrodite is reviewing user log data, Aphrodite discovers that another Triffid employee is violating the acceptable use policy and watching streaming videos during work hours. What should Aphrodite do?

A. Inform Triffid management

B. Inform (ISC)2

C. Nothing

D. Inform law enforcement

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Which layer of OSI the Firewall works

A. Layer 7

B. Layer 3

C. All

D. Layer 4

Answer: C (LEAVE A REPLY)

NEW QUESTION: 25

Raj wants aphysical deterrent controlto discourage unauthorized entry. Which option best serves this purpose?

A. A wall

B. Razor tape

C. A sign

D. A hidden camera

Answer: A (LEAVE A REPLY)

A wall is a physical deterrent that prevents and discourages unauthorized access. Signs are administrative deterrents, cameras are detective controls, and razor tape is a physical barrier but typically supplements perimeter defenses rather than serving as the primary deterrent.

NEW QUESTION: 26

What is the purpose of the CIA triad terms

A. All

B. To define the purpose of security

C. To make security more understable to management and users

D. To describe security using relevant and meaningful words

Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

If a device is found that is not compliant with the security baseline, what will be the security team action

A. Report

B. Evaluate

C. Disabled or isolated into a quarantine area until it can be checked and updated.

D. Ignore
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Hoshi is an (ISC)² member who works for the Triffid Corporation as a data manager. Triffid needs a new firewall solution, and Hoshi is asked to recommend a product for Triffid to acquire and implement. Hoshi's cousin works for a firewall vendor; that vendor happens to make the best firewall available. What should Hoshi do?
A. Recommend the cousin's product
B. Disclose the relationship, but recommend the vendor/product
C. Hoshi should ask to be recused from the task
D. Recommend a different vendor/product
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Selvaa presents a user ID and password to log on. Which characteristic must the user ID have?
A. Authorization
B. Authentication
C. Availability
D. Identification
Answer: D (LEAVE A REPLY)
A user ID provides identification-it claims an identity. Authentication verifies that claim using credentials like a password.

NEW QUESTION: 30
Government can imposes financial penalties as a consequence of breaking a
A. Policy
B. Procedures
C. Standard
D. Regulation
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Exhibit.

What is the purpose of a Security Information and Event Management (SIEM) system?

A. Encrypting files

B. Monitoring and analyzing security events -

C. Blocking malicious websites

D. Managing user passwords

Answer: B (LEAVE A REPLY)

A Security Information and Event Management (SIEM) system is designed tocollect, correlate, analyze, and alert on security eventsgenerated across an organization's IT environment. SIEM platforms aggregate logs from diverse sources such as servers, firewalls, endpoints, applications, and cloud services, providing centralized visibility into security activity.

The core value of a SIEM lies inevent correlation and contextual analysis. By correlating events across systems and over time, a SIEM can detect suspicious patterns that individual logs alone would not reveal- such as lateral movement, privilege escalation, or coordinated attacks. SIEMs also support real-time alerting, dashboards, querying, and incident investigation, enabling security teams to respond faster and more effectively.

SIEM systems donotencrypt files (that's cryptography), block websites directly (that's firewalls or secure web gateways), or manage passwords (that's IAM). Instead, they serve as thecentral nervous system of a Security Operations Center (SOC), supporting monitoring, detection, compliance reporting, and incident response workflows as recommended by NIST and other security frameworks.

NEW QUESTION: 32
How often should an organization test its BCP?
A. Continually
B. Annually
C. Routinely
D. Daily
Answer: C (LEAVE A REPLY)
BCPs should be testedroutinely(e.g., tabletop, simulations) to ensure readiness and relevance.

NEW QUESTION: 33
When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called_____
A. Attack
B. Malware
C. Event
D. Zero-day
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
A security event does not affect confidentiality, integrity, or availability. What is it?
A. Exploit
B. Breach
C. Incident
D. Event
Answer: (SHOW ANSWER)
If CIA is not impacted, the occurrence remains asecurity event, not an incident or breach.

NEW QUESTION: 35
An ISC2 member is offered an illicit copy of a movie. What should they do?
A. Inform ISC2
B. Inform law enforcement
C. Accept the movie
D. Refuse to accept
Answer: D (LEAVE A REPLY)
The ISC2 Code of Ethics requires members to act lawfully and ethically. Accepting pirated material violates this obligation.

NEW QUESTION: 36
A logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.
A. LAN
B. VPN
C. WLAN
D. VLAN
Answer: D (LEAVE A REPLY)
A Virtual Local Area Network (VLAN) is a logical segmentation of network devices that allows systems to appear as though they are on the same local network, regardless of their physical location. VLANs operate at the Data Link layer (Layer 2) and use tagging (such as IEEE 802.1Q) to separate broadcast domains logically. VLANs improve security, performance, and manageability by isolating traffic between different groups of systems. Devices in the same VLAN can communicate as if they were on the same LAN, even if they are physically distributed across different switches or buildings.
LAN refers to a physical local network, VPN provides encrypted tunnels across networks, and WLAN refers to wireless LANs. Only VLANs provide logical grouping independent of geography.

NEW QUESTION: 37
A one-way spinning door or barrier that allows only one person at a time to enter a building or area.
A. Turnstile
B. Mantrap
C. Bollard
D. Gate
Answer: (SHOW ANSWER)
Aturnstileis a physical access control device designed to allow only one individual to pass at a time. Turnstiles are commonly used to prevent tailgating and unauthorized entry in offices, transit stations, and secure facilities. Unlike mantraps, turnstiles typically allow one-way movement and do not lock a person inside an enclosed space.

NEW QUESTION: 38
The last phase in the data security cycle is
A. Backup
B. Archival
C. Encryption
D. Destruction
Answer: D (LEAVE A REPLY)

NEW QUESTION: 39
Which works by encapsulating one packet inside another?
A. Network segmentation
B. Load balancing

C. Tunneling
D. Data encryption
Answer: (SHOW ANSWER)
Tunneling encapsulates packets to securely transmit them across networks, commonly used in VPNs.

NEW QUESTION: 40
Which of the following is unlikely to be a member of the disaster recovery team?
A. Executive management
B. Public relations
C. Billing clerk
D. IT personnel
Answer: C (LEAVE A REPLY)
A disaster recovery team typically includes executive leadership, IT personnel, legal representatives, and public relations staff. These roles are critical for decision-making, technical recovery, and external communication.
A billing clerk is unlikely to be part of the disaster recovery team because the role does not typically contribute to recovery strategy, system restoration, or crisis communication.

NEW QUESTION: 41
The prevention of authorized access to resources or the delaying of time-critical operations is known as:
A. ARP poisoning
B. SYN flood
C. Denial-of-Service (DoS)
D. All
Answer: C (LEAVE A REPLY)
ADenial-of-Service (DoS)attack disrupts availability by overwhelming systems or resources, preventing legitimate access.

NEW QUESTION: 42
A hacker gains unauthorized access and steals confidential data. What term best describes this?
A. Event
B. Breach
C. Intrusion
D. Exploit
Answer: B (LEAVE A REPLY)
A breach occurs when unauthorized access results in the disclosure, theft, or loss of sensitive data. An intrusion may not always result in data loss, but a breach does.

NEW QUESTION: 43
What is an IPSec replay attack?
A. An attack where an attacker modifies packets in transit
B. An attack where an attacker eavesdrops on network traffic

C. An attack where an attacker overloads a network with traffic
D. An attack where an attacker attempts to inject packets in an existing session
Answer: D (LEAVE A REPLY)
An IPSec replay attack occurs when an attacker captures legitimate encrypted packets and attempts to retransmit (replay) them to gain unauthorized access or disrupt communication. The attacker does not need to decrypt the packets; instead, they rely on resending previously valid packets within an existing session.
Without proper protections, replayed packets could be accepted as valid, allowing attackers to impersonate legitimate users or repeat sensitive actions. IPSec defends against replay attacks usingsequence numbers and sliding windows, which ensure packets are processed only once and in the correct order.
Packet modification, eavesdropping, and traffic flooding are different attack types and are not specifically replay attacks. Replay attacks are particularly dangerous in authentication and session-based protocols, which is why anti-replay protection is a mandatory IPSec feature defined by the IETF.

NEW QUESTION: 44
Is defined as the process of identifying, estimating, and prioritizing risks.
A. Risk Assessment
B. Risk Treatment
C. Risk Mitigation
D. Risk Management
Answer: A (LEAVE A REPLY)
Risk assessment is the structured process of identifying risks, estimating their likelihood and impact, and prioritizing them for treatment. It forms the analytical foundation of risk management and enables informed decision-making. Risk assessment typically includes threat identification, vulnerability analysis, likelihood determination, and impact analysis.
Risk treatment and mitigation occur after risks have been assessed, while risk management is the broader lifecycle that includes assessment, response, monitoring, and communication. Standards such as NIST SP 800-30 emphasize risk assessment as a critical early step in managing cybersecurity risk.

NEW QUESTION: 45
Which of the following best describes a zero-day vulnerability?
A. A vulnerability that has not yet been discovered or publicly disclosed.
B. A vulnerability that affects only legacy systems.
C. A vulnerability that can only be exploited by experienced hackers.
D. A vulnerability that has been identified and patched by software vendors
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
What is the potential impact of an IPSec reply attack
A. Modification of network traffic
B. ALL
C. Disruption of network communication

D. Unauthorized access to network resources
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which of the following is NOT one of the three main components of a sql database?
A. Tables
B. Object-oriented interfaces
C. Schemas
D. Views
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
What is the main challenge in achieving non-repudiation in electronic transactions?
A. Verifying sender and recipient identity
B. Ensuring message authenticity and integrity
C. Preventing message tampering
D. All of the above
Answer: (SHOW ANSWER)
Non-repudiation requires strong identity verification, message integrity, and tamper resistance, typically implemented using digital signatures and PKI.

NEW QUESTION: 49
In which access control model can the creator of an object delegate permissions?
A. MAC
B. RBAC
C. ABAC
D. DAC
Answer: (SHOW ANSWER)
Discretionary Access Control (DAC) allows the owner or creator of an object to decide who can access it and what permissions they receive. This delegation capability is a defining feature of DAC systems.
MAC enforces centrally controlled policies, RBAC assigns permissions through roles, and ABAC uses attributes evaluated by a policy engine. Only DAC explicitly allows object owners to grant or revoke access at their discretion.

NEW QUESTION: 50
Why is identifying roles and responsibilities important in IR planning?
A. To prevent incidents
B. To ensure everyone knows their role
C. To reduce impact
D. To select containment strategy
Answer: (SHOW ANSWER)
Clear roles ensure fast, coordinated response, reduce confusion, and prevent duplicated or missed actions during incidents.

NEW QUESTION: 51
Which type of attack takes advantage of vulnerabilities in validation?
A. Pharming attacks
B. DNS poisoning
C. Cross-site scripting (XSS)
D. ARP spoofing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
Which plan is activated when Incident Response and BCP fail?
A. Risk management
B. BIA
C. DRP
D. None
Answer: C (LEAVE A REPLY)
When incidents escalate beyond containment and business continuity measures are insufficient, theDisaster Recovery Plan (DRP)is activated to restore IT systems and infrastructure.

NEW QUESTION: 53
Which of the following cloud service models provides the most suitable environment for customers to build and operate their own software?
A. PaaS
B. SaaS
C. laaS
Answer: (SHOW ANSWER)

NEW QUESTION: 54
Of the following, which would probably not be considered a threat?
A. Natural disaster
B. An external attacker trying to gain unauthorized access to the environment

C. A laptop with sensitive data on it
D. Unintentional damage to the system cause by a user
Answer: (SHOW ANSWER)

NEW QUESTION: 55
What is the primary goal of implementing input validation in application security?
A. To validate and sanitize user inputs to prevent code injection attacks (Correct)
B. To prevent unauthorized access to the application
C. To ensure all inputs are stored in a secure database
D. To encrypt sensitive data transmitted between the client and server
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which is a component of a Business Continuity (BC) plan?
A. All
B. Immediate response procedures
C. Management authority guidance
D. Notification systems and call trees
Answer: A (LEAVE A REPLY)
A complete BCP includes response procedures, communication plans, and management authority to ensure coordinated recovery.

NEW QUESTION: 57
An employee launched a privilege escalation attack to gain root access on one of the organization's database servers. The employee has an authorized user account on the server. What log file would MOST likely contain relevant information?
A. Database application log
B. Operating system log
C. IDS log
D. Firewall log
Answer: B (LEAVE A REPLY)
Operating system logs are the most relevant source of information for detecting and investigating privilege escalation attacks. These logs record authentication events, privilege changes, process executions, and system- level actions.
Because the attacker already had authorized access, firewall and IDS logs may show little or no suspicious activity. Database logs focus on database-level operations, not OS privilege changes.
OS logs provide the best visibility into actions such as sudo usage, kernel exploits, and unauthorized permission changes. They are essential for forensic analysis and incident response involving insider threats.

NEW QUESTION: 58
A structured way to align IT with business goals while managing risk and regulations:

A. GRC
B. Policies
C. Law
D. Standard
Answer: (SHOW ANSWER)
GRC (Governance, Risk, and Compliance) integrates business objectives with risk management and regulatory compliance.

NEW QUESTION: 59
Which term describes a communication tunnel that provides point-to-point transmission of both authentication and data traffic over an untrusted network?
A. None of the Above
B. Zero Trust
C. VPN
D. DMZ
Answer: C (LEAVE A REPLY)

NEW QUESTION: 60
A power outage disrupts operations. Which plan helps sustain operations?
A. DRP
B. IRP
C. BCP
D. All
Answer: C (LEAVE A REPLY)
Business Continuity Plans (BCP) focus on sustaining operations using alternative processes and resources during disruptions.

NEW QUESTION: 61
A security event, or combination of security events, that constitutes a secu incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization
A. Attack
B. Exploit
C. Intrusion
D. Threat
Answer: C (LEAVE A REPLY)

NEW QUESTION: 62
What principle states that individuals should only have the minimum set of permissions necessary to carry out their job functions?
A. Least privilege
B. Two-person control
C. Job rotation
D. Separation of privileges
Answer: A (LEAVE A REPLY)
The principle of least privilege states that users, systems, and processes should be granted only the minimum permissions required to perform their assigned tasks-nothing more. This principle reduces the attack surface and limits potential damage from compromised accounts or insider threats.
If an attacker gains access to a low-privilege account, the impact is significantly reduced compared to a highly privileged account. Least privilege also helps prevent accidental misuse of system resources.
Two-person control requires two individuals to approve an action. Job rotation reduces fraud by changing responsibilities. Separation of privileges ensures critical tasks require multiple permissions. While all are valid security concepts, least privilege directly addresses permission minimization.
This principle is foundational in access control models, identity and access management (IAM), and zero trust architectures. NIST and CIS explicitly recommend least privilege as a core security control for protecting systems and sensitive data.

NEW QUESTION: 63
An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available.
A. HTTP
B. IGMP
C. IP
D. ICMP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
What is the process of verifying a users identity called?
A. Authorization
B. Identification
C. Autentication
D. Confidentiality
Answer: C (LEAVE A REPLY)

NEW QUESTION: 65

An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n)

A. Event

B. Exploit

C. Intrusion

D. Malware

Answer: C (LEAVE A REPLY)

NEW QUESTION: 66

Preenka works at an airport. There are red lines painted on the ground next to the runway; Preenka has been instructed that nobody can step or drive across a red line unless they request, and get specific permission from, the control tower. This is an example of a(n)_____ control.

A. Administrative

B. Technical

C. Critical

D. Physical

Answer: A (LEAVE A REPLY)

NEW QUESTION: 67

Which is strongly used for Securing Wi-Fi

A. SSL

B. WEP

C. WPA2

D. WPA

Answer: C (LEAVE A REPLY)

NEW QUESTION: 68

What is the primary goal of a risk management process in cybersecurity?

A. to identify, assess, and mitigate cybersecurity risks to an acceptable level (Correct)

B. to transfer all cybersecurity risks to a third party

C. to eliminate all cybersecurity risks

D. to ignore cybersecurity risks and focus on incident response

Answer: (SHOW ANSWER)

NEW QUESTION: 69

What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?

A. defense in depth

B. separation of duties

C. Least privilege (Correct)

D. need-to-know basis

Answer: (SHOW ANSWER)

NEW QUESTION: 70
In information systems terms, the activities necessary to restore IT and communications services of an organization during and after an outage
A. IR
B. BC
C. DR
D. Risk Management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Uses multiple types of access controls in literal or theoretical
layers to help an organization avoid a monolithic security
A. VPN
B. VLAN
C. DMZ
D. Defence in Depth
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
Which type of authentication issomething which you know?
A. Type 1
B. Type 2
C. Type 3
D. Type 4
Answer: (SHOW ANSWER)
Type 1 authenticationrefers to "something you know," such as a password, PIN, or passphrase. This is the most common and oldest form of authentication used in information systems.
Other authentication types include Type 2 (something you have, such as a smart card or token) and Type 3 (something you are, such as biometrics). Some models also define additional types, such as location-based or behavior-based authentication.
While easy to implement, Type 1 authentication is considered the weakest because secrets can be guessed, reused, stolen, or phished. For this reason, security best practices strongly recommend combining it with other authentication types using multi-factor authentication (MFA).
NIST and CIS guidelines consistently discourage reliance on single-factor, knowledge-based authentication for sensitive systems due to its susceptibility to compromise.

NEW QUESTION: 73
The concept that the deployment of multiple types of controls provides better security than using a single type of control.

A. Internet
B. Defense in depth
C. VPN
D. Least privilege
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Jengi is setting up security for a home network. Jengi decides to configure MAC address filtering on the router, so that only specific devices will be allowed to join the network. This is an example of a(n)_____ control.
A. Physical
B. Substantial
C. Administrative
D. Technical
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
A transaction over $50,000 requires approval from both a manager and an accountant. Which concept applies?
A. MAC
B. Defense in Depth
C. Two-Person Integrity
D. Principle of Least Privilege
Answer: (SHOW ANSWER)
Two-Person Integrityensures no single individual can complete a sensitive action alone, reducing fraud and insider threats.

NEW QUESTION: 76
What is the most important aspect of security awareness/training?
A. Ensuring the confidentiality of data
B. Protecting health and human safety
C. Protecting assets
D. Maximizing business capabilities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
WF attack in which a subscriber currently authenticated to an Server and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the Server
A. Spoofing
B. ALL
C. XSS
D. CSRF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 78
When operating in a cloud environment, which cloud deployment model provides security teams with the greatest access to forensic information?
A. FaaS
B. SaaS
C. PaaS
D. IaaS
Answer: D (LEAVE A REPLY)
Infrastructure as a Service (IaaS) provides security teams with the greatest access to forensic data because customers retain control over operating systems, logs, storage, and network configurations.
In SaaS and FaaS models, the provider controls most of the infrastructure, limiting visibility. PaaS provides partial access but still restricts OS-level forensics.
IaaS allows collection of disk images, memory dumps, system logs, and network traffic, which are essential for incident response and forensic investigations.
Security teams prefer IaaS for high-control environments where deep visibility is required.

NEW QUESTION: 79
What is the goal of an incident response effort?
A. Save money
B. Punish wrongdoers
C. Reduce the impact of incidents on operations
D. No incident ever happen
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
What is the benefit of subnetting?
A. By increasing network bandwidth
B. By improving network security
C. By reducing network congestion
D. By simplifying network management
Answer: C (LEAVE A REPLY)

Subnetting divides a large network into smaller, logical segments called subnets. One of the primary benefits of subnetting isreducing network congestion. In a flat network, broadcast traffic is sent to all devices, which can significantly degrade performance as the network grows. By creating subnets, broadcast domains are limited, ensuring that broadcast traffic stays within a specific segment instead of flooding the entire network.
While subnetting can indirectly improve security and management, its most direct and measurable benefit is performance improvement through reduced broadcast traffic. Smaller subnets result in fewer devices competing for bandwidth, which enhances efficiency and reliability.
Subnetting also supports scalability and fault isolation. Network issues in one subnet are less likely to impact others. This concept is foundational in enterprise networks and is heavily emphasized in network design standards and certifications such as Security+, CCNA, and CISSP.

NEW QUESTION: 81
What is meant by non-repudiation?
A. It is a security feature that prevents session replay attacks.
B. If a user does something, they can't later claim that they didn't do it.
C. It is part of the rules set by administrative controls.
D. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
The section of the IT environment that is closest to the external world; where we locate IT systems that communicate with the Internet.
A. VLAN
B. RBAC
C. DMZ
D. MAC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 83
The city of Grampon wants to ensure that all of its citizens are protected from malware, so the city council creates a rule that anyone caught creating and launching malware within the city limits will receive a fine and go to jail. What kind of rule is this?
A. Law
B. Standard
C. Procedure
D. Policy
Answer: A (LEAVE A REPLY)

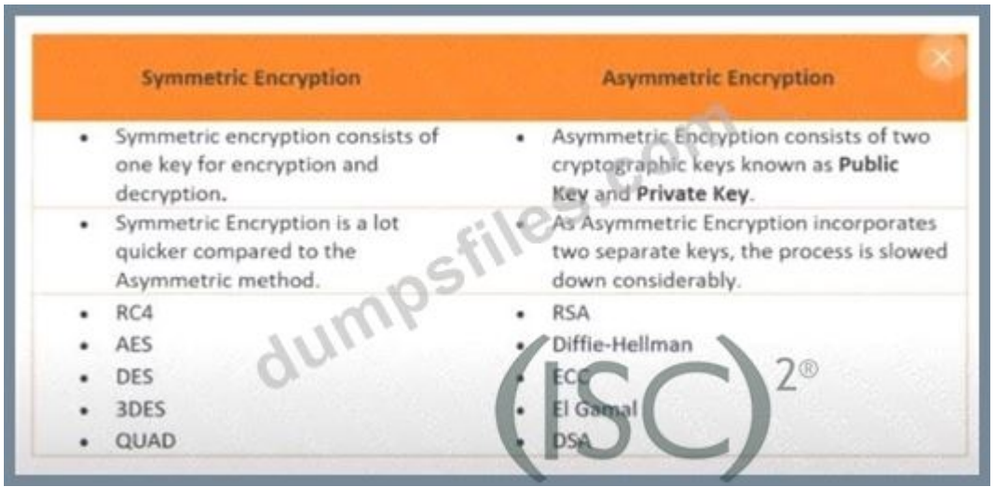
NEW QUESTION: 84
Communication between end systems is encrypted using a key, often known as_____?

A. Public Key
B. Section Key
C. Session Key
D. Temporary Key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
The Bell and LaPadula access control model is a form of
A. DAC
B. ABAC
C. MAC
D. RBAC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
organization experiences a security event that potentially jeopardizes the confidentiality, integrity or availability of its information system. What term best describes this situation?
A. Incident
B. Breach
C. Exploit
D. Event
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
Exhibit.



How many keys would be required to support 50 users in an asymmetric cryptography system?
A. 100
B. 200
C. 50
D. 1225

Answer: A (LEAVE A REPLY)

NEW QUESTION: 88
What is multi-factor authentication (MFA)?
A. A type of authentication that uses only one factor
B. A type of authentication that uses more than two methods (Correct)
C. A type of authentication that uses only two methods
D. A type of authentication that uses only one method
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
What is the purpose of the CIA triad?
A. Make security understandable
B. Describe security concepts
C. Define the purpose of security
D. All
Answer: D (LEAVE A REPLY)
The CIA triad provides a foundational framework for understanding and designing security controls.

NEW QUESTION: 90
What is the purpose of immediate response procedures in a BCP?
A. To notify personnel the BCP is activated
B. To guide management
C. To protect CIA
D. To account for operations
Answer: (SHOW ANSWER)
Immediate response checklists ensure rapid communication and awareness when a BCP is enacted.

NEW QUESTION: 91
Which is strongly used for securing Wi-Fi?
A. WPA2
B. WEP
C. WPA
D. SSL
Answer: A (LEAVE A REPLY)
WPA2uses strong encryption (AES) and is significantly more secure than WEP or WPA.

NEW QUESTION: 92
A set of rules that everyone must comply with and that usually carry monetary penalties for noncompliance are:
A. Standards
B. Policies
C. Procedures
D. Laws or regulations
Answer: (SHOW ANSWER)
Laws and regulations are legally enforceable and can impose fines or penalties. Standards and policies are not legally binding unless mandated by regulation.

NEW QUESTION: 93
Cyril wants to ensure all the devices on his company's internal IT environment are properly synchronized. Which of the following protocols would aid in this effort?
A. HTTP (Hypertext Transfer Protocol)
B. NTP (Network Time Protocol)
C. SMTP (Simple Mail Transfer Protocol)
D. FTP (File Transfer Protocol)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Which of the following is NOT a feature of a cryptographic hash function?
A. Deterministic
B. Unique
C. Useful
D. Reversible
Answer: D (LEAVE A REPLY)
Cryptographic hash functions areone-wayfunctions and are intentionallynot reversible. Given a hash value, it should be computationally infeasible to recover the original input.
Hash functions are deterministic (same input produces the same output), designed to minimize collisions (unique in practice), and useful for integrity verification, password storage, and digital signatures.
Reversibility would completely undermine their security purpose.

NEW QUESTION: 95
A means to allow remote users to have secure access to the internal IT environment.
A. VPN
B. VLAN
C. Internet

D. MAC
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following is not an appropriate control to add to privileged accounts?
A. Increased logging
B. Increased auditing
C. Multifactor authentication
D. Security deposit
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A set of security controls or system settings used to ensure uniformity of configuration through the IT environment?
A. Patches
B. Inventory
C. Baseline
D. Policy
Answer: C (LEAVE A REPLY)
A baseline is a documented set of approved security controls, configurations, and system settings used as a standard across an IT environment. Baselines ensure consistency, security, and compliance by defining how systems should be configured before deployment and during operation.
Security baselines are commonly derived from frameworks such as CIS Benchmarks, NIST SP 800-53, and vendor hardening guides. They help reduce misconfigurations, which are a leading cause of security breaches.
Patches address specific vulnerabilities, inventory tracks assets, and policies define high-level rules and expectations. Baselines translate policies into actionable technical settings, such as password policies, logging configurations, and service restrictions.
By enforcing baselines, organizations improve security posture, simplify audits, and enable faster incident response. Any deviation from the baseline can be detected and investigated, making baselines a cornerstone of secure and well-managed IT environments.

NEW QUESTION: 98
What security feature used in HTTPS
A. SSH
B. IPSec
C. ICMP
D. SSL/TLS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99

Mark works in the security office. During research, Mark learns that a configuration change could better protect the organization's IT environment. Mark makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of_____

A. Defense in depth
B. Holistic security
C. Segregation of duties
D. Threat intelligence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
A security event in which an intruder gains or attempts unauthorized access to a system is called:
A. Intrusion
B. Exploit
C. Threat
D. Attack
Answer: A (LEAVE A REPLY)
Anintrusionis an unauthorized attempt to access systems or resources, whether successful or not.

NEW QUESTION: 101
The amount of risk, at a broad level, that an organization is
willing to accept in pursuit of its strategic objectives.
A. Risk Assessment
B. Risk Appetite
C. Risk Transfer
D. Risk Management
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following properties is NOT guaranteed by digital signatures?
A. Authentication
B. Confidentiality
C. Non-repudiation
D. Integrity
Answer: B (LEAVE A REPLY)
Digital signatures provideauthentication,integrity, andnon-repudiation, but they donot provide confidentiality.
A digital signature verifies who sent the message and ensures it was not altered, but the content remains readable unless encryption is also applied.
Confidentiality requires encryption, typically using symmetric or asymmetric cryptography. Digital signatures are often combined with encryption (such as in TLS or secure email), but by themselves they do not hide message contents.

NEW QUESTION: 103
Which of the following is not a typical benefit of cloud computing services?
A. Metered usage
B. Scalability
C. Freedom from legal constraints
D. Reduced cost of ownership/investment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
John is concerned about a possible conflict of interest from a consulting side job. Which source should he consult?
A. ISC2 Code of Ethics
B. Organizational Code of Ethics
C. Country Code of Ethics
D. Organizational Security Policy
Answer: B (LEAVE A REPLY)
Potential conflicts of interest must be evaluated against the organization's internal code of ethics. While professional codes (like ISC2) are important, employment-related decisions are governed primarily by organizational ethics and HR policies.

NEW QUESTION: 105
What is the purpose of immediate response procedures and checklists in a BCP
A. To safeguard the confidentiality, integrity and availability of information
B. To ensure business operations are accounted for in the plan
C. To provide guidance for management
D. To notify personnel that the BCP is being enacted
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
An integrated platform and graphical tool for security testing of web applications is:
A. Burp Suite
B. Wireshark
C. Fiddler
D. Zenmap
Answer: A (LEAVE A REPLY)
Burp Suiteis widely used for web application security testing, including vulnerability scanning, interception, and penetration testing.

NEW QUESTION: 107
A company experiences a major IT outage and cannot perform critical business functions. Which plan helps recovery?
A. BCP
B. IRP
C. DRP
D. BIA
Answer: C (LEAVE A REPLY)
A Disaster Recovery Plan (DRP) provides procedures to restore IT systems, applications, and infrastructure after an outage.

NEW QUESTION: 108
Dani is an ISC2 member and an employee of New Corporation. One of Dani's colleagues offers to share a file that contains an illicit copy of a newly released movie. What should Dani do
A. Inform law enforcement
B. Refuse to accept
C. Accept the movie
D. Inform ISC2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
What are registered port used for
A. Common protocols at the core of TCP/IP model
B. Used for web servers
C. Used for in housed or opensource applications
D. Proprietary applications from vendors and develope
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following statements is true?
A. Logical access controls can protect the IT environment perfectly; there is no reason to deploy any other controls.
B. Administrative access controls can protect the IT environment perfectly; there is no reason to deploy any other controls.

C. It is best to use a blend of controls in order to provide optimum security.
D. Physical access controls can protect the IT environment perfectly; there is no reason to deploy any other controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Which type of application can intercept sensitive information such as passwords on a network segment?
A. Log server
B. Network scanner
C. Firewall
D. Protocol analyzer
Answer: D (LEAVE A REPLY)
A protocol analyzer, also known as a packet sniffer, captures and inspects network traffic flowing across a network segment. If traffic is unencrypted, protocol analyzers can intercept sensitive information such as usernames, passwords, session tokens, and application data.
Log servers store logs, network scanners identify hosts and services, and firewalls filter traffic based on rules. Only protocol analyzers are designed to capture and inspect packet contents.
This capability makes protocol analyzers valuable for troubleshooting and for attackers conducting eavesdropping attacks. Encryption protocols such as TLS are critical defenses against this risk.

NEW QUESTION: 112
Which of the following is a common security measure to prevent Cross Site Scripting (XSS) attacks in web applications?
A. using a firewall to block incoming traffic
B. validating and sanitizing user input (Correct)
C. encrypting data during transmission
D. implementing strong password policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 113
Which common cloud service model only offers the customer access to a given application?
A. Lunch as a service (LaaS)
B. Infrastructure as a service (IaaS)
C. Software as a service (SaaS)
D. Platform as a service (PaaS)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
What is the range of well-known ports?
A. 0-1023
B. 1024-49151

C. 49152-65535
D. None
Answer: (SHOW ANSWER)
Well-known ports (0-1023) are reserved for core services such as HTTP (80), HTTPS (443), FTP (21), and SSH (22).

NEW QUESTION: 115
The process of how an organization is managed and how decisions are made is called:
A. Standard
B. Policy
C. Procedure
D. Governance
Answer: D (LEAVE A REPLY)
Governancedefines oversight, accountability, and decision-making structures within an organization.

NEW QUESTION: 116
Example of a deterrent control:
A. CCTV
B. BCP
C. DRP
D. IRP
Answer: (SHOW ANSWER)
Deterrent controls are designed to discourage individuals from attempting unauthorized or malicious actions. CCTV systems act as deterrent controls because their visible presence can discourage theft, vandalism, or unauthorized access by increasing the perceived risk of being caught.
Business Continuity Plans (BCP), Disaster Recovery Plans (DRP), and Incident Response Plans (IRP) are corrective and recovery-focused controls, not deterrents. They address what happensafteran incident occurs.
Deterrent controls are often combined with preventive and detective controls to form a layered security strategy. Examples include warning signs, lighting, guards, and surveillance cameras. These controls play an important psychological role in reducing security incidents.

NEW QUESTION: 117
What is the difference between Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)?
A. BCP restores IT systems, DRP maintains business functions
B. DRP restores IT and communications, BCP maintains critical business functions
C. They are the same
D. BCP only applies before disasters
Answer: B (LEAVE A REPLY)
Disaster Recovery Planning focuses on restoringIT systems, infrastructure, and communicationsafter a disruption. Business Continuity Planning focuses onmaintaining critical business functionsduring and after incidents, often using alternative processes.

BCP is broader than DRP and includes people, processes, facilities, and third parties, while DRP is IT-centric. Both plans complement each other but serve different purposes.

NEW QUESTION: 118
Which of the following is an endpoint?
A. Router
B. Firewall
C. Laptop
D. Switch
Answer: (SHOW ANSWER)
Endpoints are user-facing devices such as laptops, desktops, and mobile devices.

NEW QUESTION: 119
Example of dynamic authorization:
A. DAC
B. RBAC
C. MAC
D. ABAC
Answer: D (LEAVE A REPLY)
Attribute-Based Access Control (ABAC) is considered a dynamic authorization model because access decisions are made in real time based on attributes of the user, resource, action, and environment. These attributes can include time of day, device type, location, data sensitivity, and user role.
Unlike RBAC or MAC, which rely on static roles or labels, ABAC evaluates policies dynamically using a policy decision point (PDP). This makes ABAC ideal for modern cloud, zero trust, and highly distributed environments.
DAC allows owners to grant permissions, RBAC uses predefined roles, and MAC relies on fixed security labels. ABAC provides the most flexible and context-aware authorization.

NEW QUESTION: 120
Larry and Fern both work in the data center. In order to enter the data center to begin their workday, they must both present their own keys (which are different) to the key reader, before the door to the data center opens.
Which security concept is being applied in this situation?
A. Dual control
B. Least privilege
C. Segregation of duties
D. Defense in depth
Answer: A (LEAVE A REPLY)

NEW QUESTION: 121
XenServer, LVM, Hyper-V, and ESXi are:
A. Type 2 hypervisors
B. Type 1 hypervisors

C. Both
D. None
Answer: (SHOW ANSWER)
These areType 1 (bare-metal) hypervisors, running directly on hardware without a host operating system, offering higher performance and security.

NEW QUESTION: 122
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
A. Availablity
B. DDOS
C. Authentication
D. Authetication
Answer: (SHOW ANSWER)

NEW QUESTION: 123
provide integrity services that allow a recipient to verify that a message has not been altered.
A. encryption
B. decryption
C. Hashing
D. encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 124
What is the primary purpose of a honeytoken in cybersecurity?
A. To lure and detect attackers
B. To encrypt sensitive data
C. To enhance network performance
D. To manage user access
Answer: A (LEAVE A REPLY)
Honeytokens are decoy data elements designed to lure attackers and detect unauthorized access. Examples include fake credentials, files, or database entries that have no legitimate use.

When a honeytoken is accessed, it triggers an alert, indicating a compromise. Honeytokens are valuable for detecting insider threats and lateral movement.
They do not encrypt data, improve performance, or manage access. Honeytokens are part of deception-based security strategies that enhance detection capabilities.

NEW QUESTION: 125
Which allows extremely granular restrictions down to individual machines or users?
A. DMZ
B. Microsegmentation
C. VLAN
D. NAC
Answer: B (LEAVE A REPLY)
Microsegmentation enables fine-grained, software-defined security controls, limiting lateral movement within networks.

NEW QUESTION: 126
Which of these tools is commonly used to crack passwords?
A. Burp Suite
B. Nslookup
C. Wireshark
D. John the Ripper
Answer: (SHOW ANSWER)
John the Ripper is a well-known password cracking tool used to test the strength of passwords by performing brute-force, dictionary, and hybrid attacks. It is commonly used by security professionals during penetration testing and password audits to identify weak credentials.
Burp Suite is a web application testing tool, Nslookup is a DNS query utility, and Wireshark is a packet analyzer. None of these tools are designed specifically for password cracking.
While John the Ripper can be used maliciously, it is also widely used defensively to improve password policies and enforce strong authentication practices. Its existence highlights the importance of strong passwords, hashing, salting, and multi-factor authentication.

NEW QUESTION: 127
An organization must always be prepared to _____ when applying a patch.
A. Settle lawsuits
B. Pay for the updated content
C. Buy a new system
D. Rollback
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
What does Criticality represents?

A. The importance an organization gives to data or an information system in performing its operations or achieving its mission
B. The need for security professional to ensure the appropriate levels of availavility are provided
C. All of the above
D. The need for consultation with the involved business ensure critical systems are identified and available
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
Why is security training important?
A. Because it fulfills regulatory requirements
B. Because it helps people perform job duties more efficiently
C. Because it reduces the risk of attacks such as social engineering
D. All
Answer: (SHOW ANSWER)
Theprimary purpose of security trainingis to reduce the likelihood and impact of attacks-especially human-centric threats such as phishing, social engineering, and credential theft. While training may also support compliance and efficiency, its most critical role is risk reduction.
Humans are often the weakest link in security. Awareness training helps users recognize threats, follow secure practices, and respond appropriately to suspicious activity, significantly lowering the organization's attack surface.

NEW QUESTION: 130
Who should participate in creating a BCP?
A. IT only
B. Management only
C. Members across the organization
D. Finance only
Answer: C (LEAVE A REPLY)
BCP requires input from all business units to identify dependencies and ensure continuity of critical functions.

NEW QUESTION: 131
A Company IT system experienced a system crash that result in a loss of data. What term best describes this event?
A. Breach
B. Adverse Event
C. Incident
D. Event
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
The means by which a threat actor carries out their objectives.

A. Threat
B. Threat Vector
C. Exploit
D. Intrusion
Answer: B (LEAVE A REPLY)
Athreat vectoris the path or method used by a threat actor to exploit vulnerabilities, such as phishing, malware, or network attacks.

NEW QUESTION: 133
Walmart has large ecommerce presence in world. Which of these solutions would ensure the LOWEST possible latency for their customers using their services?
A. CDN
B. Load Balancing
C. SaaS
D. Decentralized Data Centers
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Which OSI layer VPN works
A. Layer 5
B. Layer 3
C. Layer 1
D. Layer 6
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Dieter wants to send a message to Lupa and wants to be sure that Lupa knows the message has not been modified in transit. What technique/tool could Dieter use to assist in this effort?
A. Asymmetric encryption
B. Hashing
C. Clockwise rotation
D. Symmetric encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 136
Which is the loopback address?
A. ::1
B. 127.0.0.1
C. 255.255.255.0
D. Both A and B
Answer: D (LEAVE A REPLY)

The loopback address allows a system to test its own network stack.127.0.0.1is the IPv4 loopback address, while::1is its IPv6 equivalent. Both route traffic internally without leaving the host.

NEW QUESTION: 137
What is privacy in the context of Information Security?
A. Ensuring data is accurate and unchanged
B. Making sure data is always accessible when needed.
C. Disclosed without their consent
D. Protecting data from unauthorized access
Answer: (SHOW ANSWER)

NEW QUESTION: 138
Which document serves as specifications for implementing policy and dictates mandatory requirements?
A. Policy
B. Guideline
C. Standard
D. Procedure
Answer: C (LEAVE A REPLY)
Standards define mandatory technical or operational requirements that must be followed to comply with policy. Guidelines are optional, and procedures provide step-by-step instructions.

NEW QUESTION: 139
An outward-facing IP address used to access the Internet.
A. DNS
B. Global Address
C. Private Address
D. Public Address
Answer: D (LEAVE A REPLY)

NEW QUESTION: 140
A company wants to ensure that its employees can evacuate the building in case of an emergency. Which physical control is best suited?
A. Fire alarms

B. Exit signs
C. Emergency lighting
D. Emergency exit doors
Answer: D (LEAVE A REPLY)
Emergency exit doors are a critical physical control designed to ensure safe and rapid evacuation during emergencies such as fires or earthquakes. These doors are typically clearly marked, unobstructed, and may include panic bars to allow easy exit without special knowledge or tools.
Fire alarms alert occupants, exit signs provide direction, and emergency lighting improves visibility, but none of these physically enable evacuation. Exit doors directly support life safety by allowing people to leave the building quickly and safely. Life safety is the highest priority in physical security design, and exit doors are mandatory under building and fire safety codes.

NEW QUESTION: 141
Type of cyber attack carried out over a LAN that involves sending malicious packets to a default gateway on a LAN
A. ARP Poisoning
B. Ping of death
C. Syn Flood
D. Trojan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
Four main components of Incident Response are:
A. Preparation, Detection and Analysis, Containment, Eradication and Recovery
B. Preparation, Detection, Analysis and Containment
C. Detection, Analysis, Containment, Eradication and Recovery
D. All
Answer: A (LEAVE A REPLY)
According to NIST SP 800-61, incident response consists of four core phases:Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity. Option A best represents these core components.

NEW QUESTION: 143
What is the purpose of defense in depth?
A. Implement only technical controls
B. Provide unrestricted access
C. Establish multiple layered security controls
D. Guarantee no cyberattacks
Answer: (SHOW ANSWER)
Defense in depth uses multiple layers of controls-administrative, technical, and physical-so that failure of one layer does not compromise security.

NEW QUESTION: 144
Security needs to be provided to ____ data.
A. Restricted
B. Private
C. Illegal
D. All
Answer: A (LEAVE A REPLY)

NEW QUESTION: 145
Port used by DNS.
A. 53
B. 80
C. 45
D. 54
Answer: A (LEAVE A REPLY)
DNS primarily usesport 53over UDP and TCP for name resolution.

NEW QUESTION: 146
A prolonged, targeted cyberattack where an intruder remains undetected for an extended period is called:
A. Spoofing
B. Phishing
C. DoS
D. Advanced Persistent Threat
Answer: D (LEAVE A REPLY)
An Advanced Persistent Threat (APT) involves stealthy, long-term access to systems for espionage, data theft, or sabotage.

NEW QUESTION: 147
A tool that aggregates log data from multiple sources, and typically analyzes it and reports potential threats.
A. Anti-malware
B. SIEM
C. Router
D. HIDS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
Natalia is concerned that users on her network may be storing sensitive information, such as Social Security numbers, on their hard drives without proper authorization or security controls. What third-party security service can she implement to best detect this activity?
A. IDS - Intrusion Detection System

B. IPS - Intrusion Prevention System
C. DLP - Data Loss Protection
D. TLS - Transport Layer Security
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) solutions are specifically designed to detect, monitor, and prevent the unauthorized storage, use, or transmission of sensitive data such as Social Security numbers, credit card data, and personal records. DLP tools can scan endpoint hard drives, servers, databases, and cloud storage to identify sensitive data based on patterns, classifications, or content inspection.
IDS and IPS focus on detecting or blocking network attacks, not improper data storage. TLS encrypts data in transit but does not detect where sensitive data resides. DLP solutions directly address Natalia's concern by identifying policy violations related to sensitive data storage.
DLP is a critical control recommended by NIST and CIS for protecting regulated data and preventing data leakage across all data states.

NEW QUESTION: 149
Modern solutions try to provide a more holistic approach detecting rootkits, ransomware and spyware.
A. Antivirus
B. IDS
C. IPS
D. Anti Malware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 150
Which prevents threats?
A. Antivirus
B. IDS
C. SIEM
D. HIDS
Answer: A (LEAVE A REPLY)
Antivirus softwareis apreventive security controldesigned to stop known malware threats before they can execute or spread within a system. Antivirus solutions use signature-based detection, heuristic analysis, and increasingly behavior-based techniques to block malicious code such as viruses, worms, trojans, and ransomware.
In contrast,IDS (Intrusion Detection Systems)andHIDS (Host-based IDS)are primarilydetective controls.
They monitor systems and networks for suspicious activity but do not inherently block threats.SIEMplatforms aggregate and analyze logs for visibility and correlation; they support detection and response but do not directly prevent threats.
According to NIST SP 800-53, preventive controls are designed to stop incidents from occurring, while detective controls identify events after or during occurrence. Therefore, antivirus is the correct choice as it directly prevents threats.

NEW QUESTION: 151
Which of the following is not a protocol of the OSI layer 3
A. IGMP
B. IP
C. SSH
D. ICMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 152
Ludwig is a security analyst at Triffid, Inc. Ludwig notices network traffic that might indicate an attack designed to affect the availability of the environment. Which of the following might be the attack Ludwig sees?
A. An insider sabotaging the power supply
B. Spoofing
C. Exfiltrating stolen data
D. DDOS (distributed denial of service)
Answer: (SHOW ANSWER)

NEW QUESTION: 153
Who should participate in creation a business continuity plan
A. Onlymembersfrom thefinancedepartment
B. only members from the IT department
C. Onlymembersfrom the management team
D. Members from across the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 154
Which document serve as specifications for the implementation of policy and dictates mandatory requirements
A. Guideline
B. Policy
C. Procedures
D. Standard
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
How often should an organization test its business continuity plan
A. Routinely
B. Annually
C. Continually
D. Daily
Answer: A (LEAVE A REPLY)

NEW QUESTION: 156
A DLP solution should be deployed so it can inspect all forms of data leaving the organization, including:
A. Posting to websites
B. Applications and APIs
C. Copying to portable media
D. All
Answer: D (LEAVE A REPLY)
Effective DLP solutions monitor all egress channels to prevent unauthorized data exfiltration, including web uploads, APIs, and removable media.

NEW QUESTION: 157
Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.
A. Virus
B. Ma I ware
C. Rootkit
D. Bot
Answer: (SHOW ANSWER)

NEW QUESTION: 158
What is multi-factor authentication (MFA)?
A. A type of authentication that uses only one method
B. A type of authentication that uses only two methods
C. A type of authentication that uses more than two methods
D. A type of authentication that uses only one factor
Answer: (SHOW ANSWER)
Multi-factor authentication (MFA) requires two or more authentication factors from different categories: something you know, something you have, and something you are.
MFA significantly increases security by reducing reliance on any single factor. Even if one factor is compromised, attackers still cannot authenticate without the others.
MFA is widely recommended by NIST, CIS, and virtually all modern security frameworks, especially for privileged accounts and remote access.

NEW QUESTION: 159
Handel is a senior manager at Triffid, Inc., and is in charge of implementing a new access control scheme for the company. Handel wants to ensure that operational managers have the utmost personal choice in determining which employees get access to which systems/dat a. Which method should Handel select?
A. Security policy
B. Role-based access control (RBAC)
C. Mandatory access control (MAC)
D. Discretionary access control (DAC)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
The mitigation of violations of security policies and recommended practices is known as:
A. Disaster recovery
B. Incident response
C. Threat hunting
D. Incident response
Answer: D (LEAVE A REPLY)
Incident response focuses on detecting, containing, eradicating, and recovering from security incidents, including violations of policies and practices.

NEW QUESTION: 161
What does a breach refer to in the context of cybersecurity?
A. An unauthorized access to a system or system resource
B. Any observable occurrence in a network or system
C. A deliberate security incident
D. A previously known system vulnerability
Answer: A (LEAVE A REPLY)
Asecurity breachrefers to an incident where an unauthorized individual successfully gains access to a system, application, network, or data resource. Unlike a general security event, a breach confirms that confidentiality, integrity, or availability has been compromised. According to NIST SP 800-61, a breach occurs when security controls fail and protected information is accessed, disclosed, altered, or destroyed without authorization.
Not every event or intrusion results in a breach. For example, a blocked attack detected by an IDS is an event, not a breach. A breach has legal, regulatory, and business implications, often triggering notification requirements, forensic investigations, and remediation actions.

NEW QUESTION: 162
Ignoring a risk and continuing business operations is known as:
A. Risk acceptance
B. Risk mitigation
C. Risk avoidance
D. Risk transfer

Answer: A (LEAVE A REPLY)
Risk acceptance acknowledges the risk and chooses to proceed without additional controls, often due to cost or low impact.

NEW QUESTION: 163
Which of the following is very likely to be used in a disaster recovery (DR) effort?
A. Contract personnel
B. Guard dogs
C. Data backups
D. Anti-malware solutions
Answer: C (LEAVE A REPLY)

NEW QUESTION: 164
Organization experiences a security event that does not affect the confidentiality integrity and availability of its information system. What term BEST describes this situation?
A. Event
B. Breach
C. Incident
D. Exploit
Answer: (SHOW ANSWER)

NEW QUESTION: 165
Bluga works for Triffid, Inc. as a security analyst. Bluga wants to send a message to several people and wants the recipients to know that the message definitely came from Blug a. What type of encryption should Bluga use?
A. Asymmetric encryption
B. Small-scale encryption
C. Hashing
D. Symmetric encryption
Answer: A (LEAVE A REPLY)

NEW QUESTION: 166
In order for a biometric security to function properly, an authorized person's physiological data must be _____.
A. Modified
B. Stored
C. Broadcast
D. Deleted
Answer: (SHOW ANSWER)

NEW QUESTION: 167
What is the primary goal of input validation?
A. Secure storage
B. Prevent unauthorized access
C. Prevent code injection attacks
D. Encrypt data
Answer: C (LEAVE A REPLY)
Input validation ensures user inputs are sanitized and conform to expected formats, preventing injection attacks such as SQL injection and command injection.

NEW QUESTION: 168
Which principle states that users should have access only to the specific data and resources needed to perform required tasks?
A. Zero Trust
B. Defense in Depth
C. Least Privilege
D. All
Answer: C (LEAVE A REPLY)
ThePrinciple of Least Privilegeensures users, applications, and systems have only the minimum permissions necessary to perform their duties. This reduces the attack surface and limits potential damage if credentials are compromised.

NEW QUESTION: 169
_____ are virtual separations within a switch used mainly to limit broadcast traffic.
A. LAN
B. WAN
C. VLAN
D. MAN
Answer: C (LEAVE A REPLY)
VLANs reduce broadcast domains, improving performance and security.

NEW QUESTION: 170
DNS operates at which OSI layer?
A. Physical

B. Network
C. Application
D. Data Link
Answer: C (LEAVE A REPLY)
DNS is an application-layer protocol that resolves domain names to IP addresses using structured queries and responses.

NEW QUESTION: 171
You experienced a power outage that disrupted access to your data center. What type of security concern occurred?
A. Availability
B. Confidentiality
C. Integrity
D. Non-Repudiation
Answer: (SHOW ANSWER)

NEW QUESTION: 172
Which control identifies that an attack has occurred or is occurring?
A. Preventive control
B. Detective control
C. Corrective control
D. Recovery control
Answer: (SHOW ANSWER)
Detective controls such as IDS and logging systems identify malicious activity.

NEW QUESTION: 173
What is the goal of Business Continuity efforts?
A. Save money
B. Impress customers
C. Ensure all IT system continue to operate
D. Keep critical business functions operational
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
What does internal consistency of information refer to?
A. Accurate and complete data
B. Protection from errors
C. All data instances being identical
D. Same display format
Answer: C (LEAVE A REPLY)
Internal consistency ensures that all copies of data remain identical in content and meaning.

NEW QUESTION: 175
A tool used to inspect outbound traffic to reduce threats
A. Firewall
B. NIDC
C. Anti-ma I ware
D. DLP
Answer: (SHOW ANSWER)

NEW QUESTION: 176
"Wiring _____" is a common term meaning "a place where wires/conduits are often run, and equipment can be placed, in order to facilitate the use of local networks."
A. Closet
B. House
C. Bracket
D. Shelf
Answer: A (LEAVE A REPLY)

NEW QUESTION: 177
Which of the following protocols is a secure alternative to using Telnet?
A. SSH
B. HTTPS
C. SFTP
D. LDAPS
Answer: A (LEAVE A REPLY)
Secure Shell (SSH) is the secure alternative to Telnet. Telnet transmits data, including credentials, in clear text, making it vulnerable to interception. SSH encrypts all communications, providing confidentiality, integrity, and authentication.
HTTPS secures web traffic, SFTP is used for file transfer, and LDAPS secures directory services-not remote terminal access. SSH is the industry-standard replacement for Telnet.

NEW QUESTION: 178
Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.
A. DR
B. AII
C. IR
D. BC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 179
What is the recommended temperature range for optimal data center uptime?

A. 62°F-69°F
B. 64°F-81°F
C. 82°F-90°F
D. 91°F-100°F
Answer: B (LEAVE A REPLY)
ASHRAE recommends64°F-81°Ffor modern data centers to balance hardware longevity and energy efficiency.

NEW QUESTION: 180
Which type of software testing focuses on examining the source code for vulnerabilities and security issues?
A. Black-box testing
B. White-box testing
C. User acceptance testing
D. Functional testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 181
Actions, processes, and tools ensuring continuity of critical operations:
A. BC
B. DR
C. IR
D. All
Answer: A (LEAVE A REPLY)
Business Continuity encompasses the strategies, processes, and tools needed to keep critical operations running during a contingency.

NEW QUESTION: 182
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.
A. Availability
B. Criticality
C. Authorization
D. Confidentiality
Answer: (SHOW ANSWER)

NEW QUESTION: 183
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
A. IRP
B. DRP
C. Security Assessment
D. Risk Assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following is often associated with DR planning?
A. Checklists
B. Antivirus
C. firewall
D. All
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
A scam where a malicious website is made to look exactly like a trusted site is called:
A. DoS
B. Virus
C. Spoofing
D. Phishing
Answer: (SHOW ANSWER)
Website spoofing involves impersonating legitimate sites to deceive users. Phishing often uses spoofed sites but is the broader attack method.

NEW QUESTION: 186
A collection of actions that must be followed in order to complete a task or process in accordance with a set of rules
A. Policy
B. Law
C. Procedure
D. Standard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187
Finance Server and Transactions Server has restored its original facility after a disaster, what should be moved in FIRST?

A. Least critical functions
B. Most critical systems
C. Management
D. Most critical functions
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
A_____creates an encrypted tunnel to protect your personal data and communications
A. IDS
B. HTTPS
C. VPN
D. Anti-virus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
The prevention of authorized access to resources or delaying time-critical operations is known as:
A. DDoS
B. Authorization
C. Authentication
D. Availability
Answer: A (LEAVE A REPLY)
Distributed Denial-of-Service (DDoS) attacks disrupt availability by overwhelming systems, preventing legitimate access.

NEW QUESTION: 190
Which type of database combines related records and fields into a logical tree structure?
A. Relational
B. Hierarchical
C. Object-oriented
D. Network
Answer: B (LEAVE A REPLY)
A hierarchical database organizes data in a tree-like structure where each parent record can have multiple child records, but each child has only one parent. This model resembles a file system hierarchy and is designed to represent one-to-many relationships efficiently.
Hierarchical databases were among the earliest database models and are still used in specific environments such as legacy systems and mainframe applications. Data access is fast when the hierarchy is well understood, but the model lacks flexibility when relationships become complex.
Relational databases use tables with rows and columns, object-oriented databases store objects, and network databases allow many-to-many relationships. Only the hierarchical model strictly enforces a tree structure.
Understanding database models is important for security professionals when evaluating access control, data exposure, and system design risks.

NEW QUESTION: 191
Governments can impose financial penalties as a consequence of breaking a:
A. Standard
B. Regulation
C. Policy
D. Procedure
Answer: B (LEAVE A REPLY)
Regulations are legally enforceable requirements issued by governments or regulatory bodies. Violating regulations such as GDPR, HIPAA, or PCI DSS can result in fines and penalties.
Standards, policies, and procedures may influence compliance but do not carry direct legal penalties unless codified into law.

NEW QUESTION: 192
Network traffic originating from outside the organization might be admitted to the internal IT environment or blocked at the perimeter by a _____.
A. Fence
B. Turnstile
C. Vacuum
D. Firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 193
Which drives for the IPv6 introduction
A. IPV6 support WiFi
B. Because IPv4 was projected to be exhausted
C. IPv4 was not secured
D. IPv4 not combatible with new devices
Answer: (SHOW ANSWER)

NEW QUESTION: 194
IDS can be described in terms of what fundamental functional components?
A. Response
B. Information sources
C. Analysis
D. All of the choices
Answer: D (LEAVE A REPLY)
An Intrusion Detection System (IDS) consists of three fundamental functional components: information sources, analysis engines, and response mechanisms. Information sources collect data such as network packets, logs, or system events. Analysis engines evaluate this data to detect suspicious behavior. Response components generate alerts or notifications.

While IDS systems typically do not block traffic (unlike IPS), they still perform response actions such as logging, alerting, and triggering workflows.
All three components work together to detect and report security incidents. This architecture is well documented in NIST intrusion detection guidance and forms the basis of both host-based and network-based IDS solutions.

NEW QUESTION: 195
255.255.255.0 represents:
A. Broadcast address
B. Unicast address
C. Subnet mask
D. Global address
Answer: C (LEAVE A REPLY)
255.255.255.0is a commonly usedsubnet mask, indicating that the first 24 bits represent the network portion of an IPv4 address. Subnet masks define how IP addresses are divided into network and host portions, enabling efficient routing and segmentation.

NEW QUESTION: 196
Triffid Corporation has a rule that all employees working with sensitive hardcopy documents must put the documents into a safe at the end of the workday, where they are locked up until the following workday. What kind of control is the process of putting the documents into the safe?
A. Physical
B. Technical
C. Administrative
D. Tangential
Answer: (SHOW ANSWER)

NEW QUESTION: 197
Permitting authorized access while preventing improper disclosure.
A. Integrity
B. Confidentiality
C. Availability
D. All
Answer: B (LEAVE A REPLY)

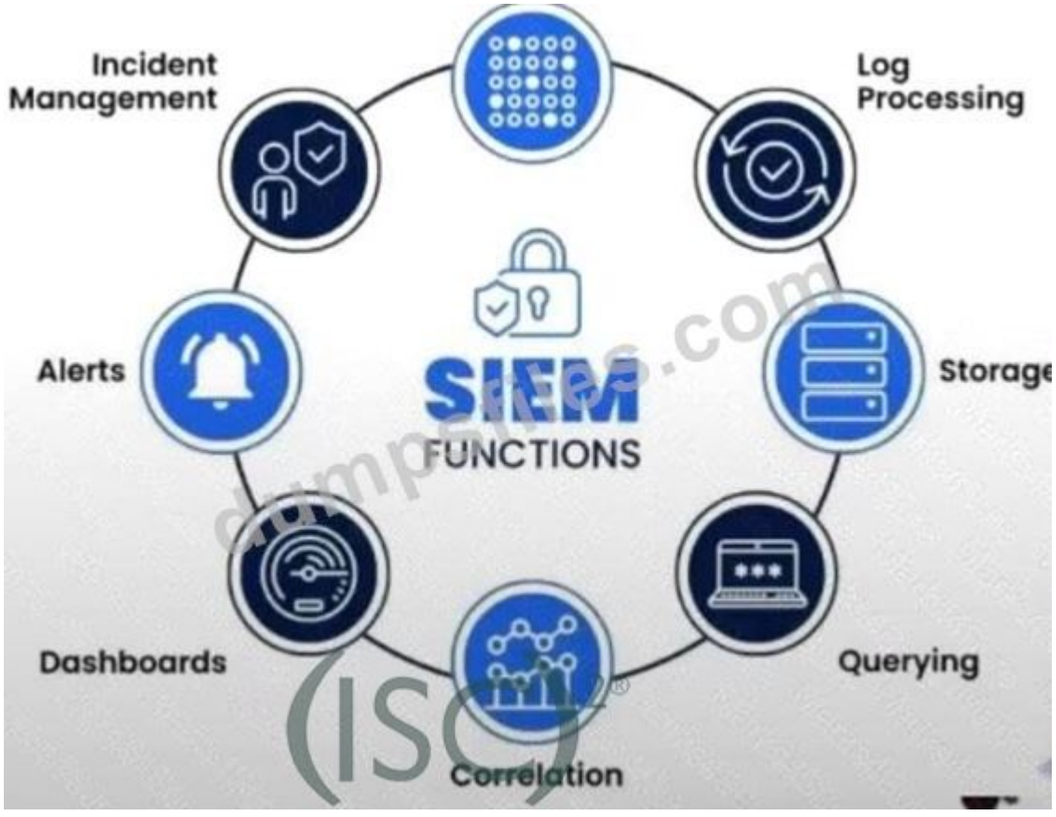
Confidentiality ensures information is accessible only to authorized individuals.

NEW QUESTION: 198
What is the difference between hub and switch
A. A hub can create separate broad cast domains when used to create Vlan
B. A hub is less likely to be used in home network
C. A hub retransmits traffic to all devices, while a switch route traffic to a specific devices
D. A switch retransmits traffic to all devices, while a hub route traffic to a specific devices
Answer: C (LEAVE A REPLY)

NEW QUESTION: 199
Gary is an attacker. Gary is able to get access to the communication wire between Dauphine's machine and Linda's machine and can then surveil the traffic between the two when they're communicating. What kind of attack is this?
A. On-path
B. Side channel
C. DDOS
D. Physical
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
A measure of an organization's baseline security performance is a:
A. Security assessment
B. Security audit
C. Security benchmark
D. Security management
Answer: C (LEAVE A REPLY)
Security benchmarks define baseline performance and configuration standards against which systems are measured.

NEW QUESTION: 201
Exhibit.



What is the purpose of a Security Information and Event Management (SIEM) system?

A. Blocking malicious websites

B. Managing user passwords

C. Encrypting files

D. Monitoring and analyzing security events -

Answer: D (LEAVE A REPLY)

NEW QUESTION: 202

An authorized simulated attack to evaluate security is called:

A. Penetration test

B. Security testing

C. Automated testing

D. Regression testing

Answer: A (LEAVE A REPLY)

Penetration testing simulates real-world attacks to identify vulnerabilities before adversaries exploit them.

NEW QUESTION: 203

Which of the following uses registered port

A. MS Sql server

B. SMB

C. HTTP

D. TCP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 204
Devid is worried about distributed denial of service attacks against his company's primary web application, which of the following options will provide the MOST resilience against large-scale ddos attacks?
A. Contract for DDoS mitigation services via the company's IPS
B. Increase the amount of bandwidth available from one or more ISPs
C. Implement a CDN
D. Increase the number of servers in the web application server cluster
Answer: (SHOW ANSWER)

NEW QUESTION: 205
Glen is an (ISC)² member. Glen receives an email from a company offering a set of answers for an (ISC)² certification exam. What should Glen do?
A. Nothing
B. Inform (ISC)²
C. Inform Glen's employer
D. Inform law enforcement
Answer: B (LEAVE A REPLY)

NEW QUESTION: 206
Which of the following best describes the puposes of a business impact analysis?
A. To provide a high level overview of the disaster recovery plan
B. To mitigate security violation and ensure that business operation can continue during a contigency
C. To document a predetermined set of instructions or procedures for restoring IT and communications services after a disruption
D. To analyze an information systems requirements and functions in order to determine system contingency priorities
Answer: (SHOW ANSWER)

NEW QUESTION: 207
Exhibit.

What is the PRIMARY purpose of a web application firewall (WAF)?

A. To monitor network traffic for intrusions

B. To protect the web server from DDoS attacks

C. To manage SSL certificates

D. To filter and block malicious web traffic and requests

Answer: (SHOW ANSWER)

NEW QUESTION: 208

A security practitioner who needs step-by-step instructions to complete a provisioning task

A. Standard

B. Policy

C. Laws or Regulations

D. Procedure

Answer: (SHOW ANSWER)

NEW QUESTION: 209

Phrenal is selling a used laptop in an online auction. Phrenal has estimated the value of the laptop to be $100, but has seen other laptops of similar type and quality sell for both more and less than that amount. Phrenal hopes that the laptop will sell for $100 or more, but is prepared to take less for it if nobody bids that amount. This is an example of _____.

A. Threat

B. Vulnerability

C. Risk tolerance

D. Risk inversion

Answer: C (LEAVE A REPLY)

NEW QUESTION: 210

What is the priority of incident response in the context of incident management
A. Reduce the impact of the incident
B. Resume interrupted operations as soon as possible
C. Protect life health and safety
D. Protect the organization mission and objectives
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
What is the primary goal of network segmentation in cybersecurity?
A. To increase network speed
B. To isolate and protect critical assets
C. To centralize data storage
D. To expand network coverage
Answer: B (LEAVE A REPLY)
Network segmentation isolates systems and resources into separate security zones to limit lateral movement by attackers. By segmenting networks, organizations protect critical assets and reduce the impact of breaches.
If one segment is compromised, segmentation prevents attackers from easily accessing other systems. This approach supports defense-in-depth and zero trust architectures.
Network segmentation is implemented using VLANs, firewalls, and access controls and is a foundational security practice recommended by NIST and CIS.

NEW QUESTION: 212
An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant
A. CSRF
B. Eavesdropping Attack
C. ARP Spoofing
D. XSS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 213
Which component of the incident response plan involves identifying critical data and systems?
A. Detection and Analysis

B. Eradication
C. Cantainment
D. Preparation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 214
What is the recommended fire suppression system for server rooms
A. Powder based
B. Foam based
C. Water based
D. ftac hacorl
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
True or False: The IT department is responsible for creating the organization's Business Continuity Plan.
A. True
B. False
Answer: (SHOW ANSWER)
BCP is anorganization-wide responsibility. While IT plays a key role, BCP requires participation from all business units, leadership, HR, facilities, and external partners.

NEW QUESTION: 216
Which of the following is an example of a "something you are" authentication factor?
A. Your password and PIN
B. A photograph of your face
C. A credit card presented to a cash machine
D. A user ID
Answer: (SHOW ANSWER)

NEW QUESTION: 217
A structured approach used to oversee and manage risk for an enterprise
A. Risk appetite
B. Risk threshold
C. Risk Assessment
D. Risk Management Framework
Answer: (SHOW ANSWER)

NEW QUESTION: 218
Which type of Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) are completely vulnerable to 0-day attacks?
Response:

A. Signature based.
B. Behavioral based.
C. Network based.
D. Heuristic based.
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Mark has purchased a Mac laptop. He is scared of losing his screen and is planning to buy an insurance policy. Which risk management strategy is this?
A. Risk acceptance
B. Risk deterrence
C. Risk transference
D. Risk mitigation
Answer: (SHOW ANSWER)
Risk transference is a risk management strategy in which an organization or individual shifts the financial impact of a risk to a third party. Purchasing insurance is a classic example of risk transference. In this scenario, Mark transfers the financial consequences of potential damage to the laptop screen to the insurance provider.
Risk acceptance involves acknowledging a risk and choosing to do nothing. Risk deterrence discourages risky behavior through controls or penalties. Risk mitigation reduces the likelihood or impact of a risk through safeguards such as protective cases or training.
Risk transference does not eliminate the risk itself; the laptop can still be damaged. However, it reduces the financial burden associated with the event. In cybersecurity, common examples include cyber insurance, outsourcing, and service-level agreements (SLAs).
This strategy is widely recognized in risk management frameworks such as NIST SP 800-30 and ISO 31000 as an appropriate option when mitigation is too costly or impractical.

NEW QUESTION: 220
Dylan is creating a cloud architecture that requires connections between systems in two different private VPCs. What would be the best way for Dylan to enable this access?
A. Public IP Address
B. Internet Gateway
C. VPN Connection
D. VPC Endpoint
Answer: (SHOW ANSWER)

NEW QUESTION: 221
Configuration settings or parameters stored as data and managed through a software graphical user interface (GUI) are examples of:
A. Logical access control
B. Physical access control
C. Administrative access control

Answer: A (LEAVE A REPLY)
Logical access controls are implemented through software and system configurations. They include settings such as user permissions, authentication mechanisms, firewall rules, and system policies managed through GUIs or command-line interfaces. Logical controls protect digital assets by restricting access based on identity and authorization.

NEW QUESTION: 222
A scammer will attempt to make a malicious website look exactly like a legitimate one that the victim knows and trusts
A. DOS
B. Spoofing
C. Virus
D. Phishing
Answer: (SHOW ANSWER)

NEW QUESTION: 223
Which attack attempts to gain information by observing a device's power consumption?
A. DoS
B. Side-channel attack
C. XSS
D. CSRF
Answer: B (LEAVE A REPLY)
Side-channel attacks exploit physical characteristics such as power usage, timing, or electromagnetic emissions to infer sensitive information like cryptographic keys.

NEW QUESTION: 224
Provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.
A. Hashing
B. Cryptography
C. AII
D. Encoding
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
If two people want to use asymmetric communication to conduct a confidential conversation, how many keys do they need?
A. 8
B. 4
C. 11
D. 1

Answer: (SHOW ANSWER)

NEW QUESTION: 226
Prachi works as a database administrator for Triffid, Inc. Prachi is allowed to add or delete users, but is not allowed to read or modify the data in the database itself. When Prachi logs onto the system, an access control list (ACL) checks to determine which permissions Prachi has.
In this situation, what is the ACL?
A. The rule
B. The object
C. The firmware
D. The subject
Answer: A (LEAVE A REPLY)

NEW QUESTION: 227
Which type of network is set up similar to the internet but is private to an organization? Select the MOST appropriate answer.
A. Extranet
B. VLAN
C. Intranet
D. VPN
Answer: C (LEAVE A REPLY)
An intranet is a private network that uses internet technologies (such as TCP/IP and web browsers) but is accessible only to an organization's internal users. It mirrors the structure and functionality of the internet while remaining private.
An extranet extends limited access to external partners. A VLAN is a logical network segmentation technique.
A VPN is a secure communication tunnel, not a network architecture.
Intranets are commonly used for internal portals, documentation, collaboration tools, and internal services.
From a security standpoint, intranets require strong authentication, segmentation, and access controls.

NEW QUESTION: 228
Risk tolerance is also known as:
A. Risk threshold
B. Risk appetite

C. Acceptable risk
D. All
Answer: D (LEAVE A REPLY)
Risk tolerance, risk appetite, and acceptable risk are closely related terms describing how much risk an organization is willing to accept.

NEW QUESTION: 229
Which attack most effectively maintains remote access and control over a victim's computer?
A. Phishing
B. Trojans
C. XSS
D. Rootkits
Answer: D (LEAVE A REPLY)
Rootkits provide stealthy, persistent control by hiding malicious processes and maintaining privileged access. They are extremely difficult to detect and remove.

NEW QUESTION: 230
Which type of control is used to restore systems or processes to their normal state after an attack has occurred
A. Recovery Control
B. Detective Control
C. Corrective Control
D. Compensatory Control
Answer: C (LEAVE A REPLY)

NEW QUESTION: 231
An outward-facing IP address used to access the Internet is a:
A. Global address
B. Private address
C. Public address
D. DNS
Answer: (SHOW ANSWER)
Public IP addresses are routable on the Internet and assigned by ISPs.

NEW QUESTION: 232
An attacker places themselves between two communicating devices is known as:
A. Phishing
B. Spoofing
C. On-Path attack
D. All
Answer: C (LEAVE A REPLY)

AnOn-Path (Man-in-the-Middle)attack allows attackers to intercept, modify, or replay communications between two parties without their knowledge.

NEW QUESTION: 233
What is the best practice to clear SSD storage after use?
A. Zero fill
B. Degaussing
C. Clearing
D. Disintegration
Answer: D (LEAVE A REPLY)
SSDs do not reliably respond to overwriting or degaussing due to wear-leveling. Physical destruction such as disintegration is the most secure sanitization method, per NIST SP 800-88.

NEW QUESTION: 234
What type of attack does the attacker store and reuse login information. Select the BEST answer?
A. Smurf attack
B. Replay attack
C. Man-in-the-middle attack
D. DDoS attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 235
Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs)
A. Simulation
B. Hypervisor
C. Cloud Controller
D. Emulation
Answer: (SHOW ANSWER)

NEW QUESTION: 236
The means by which a threat actor carries out their objectives
A. Threat
B. Intrusion
C. Exploit
D. Threat Vector
Answer: D (LEAVE A REPLY)

NEW QUESTION: 237
Why is a "Red Book" important in Business Continuity Planning?
A. To have a hard copy for easy access
B. Easy to carry and transfer

C. When disasters disable power and electronic access
D. All
Answer: C (LEAVE A REPLY)
A Red Book is ahard-copy version of critical business continuity and emergency procedures. It is essential when disasters such as hurricanes, earthquakes, or cyberattacks disable power, networks, or electronic backups. In such scenarios, electronic access may be impossible, making physical documentation vital.

NEW QUESTION: 238
Which type of fire-suppression system is typically the safest for humans?
A. Water
B. Gaseous
C. Dirt
D. Oxygen-depletion
Answer: (SHOW ANSWER)

NEW QUESTION: 239
The DevOps team has updated the application source code. Tom discovered that many unauthorized changes have been made. What is the BEST control Tom can implement to prevent a recurrence of this problem?
A. Backup
B. File labels
C. Security audit
D. Hashing
Answer: (SHOW ANSWER)
Hashing is the best control for detecting unauthorized changes to source code. By generating cryptographic hash values for approved versions of files, any modification-intentional or accidental-will result in a different hash, immediately indicating tampering.
Backups help recover data but do not prevent or detect unauthorized changes. File labels provide classification but do not ensure integrity. Security audits review compliance but do not continuously detect changes.
Hashing supports integrity assurance, which is a core security objective. Tools such as file integrity monitoring (FIM) systems rely on hashing to alert administrators when files are altered unexpectedly.
NIST and CIS controls emphasize hashing and integrity monitoring as essential for protecting code repositories, system files, and critical configurations, especially in DevOps and CI/CD environments.

NEW QUESTION: 240
Which is the first step in the risk management process?
A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment
Answer: C (LEAVE A REPLY)

Risk identification is the first step in the risk management process. Organizations must first identify assets, threats, and vulnerabilities before they can assess likelihood or impact. Without knowing what risks exist, meaningful assessment and mitigation are impossible.

NEW QUESTION: 241
How do you distinguish authentication and identification?
A. Both are the same
B. Authentication verifies identity
C. Authentication verifies identity; identification claims identity
D. Identification verifies identity
Answer: B (LEAVE A REPLY)
Identification is the act of claiming an identity (e.g., username). Authentication is the process of verifying that claim (e.g., password, biometrics). Authorization follows authentication.

NEW QUESTION: 242
What is the benefit of subnet
A. By simplifying network management
B. By reducing network congestion
C. By improving network security
D. By increasing network bandwidth
Answer: B (LEAVE A REPLY)

NEW QUESTION: 243
A newly enforced BYOD policy represents which control type?
A. Physical control
B. Logical control
C. Administrative control
D. Technical control
Answer: (SHOW ANSWER)
Policies are administrative controls that define acceptable behavior and organizational rules.

NEW QUESTION: 244

A collection of actions that must be followed to complete a task or process in accordance with a set of rules is known as:

A. Policy

B. Procedure

C. Law

D. Standard

Answer: B (LEAVE A REPLY)

Aprocedureis a detailed, step-by-step set of instructions that explainshowto perform a task in compliance with policies and standards. Procedures translate high-level requirements into actionable guidance for staff.

Policies define what must be done, standards specify mandatory requirements, and procedures explain exactly how to carry them out. Laws are external legal mandates, not internal operational documents.

For example, a security policy may require access reviews, a standard may define review frequency, and a procedure will outline the exact steps to conduct the review. Procedures ensure consistency, reduce errors, and support compliance and auditing efforts.

NEW QUESTION: 245

An attack in which an attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the claimant is known as:

A. Eavesdropping attack

B. CSRF

C. XSS

D. ARP spoofing

Answer: A (LEAVE A REPLY)

An eavesdropping attack occurs when an attacker passively intercepts network communications to capture sensitive information such as credentials, session tokens, or authentication exchanges. This data can later be reused in impersonation or replay attacks.

CSRF and XSS are application-layer attacks, while ARP spoofing is an active network attack. Eavesdropping relies on unencrypted or weakly protected communications, highlighting the importance of TLS and secure authentication protocols.

NEW QUESTION: 246

Proper alignment of security policy and business goals within the organization is important because:

A. Bad security policy can be illegal

B. Security policy that conflicts with business goals can inhibit productivity

C. Security should always be as strict as possible

D. Security is more important than business

Answer: B (LEAVE A REPLY)

NEW QUESTION: 247

Which of the following is a characteristic of cloud computing?

A. Broad network access

B. Rapid elasticity
C. Measured service
D. All
Answer: D (LEAVE A REPLY)
Cloud computing is defined by five essential characteristics per NIST: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Therefore, all listed options are valid characteristics.

NEW QUESTION: 248
The first phase of the System Development Life Cycle (SDLC) is:
A. Requirements analysis
B. Feasibility study
C. Design
D. Development
Answer: B (LEAVE A REPLY)
The feasibility study determines whether a project is technically, economically, and operationally viable before development begins.

NEW QUESTION: 249
Tekila works for a government agency. All data in the agency is assigned a particular sensitivity level, called a "classification." Every person in the agency is assigned a "clearance" level, which determines the classification of data each person can access.
What is the access control model being implemented in Tekila's agency?
A. DAC (discretionary access control)
B. RBAC (role-based access control
C. MAC (mandatory access control)
D. FAC (formal access control)
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Security control used to protect against environmental threats such as fire, flood and earth quakes
A. Thechnical control
B. Physical control
C. Adminstrative Control
D. Logical Control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
An approach using software-based controllers and APIs to direct network traffic:
A. VLAN
B. SDN

C. VPN
D. SAN
Answer: B (LEAVE A REPLY)
Software-Defined Networking (SDN) separates the control plane from the data plane, enabling centralized and programmable network management.

NEW QUESTION: 252
Triffid, Inc., has many remote workers who use their own IT devices to process Triffid's information. The Triffid security team wants to deploy some sort of sensor on user devices in order to recognize and identify potential security issues. Which of the following is probably most appropriate for this specific purpose?
A. NIDS (network-based intrusion-detection systems)
B. LIDS (logistical intrusion-detection systems)
C. Firewalls
D. HIDS (host-based intrusion-detection systems)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 253
What type of attack does the attacker store and reuse login information? Select the BEST answer.
A. Man-in-the-middle attack
B. Smurf attack
C. DDoS attack
D. Replay attack
Answer: D (LEAVE A REPLY)
A replay attack occurs when an attacker captures valid authentication data-such as login credentials, session tokens, or cryptographic handshakes-and later reuses that data to gain unauthorized access. The attacker does not need to know the actual password; instead, they replay previously captured authentication information. Replay attacks often exploit systems that lack proper protections such as timestamps, nonces, session expiration, or cryptographic challenge-response mechanisms. These attacks are particularly dangerous in poorly secured authentication protocols or legacy systems.
A man-in-the-middle attack involves intercepting and potentially altering communications in real time, while a replay attack focuses on reusing captured data. Smurf attacks and DDoS attacks target availability, not authentication.
Security controls such as time-based tokens, one-time passwords, mutual authentication, and secure protocols (e.g., TLS) are commonly used to prevent replay attacks. NIST authentication guidelines explicitly recommend replay resistance as a core requirement for secure authentication systems.

NEW QUESTION: 254
What is remanence?
A. The ability of retaining magnetization in a storage disk after deletion
B. Files or pieces of files get scattered throughout your disks
C. Data corruption due to disk failure

D. All

Answer: A (LEAVE A REPLY)

Data remanence refers to the residual representation of data that remains on storage media even after attempts have been made to delete or erase it. When files are deleted, the operating system typically removes references to the data rather than overwriting the actual bits on the disk. As a result, the data may still be recoverable using forensic tools.

Remanence is especially relevant for magnetic storage, solid-state drives, and backup media. Because of this risk, security standards recommend proper media sanitization techniques such as overwriting, degaussing, or physical destruction. NIST SP 800-88 specifically addresses media sanitization methods to mitigate remanence risks.

This concept is critical when disposing of or repurposing storage devices, particularly those that previously contained sensitive or regulated data.

NEW QUESTION: 255

You are reviewing log data from a router; there is an entry that shows a user sent traffic through the router at 11:45 am, local time, yesterday. This is an example of a(n) _____.

A. Attack

B. Incident

C. Threat

D. Event

Answer: D (LEAVE A REPLY)

NEW QUESTION: 256

Derrick logs on to a system in order to read a file. In this example, Derrick is the _____?

A. Subject

B. Object

C. Process

D. Predicate

Answer: A (LEAVE A REPLY)

In access control models, asubjectis an active entity that requests access to a resource. In this scenario, Derrick is the subject because he is the user initiating an action-logging into a system and attempting to read a file. Subjects can be users, processes, or systems acting on behalf of users.

Anobject, by contrast, is a passive entity that is being accessed, such as a file, database, printer, or network resource. The file Derrick wants to read is the object. Access control systems evaluate whether a subject has the appropriate permissions to perform an action (such as read, write, or execute) on an object.

This subject-object relationship is foundational to many security models, including discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Proper identification of subjects is essential for authentication, authorization, auditing, and accountability. By clearly defining who the subject is, organizations can enforce least privilege, track user actions, and maintain strong security governance across systems.

NEW QUESTION: 257
Which of these components is very likely to be instrumental to any disaster recovery (DR) effort?
A. Routers
B. Laptops
C. Firewalls
D. Backups
Answer: (SHOW ANSWER)
Backups are one of the most critical components of any disaster recovery (DR) strategy. Disaster recovery focuses on restoring systems, data, and operations after a disruptive event such as a cyberattack, natural disaster, hardware failure, or human error. Without reliable backups, recovery may be impossible or severely delayed.
Backups ensure that critical data can be restored to a known good state, minimizing data loss and downtime. Industry frameworks such as NIST SP 800-34 and ISO/IEC 27031 emphasize backups as a foundational DR control. They support recovery time objectives (RTOs) and recovery point objectives (RPOs), which define how quickly systems must be restored and how much data loss isacceptable.
While routers, laptops, and firewalls are important infrastructure components, they can typically be replaced or reconfigured. Lost or corrupted data, however, may be irreplaceable without backups. Best practices include maintaining regular, automated backups, storing them offsite or in the cloud, and protecting them from ransomware using immutable or offline storage. Testing backups regularly is also essential to ensure they are usable during an actual disaster.

NEW QUESTION: 258
A DDoS attack flooding ICMP packets is called:
A. DoS
B. SYN flood
C. Smurf attack
D. Phishing
Answer: (SHOW ANSWER)
A Smurf attack amplifies ICMP traffic to overwhelm targets.

NEW QUESTION: 259
Security commensurate with risk and magnitude of harm is known as:
A. Risk management

B. Risk assessment
C. Risk mitigation
D. Adequate security
Answer: D (LEAVE A REPLY)
Adequate securitymeans applying controls proportional to risk and potential impact, a core concept in NIST frameworks.

NEW QUESTION: 260
An employee launched a privilege escalation attack to gain root access on one of the organization's database servers. The employee has an authorized user account on the server. What log file would MOST likely contain relevant information?
A. Database application log
B. Firewall log
C. Operating system log
D. IDS log
Answer: (SHOW ANSWER)
Operating system logs are the most relevant source of information for detecting and investigating privilege escalation attacks. These logs record authentication events, privilege changes, process executions, and system- level actions.
Because the attacker already had authorized access, firewall and IDS logs may show little or no suspicious activity. Database logs focus on database-level operations, not OS privilege changes.
OS logs provide the best visibility into actions such as sudo usage, kernel exploits, and unauthorized permission changes. They are essential for forensic analysis and incident response involving insider threats.

NEW QUESTION: 261
A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period of time.
A. Spoofing
B. Phishing
C. Advanced Persistent Threat
D. DOS
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Who must follow HIPAA compliance?
A. Energy sector
B. Health care
C. Finance sector
D. All
Answer: B (LEAVE A REPLY)

HIPAA applies to healthcare providers, insurers, and their business associates to protect patient health information (PHI).

NEW QUESTION: 263
Which security control is designed to prevent unauthorized access to sensitive information by ensuring it is accessible only to authorized users?
A. Encryption
B. Firewall
C. Antivirus
D. Access control
Answer: D (LEAVE A REPLY)
Access control ensures that only authorized users can access specific resources. It includes authentication, authorization, and enforcement mechanisms.
Encryption protects data confidentiality, firewalls control network traffic, and antivirus detects malware. Only access control directly governs who can access sensitive information.

NEW QUESTION: 264
A/hich layer of the OSI Layer model is the target of a buffer overflow attack
A. Layer 7
B. Layer 4
C. Layer 3
D. Layer 5
Answer: (SHOW ANSWER)

NEW QUESTION: 265
Which type of control minimizes the impact of an attack and restores normal operations as quickly as possible?
A. Compensatory control
B. Corrective control
C. Recovery control
D. Detective control
Answer: C (LEAVE A REPLY)
Recovery controls restore systems and data after an incident. Examples include backups, failover systems, and disaster recovery procedures.

NEW QUESTION: 266
What is the shortened form of
2001:0db8:0000:0000:0000:ffff:0000:0001?
A. 2001:db8::ffff:0:1
B. 2001:db8:0000:ffff:0:1
C. 2001:db80::ffff:0000:1
D. 2001:db8::ffff:0000:0001

Answer: A (LEAVE A REPLY)
IPv6 allows removal of leading zeros and compression of consecutive zero blocks using "::", making option A correct.

NEW QUESTION: 267
Which security control mostly used to prevent data breach
A. Logical Control
B. Physical control
C. Adminstrative Control
D. RBAC
Answer: (SHOW ANSWER)

NEW QUESTION: 268
The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats.
A. Principle of Least Privilege
B. Segregation of Duties
C. Privileged Account
D. Rule-based access control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 269
Which zero-trust component breaks LANs into very small, localized security zones?
A. Zero Trust
B. DMZ
C. VPN
D. Microsegmentation
Answer: D (LEAVE A REPLY)
Microsegmentationdivides networks into granular zones protected by internal firewalls or policy enforcement points. It limits lateral movement and is a core Zero Trust principle.

NEW QUESTION: 270
A company security team detected a cyber attack against it information systems and activates a set of procedures to mitigate the attack., What type of plan is this?
A. Incident response plan
B. Disaster recvoery plan
C. Business continuty plan
D. Security operation plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 271

Finance Server and Transaction Server have restored their original facility after a disaster. What should be moved in FIRST?

A. Management

B. Most critical systems

C. Most critical functions

D. Least critical functions

Answer: B (LEAVE A REPLY)

When restoring operations after a disaster,most critical systemsmust be restored first. Systems enable business functions, and without them, functions cannot operate.

Disaster recovery focuses on restoring IT infrastructure in priority order based on business impact analysis (BIA). While functions are important, they depend on systems to operate. Management and least critical functions are lower priorities.

NIST and ISO/IEC business continuity standards emphasize restoring mission-critical systems first to minimize downtime and financial loss.

NEW QUESTION: 272

Business continuity planning is a reactive procedure that restores business operations after a disruption occurs.

A. False

B. True

Answer: A (LEAVE A REPLY)

NEW QUESTION: 273

What does Personally Identifiable Information (PII) pertain to?

A. Information about an individual's health status

B. The importance assigned to information by its owner

C. Trade secrets, research, business plans and intellectual property

D. Data about an individual that could be used to identify them (Correct)

Answer: (SHOW ANSWER)

NEW QUESTION: 274

What is meant by non-repudiation?

A. If a user does something, they can't later claim that they didn't do it.

B. Controls to protect the organization's reputation from harm due to inappropriate social media postings by employees, even if on their private accounts and personal time.
C. It is part of the rules set by administrative controls.
D. It is a security feature that prevents session replay attacks.
Answer: A (LEAVE A REPLY)
Non-repudiation is a core security principle that ensures an individual or system cannot deny having performed a specific action. In cybersecurity, this concept is critical for accountability, auditing, and legal enforcement. Non-repudiation provides assurance that an action-such as sending an email, approving a transaction, or signing a document-can be definitively attributed to a specific user.
This principle is commonly enforced using cryptographic techniques such as digital signatures, public key infrastructure (PKI), hashing, and secure logging. For example, when a user digitally signs a document using their private key, anyone can later verify that signature using the corresponding public key. This prevents the signer from denying authorship.
Non-repudiation is particularly important in financial systems, legal documents, and regulated environments where proof of action is required. It differs from authentication, which verifies identity, and authorization, which defines permissions. Non-repudiation focuses on ensuring that actions are traceable and undeniable, supporting forensic investigations and compliance with security and legal requirements.

NEW QUESTION: 275
Load balancing primarily safeguards which CIA triad element?
A. Confidentiality
B. Availability
C. Integrity
D. All
Answer: B (LEAVE A REPLY)
Load balancing improves availability by distributing traffic across multiple systems, preventing overload and downtime.

NEW QUESTION: 276
When is the Business Continuity Plan Enacted?
A. When there is a loss of business operations
B. When there is a event
C. When there is a natural disaster
D. When there is a incident
Answer: A (LEAVE A REPLY)

NEW QUESTION: 277
What is the focus of disaster recovery planning after a data center outage?
A. Maintaining business functions
B. Fixing hardware
C. Restoring IT and communications

D. Emergency response guidance
Answer: (SHOW ANSWER)
Disaster Recovery Planning focuses on restoring IT infrastructure, systems, and communications after major disruptions.

NEW QUESTION: 278
A VLAN is a _____ method of segmenting networks.
A. Secret
B. Regulated
C. Physical
D. Logical
Answer: D (LEAVE A REPLY)

NEW QUESTION: 279
Why is an asset inventory so important?
A. It tells you what to encrypt
B. The law requires it
C. It contains a price list
D. You can't protect what you don't know you have
Answer: (SHOW ANSWER)
An accurate asset inventory is foundational to security. Without knowing what assets exist, organizations cannot secure, monitor, or protect them effectively.

NEW QUESTION: 280
The practice of sending fraudulent communications that appear to come from a reputable source
A. Phishing
B. Spoofing
C. Virus
D. DOS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 281
Which of the following is a characteristic of cloud
A. Broad Network Access
B. Measured Service
C. Rapid Elasticity
D. All
Answer: (SHOW ANSWER)

NEW QUESTION: 282
In what way do a victim's files get affected by ransomware?

A. By destroying them
B. By encrypting them
C. By stealing them
D. By selling them
Answer: (SHOW ANSWER)
Ransomware affects victims' files primarily byencryptingthem, rendering the data inaccessible without a decryption key. Attackers then demand a ransom in exchange for restoring access.
While modern ransomware may also steal data, encryption is the defining characteristic of ransomware attacks. Destroying or selling files is not the primary mechanism.
Strong backups, access controls, and endpoint protection are key defenses against ransomware, as emphasized by NIST and CIS.

NEW QUESTION: 283
An attacker outside the organization attempts to gain access to the organization's internal files. This is an example of a(n) _____.
A. Exploit
B. Publication
C. Intrusion
D. Disclosure
Answer: (SHOW ANSWER)

NEW QUESTION: 284
What is the end goal of DRP
A. DR site activated
B. Shifting the Infrastructure to new place
C. Business restored to full last-known reliable operations.
D. All System backup restored
Answer: C (LEAVE A REPLY)

NEW QUESTION: 285
A company network has been infected with malware and all its servers are down. What is the first step that the Disaster Recovery team should take to restore the systems?
A. Restore data from backup systems
B. Contact the enforcement to investigate the cyberattack
C. Conduct a risk assessment of determine the extent of the damage
D. Disconnect the affected systems from the network
Answer: D (LEAVE A REPLY)

NEW QUESTION: 286
An unusual occurrence in a system or network is best described as:
A. Breach

B. Exploit
C. Event
D. Intrusion
Answer: (SHOW ANSWER)
An event is any observable occurrence. Not all events are incidents or breaches, but incidents start as events.

NEW QUESTION: 287
Trina is a security practitioner at Triffid, Inc. Trina has been tasked with selecting a new product to serve as a security control in the environment. After doing some research, Trina selects a particular product. Before that product can be purchased, a manager must review Trina's selection and determine whether to approve the purchase. This is a description of:
A. Defense in depth
B. Two-person integrity
C. Software
D. Segregation of duties
Answer: D (LEAVE A REPLY)

NEW QUESTION: 288
IDS can be described in terms of what fundamental functional components?
A. Response
B. All of the choices.
C. Information Sources
D. Analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 289
Example of Type 1 authentication:
A. Password
B. Smart card
C. Fingerprint
D. RSA token
Answer: (SHOW ANSWER)

Type 1 authentication is "something you know," such as passwords or PINs. Other options represent possession-based or biometric authentication.

NEW QUESTION: 290
Which of the following attacks can TLS help mitigate?
A. Man-in-the-middle (MiTm) Attacks (Correct)
B. SQL Injection Attacks
C. Cross-site Scripting (XSS) Attacks
D. Social Engineering Attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
Which penetration testing technique requires the team to do the MOST work and effort?
A. Blue box
B. Black box
C. Gray box
D. White box
Answer: B (LEAVE A REPLY)

NEW QUESTION: 292
6 Which access control method uses attributes and rules to define access policies that are evaluate by a central Policy Decision Point (PDP)
A. DAC
B. MAC
C. RBAC
D. ABAC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 293
Which type of encryption uses only one shared key to encrypt and decrypt?
A. Public key
B. Symmetric
C. Asymmetric
D. TCB key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 294
In which of the following phases of an incident recovery plan the incident responses prioritized
A. Preparation
B. Post incident activity
C. Detection and analysis

D. Containment eradication and recovery
Answer: C (LEAVE A REPLY)

NEW QUESTION: 295
Requires that all instances of the data be identical in form,
A. Availability
B. Consistency
C. Confidentiality
D. ALL
Answer: (SHOW ANSWER)

NEW QUESTION: 296
A company needs to protect its confidential data from unauthorized access which logical control is best suited for this scenario
A. Hashing
B. Encryption
C. Antivirus
D. Firewall
Answer: B (LEAVE A REPLY)

NEW QUESTION: 297
What is the highest priority during incident response?
A. Protect mission
B. Reduce impact
C. Protect life, health, and safety
D. Resume operations
Answer: C (LEAVE A REPLY)
Human safety always takes precedence over systems, data, and business operations.

NEW QUESTION: 298
Which threat is directly associated with malware?
A. APT
B. Ransomware
C. Trojan
D. DDoS
Answer: C (LEAVE A REPLY)
ATrojanis a direct form of malware that disguises itself as legitimate software to perform malicious actions.

NEW QUESTION: 299
Which is the Not the component of a Business Continuity (BC) plan
A. Manacomont

B. Guidance for management, including designation of authority for specific managers
C. Immediate response procedures and checklists
D. Notification systems and call trees for alerting personnel
Answer: (SHOW ANSWER)

NEW QUESTION: 300
What federal law requires the use of vulnerability scanning on information systems operated by federal government agencies?
A. GLBA
B. FISMA
C. HIPAA
D. FERPA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 301
What is the most important goal of a business continuity effort?
A. Ensure all IT systems function during a potential interruption
B. Ensure the organization survives a disaster
C. Preserve health and human safety
D. Ensure all business activities are preserved during a potential disaster
Answer: (SHOW ANSWER)

NEW QUESTION: 302
The Triffid Corporation publishes a policy that states all personnel will act in a manner that protects health and human safety. The security office is tasked with writing a detailed set of processes on how employees should wear protective gear such as hardhats and gloves when in hazardous areas. This detailed set of processes is a _____.
A. Procedure
B. Policy
C. Law
D. Standard
Answer: A (LEAVE A REPLY)

NEW QUESTION: 303
What is the purpose of defense in depth in information security
A. To guarantee that a cyber attack will not occur
B. To Implement only technical controls to prevent a cyber attack
C. To establish variable barriers across multiple layers and mission of the organization
D. To provide unrestricted access to organization assets
Answer: (SHOW ANSWER)

NEW QUESTION: 304
What is the primary purpose of a firewall?
A. Encrypt data transmissions
B. Prevent unauthorized access
C. Monitor network traffic
D. Backup critical data
Answer: B (LEAVE A REPLY)
Firewalls control and filter network traffic based on security rules to prevent unauthorized access. While they may monitor traffic, their primary function is enforcing access control at network boundaries.

NEW QUESTION: 305
A set of instructions to detect, respond to, and recover from security incidents is a:
A. BCP
B. IRP
C. DRP
D. None
Answer: B (LEAVE A REPLY)
An Incident Response Plan (IRP) defines procedures for managing and mitigating security incidents.

NEW QUESTION: 306
A previously unknown vulnerability with no public listing is called:
A. Malware
B. Zero-day
C. Event
D. Attack
Answer: B (LEAVE A REPLY)
A zero-day vulnerability is unknown to the vendor and security community and has no available patch. Because defenders have "zero days" to fix it, zero-day vulnerabilities are highly dangerous.

NEW QUESTION: 307
An employee unintentionally shares confidential information with an unauthorized party. What term best describes this situation?
A. Event

B. Exploit
C. Breach
D. Intrusion
Answer: C (LEAVE A REPLY)

NEW QUESTION: 308
Using Mandatory Access Control (MAC), we would use clearance for assigning which of these?
Response:
A. Authentication.
B. Availability.
C. Authorization.
D. Auditing.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 309
Which security control is most commonly used to prevent data breaches?
A. Physical control
B. Logical control
C. Administrative control
D. RBAC
Answer: B (LEAVE A REPLY)
Logical (technical) controls such as encryption, access controls, DLP, and firewalls directly prevent unauthorized data access and exfiltration.

NEW QUESTION: 310
Which of the following is likely to be included in the business continuity plan?
A. Alternate work areas for personnel affected by a natural disaster
B. The organization's approach security approach
C. Log data from all systems
D. Last year's budget information
Answer: (SHOW ANSWER)

NEW QUESTION: 311
What does the term "Two-factor authentication" refer to in cybersecurity?
A. Using two different antivirus programs
B. Verifying identity with two independent factors
C. Accessing two different networks simultaneously
D. Changing passwords every two weeks
Answer: (SHOW ANSWER)
Two-factor authentication (2FA) requires users to verify their identity usingtwo independent authentication factorsfrom different categories, such as something you know and something you have.

The purpose of 2FA is to strengthen authentication security and reduce the risk of unauthorized access. Even if one factor is compromised, the attacker cannot authenticate without the second factor.
2FA is a subset of multi-factor authentication and is strongly recommended by modern security standards, particularly for remote access, cloud services, and privileged accounts.

NEW QUESTION: 312
What does the termbusinessin business continuity planning refer to?
A. The financial performance of the organization
B. The technical systems of the organization
C. The operational aspects of the organization
D. The physical infrastructure of the organization
Answer: (SHOW ANSWER)
In Business Continuity Planning (BCP), the termbusinessrefers primarily to theoperational aspects of the organization-the people, processes, and activities required to deliver products and services. While IT systems, finances, and facilities support operations, BCP focuses on ensuring thatcritical business functions continueduring and after disruptions.
This includes customer service, supply chain operations, payroll, compliance activities, and decision-making processes. BCP is broader than disaster recovery, which focuses mainly on restoring IT systems. According to NIST SP 800-34, business continuity emphasizes mission-essential functions and their dependencies, including personnel, third parties, facilities, and technology.

NEW QUESTION: 313
Faking the sender address in a transmission to gain illegal entry into a secure system
A. Phishing
B. ALL
C. Spoofing
D. ARP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 314
A company wants employees to access resources from anywhere in the world. Which access control model is best?
A. DAC
B. RBAC
C. MAC
D. ABAC
Answer: D (LEAVE A REPLY)
ABAC supports dynamic, context-aware access decisions based on attributes such as location, device, and time-ideal for global access scenarios.

NEW QUESTION: 315

A large organization is planning to create a DRP. Which of the following is the BEST document to provide a high-level overview of the plan?
A. Technical guides for IT personnel
B. Department specific plans
C. Execute summary
D. Full copies of the plan for critical disaster recovery team members
Answer: C (LEAVE A REPLY)

NEW QUESTION: 316
Firewalls operate at which OSI layers?
A. Layer 3
B. Layer 4
C. Layer 7
D. All
Answer: D (LEAVE A REPLY)
Modern firewalls operate at Layers 3, 4, and 7, supporting packet filtering, stateful inspection, and application-layer filtering.

NEW QUESTION: 317
A DDoS attack affects which OSI layers?
A. Network layer
B. Transport layer
C. Physical layer
D. Both A and B
Answer: D (LEAVE A REPLY)
DDoS attacks can target bothLayer 3 (Network)andLayer 4 (Transport)by overwhelming IP routing, ICMP traffic, TCP SYN floods, or UDP floods. Hence, both layers are impacted.

NEW QUESTION: 318
Scans networks to determine everything that is connected as well as other information.
A. Wireshark
B. Burbsuite
C. Zen Mao

D. Fiddler
Answer: C (LEAVE A REPLY)

NEW QUESTION: 319
The harmonization of automated computing tasks, providing a consolidated and reusable workflow
A. Cloud Controller
B. Cloud Manager
C. Cloud Orchestration
D. Cloud broker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 320
Mark has purchased a MAC LAPTOP. He is scared of losing his screen and planning to buy an insurance policy. So, which risk management strategy is?
A. Risk transference
B. Risk acceptance
C. Risk deterrence
D. Risk mitigation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 321
What is a security token used to authenticate a user to a web application, typically after they log in?
A. CAPTCHA
B. API key
C. CSRF token
D. Session token
Answer: D (LEAVE A REPLY)
A session token is used to maintain a user's authenticated state after login. Once a user successfully authenticates, the server issues a session token that is stored by the client and sent with subsequent requests. The server uses this token to identify the user without requiring reauthentication on every request. Session tokens must be protected against theft through secure cookies, encryption, and proper expiration.
CAPTCHAs prevent automated abuse, API keys authenticate applications, and CSRF tokens prevent request forgery. Only session tokens authenticate users across requests.
Proper session management is critical for web application security and is emphasized in OWASP and NIST guidance.

NEW QUESTION: 322
Which layer provides the services to user?
A. Physical Layer
B. Presentation Layer
C. Application layers

D. Session Layers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 323
Uses multiple types of access controls in layered fashion to avoid monolithic security:
A. DMZ
B. VLAN
C. Defense in Depth
D. VPN
Answer: (SHOW ANSWER)
Defense in Depth employs administrative, technical, and physical controls across multiple layers to reduce reliance on any single security mechanism. This approach increases resilience and detection capability.

NEW QUESTION: 324
System capabilities designed to detect and prevent the unauthorized use and transmission of information.
A. Crytography
B. Data Loss Prevention
C. SOC
D. SIEM solutions
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation
A. EMI Shielding
B. ALL
C. Screening rooms
D. White noise generators
Answer: (SHOW ANSWER)

NEW QUESTION: 326
When an attacker is using a brute force attack to break a password, what are they doing?
Response:
A. Looking at the hash values and comparing it to thousands or millions of pre-calculated hashes.
B. Trying every possible key to, over time, break any encryption.
C. Trying to recover the key without breaking the encryption.
D. Looking at common letter frequency to guess the plaintext.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 327

Olaf is a member of (ISC)² and a security analyst for Triffid Corporation. During an audit, Olaf is asked whether Triffid is currently following a particular security practice. Olaf knows that Triffid is not adhering to that standard in that particular situation, but that saying this to the auditors will reflect poorly on Triffid. What should Olaf do?

A. Lie to the auditors

B. Tell the auditors the truth

C. Ask (ISC)2 for guidance

D. Ask supervisors for guidance

Answer: D (LEAVE A REPLY)

NEW QUESTION: 328

Which is related to Standard

A. ALL

B. NIST

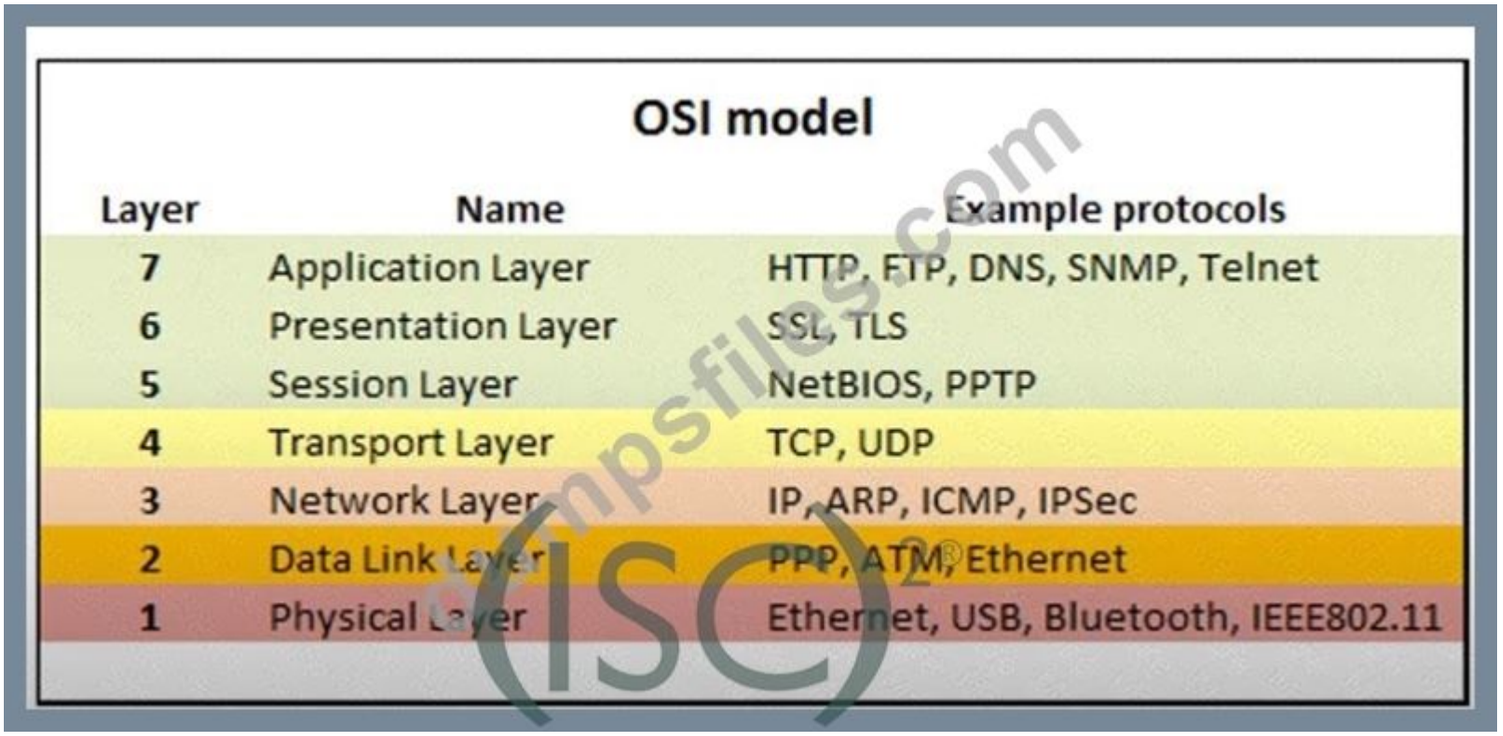
C. HIPAA

D. GDPR

Answer: (SHOW ANSWER)

NEW QUESTION: 329

Exhibit.



IPSec works in which layer of OSI Model

A. Layer 3

B. Layer 2

C. Layer 5

D. Layer 7

Answer: A (LEAVE A REPLY)

NEW QUESTION: 330
For which of the following systems would the security concept of availability probably be most important?
A. Online streaming of camera feeds that display historical works of art in museums around the world.
B. Retail records of past transactions
C. Medical systems that store patient data
D. Medical systems that monitor patient condition in an intensive care unit
Answer: (SHOW ANSWER)

NEW QUESTION: 331
Shaun is planning to protect data in all states (at rest, in motion, and in use), defending against data leakage. What is the BEST solution to implement?
A. End-to-end encryption
B. Hashing
C. DLP
D. Threat modeling
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) is designed to protect sensitive data across all states: at rest, in motion, and in use. DLP solutions monitor, detect, and prevent unauthorized access, sharing, or exfiltration of data.
While encryption protects data at rest and in transit, it does not prevent authorized users from misusing data. Hashing ensures integrity, not confidentiality. Threat modeling identifies risks but does not enforce protection.
DLP tools enforce policies, inspect content, and prevent data leakage through email, web uploads, removable media, and cloud services. They are especially valuable for protecting regulated data such as PII and financial records.
NIST and CIS recognize DLP as a critical control for comprehensive data protection strategies.

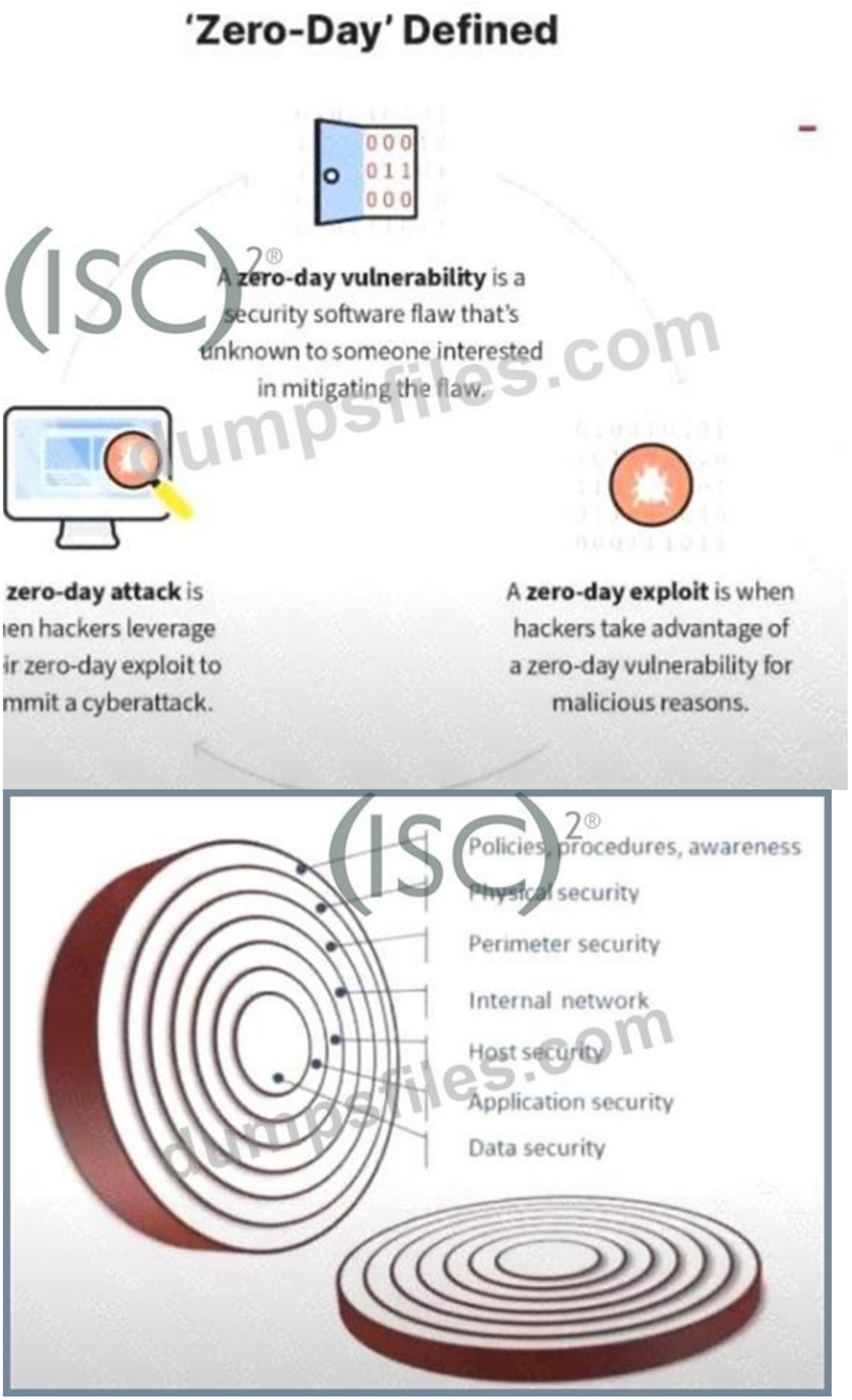
NEW QUESTION: 332
What is the access control model being implemented in Tekila's agency?
A. Discretionary access control (DAC)
B. Role-based access control (RBAC)
C. Formal access control (FAC)
D. Mandatory access control (MAC)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 333
What is the range of private (dynamic/ephemeral) ports?
A. None
B. 0 - 1023
C. 49152 - 65535
D. 1023 - 49151
Answer: C (LEAVE A REPLY)
Private or ephemeral ports (49152-65535) are dynamically assigned to client applications for temporary communication sessions.

NEW QUESTION: 334
What is the potential impact of an IPSec replay attack?
A. Modification of network traffic
B. Disruption of network communication
C. Unauthorized access to network resources
D. All
Answer: B (LEAVE A REPLY)
Replay attacks disrupt communication by resending captured packets, potentially causing session confusion or denial of service. IPSec mitigates this using sequence numbers.

NEW QUESTION: 335
Exhibit.



What kind of vulnerability is typically not identifiable through a standard vulnerability assessment?

A. File permissions
B. Cross-site scripting
C. Zero-day vulnerability
D. Buffer overflow
Answer: C (LEAVE A REPLY)

NEW QUESTION: 336
An analysis of system requirements and interdependencies used to prioritize recovery is known as:
A. BIA
B. DR
C. BCP
D. IRP
Answer: (SHOW ANSWER)
A Business Impact Analysis (BIA) identifies critical systems, dependencies, and acceptable downtime. It is foundational to both BCP and DRP development.

NEW QUESTION: 337
What is the primary goal of an incident management team?
A. Reduce impact and restore services
B. Gathering and analyzing information
C. Conducting lessons learned meetings
D. Root cause analysis
Answer: A (LEAVE A REPLY)
The primary objective of incident management is to minimize business impact and restore normal operations as quickly as possible. Analysis and lessons learned occur later in the lifecycle.

NEW QUESTION: 338
System capabilities designed to detect and prevent unauthorized use and transmission of information are known as:
A. SOC
B. SIEM solutions
C. Data Loss Prevention
D. Cryptography
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP)systems monitor, detect, and block unauthorized data exfiltration across endpoints, networks, and cloud services.

NEW QUESTION: 339
One of the benefits of computer-based training (CBT):
A. Expensive
B. Scalable

C. Personal interaction with instructor
D. Interacting with other participants
Answer: B (LEAVE A REPLY)

NEW QUESTION: 340
The primary functionality of Privileged Access Management (PAM) is:
A. Validate access to a file
B. Prevent unauthorized access to assets
C. Provide just-in-time access to critical resources
D. Manage centralized access control
Answer: C (LEAVE A REPLY)
PAM solutions focus onjust-in-time (JIT) access, granting elevated privileges only when needed and revoking them afterward. This reduces standing privileges and minimizes attack surfaces.

NEW QUESTION: 341
The right of an individual to control the distribution of information about themselves is:
A. Confidentiality
B. Integrity
C. Privacy
D. Availability
Answer: (SHOW ANSWER)
Privacy focuses on individual rights over personal information, distinct from confidentiality which focuses on access control.

NEW QUESTION: 342
Devid's team recently implemented a new system that gathers information from a variety of different log sources, analyses that information, and then triggers automated playbooks in response to security events, what term BEST describes this technology?
A. SIEM
B. Log Repository
C. SOAR
D. IPS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 343
In the context of cybersecurity, typical threat actors include the following:
A. Technology (such as free-running bots and artificial intelligence
B. All
C. Insiders (either deliberately, by simple human error, or by gross incompetence).
D. Outside individuals or informal groups (either planned or opportunistic, discovering vulnerability).
Answer: B (LEAVE A REPLY)