ISC.CC.v2026-07-17.q172

Exam Code:	CC
Exam Name:	Certified in Cybersecurity (CC)
Certification Provider:	ISC
Free Question Number:	172
Version:	v2026-07-17
# of views:	108
# of Questions views:	1865
https://www.freecram.net/torrent/ISC.CC.v2026-07-17.q172.html	

NEW QUESTION: 1
Which threat is directly associated with malware?
A. APT
B. Ransomware
C. Trojan
D. DDoS
Answer: (SHOW ANSWER)
ATrojanis a direct form of malware that disguises itself as legitimate software to perform malicious actions.

NEW QUESTION: 2
Load balancing primarily safeguards which CIA triad element?
A. Confidentiality
B. Availability
C. Integrity
D. All
Answer: (SHOW ANSWER)
Load balancing improves availability by distributing traffic across multiple systems, preventing overload and downtime.

NEW QUESTION: 3
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: 4
Which scenario best represents defense in depth?
A. Relying only on a firewall
B. Storing all data on one server
C. Requiring only a username and password
D. None
Answer: (SHOW ANSWER)
Defense in depth requiresmultiple layers of security controls. None of the listed scenarios include layered controls, making "None" the correct answer.

NEW QUESTION: 5
Who should participate in creating a Business Continuity Plan?
A. Management only
B. IT only
C. Finance only
D. Members across the organization
Answer: (SHOW ANSWER)
BCP requires cross-functional participation to identify dependencies, workflows, and recovery priorities across all departments.

NEW QUESTION: 6
Communication between end systems is encrypted using a key, often known as _____?
A. Temporary key
B. Section key
C. Public key
D. Session key
Answer: (SHOW ANSWER)
A session key is a temporary cryptographic key used to encrypt communication between two systems for a single session. Session keys are typically symmetric keys generated during secure key exchange processes such as TLS handshakes.
They provide confidentiality and efficiency because symmetric encryption is much faster than asymmetric encryption. Once the session ends, the key is discarded, limiting exposure even if the key is later compromised.

Public keys are used for key exchange and authentication, not bulk data encryption. "Temporary key" and
"section key" are not standard cryptographic terms.
Session keys are fundamental to secure network communications and are recommended by all modern cryptographic standards due to their performance and security benefits.

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: C (LEAVE A REPLY)
Risk Avoidanceeliminates risk by discontinuing activities that expose the organization to unacceptable threats.

NEW QUESTION: 8
A company network experiences a sudden flood of network packets that causes major slowdown in Internet traffic. What type of event is this?
A. Security incident
B. Natural disaster
C. Exploit
D. Adverse event
Answer: (SHOW ANSWER)
A sudden flood of network packets causing degraded performance is best classified as anadverse event. An adverse event is any occurrence that negatively affects system performance, availability, or operations but may not yet meet the threshold of a confirmed security incident. According to NIST definitions, events such as traffic spikes, system slowdowns, or anomalous behavior are initially treated as adverse events until further analysis confirms malicious intent.
If investigation later confirms the flood was caused by a deliberate denial-of-service attack, the classification may escalate to asecurity incident. However, without confirmation of intent or compromise, adverse event is the most accurate term.

NEW QUESTION: 9
The method of distributing network traffic equally across a pool of resources is called:
A. VLAN
B. DNS
C. VPN
D. Load balancing
Answer: (SHOW ANSWER)

Load balancing distributes incoming traffic across multiple servers or resources to improve performance, scalability, and availability. It prevents overload of a single system and supports high availability architectures.

NEW QUESTION: 10

Which is related to standards?

A. NIST

B. GDPR

C. HIPAA

D. All

Answer: (SHOW ANSWER)

NIST publishes standards and frameworks. GDPR and HIPAA are regulations and laws, not standards bodies.

NEW QUESTION: 11

Which type of attack takes advantage of vulnerabilities in validation?

A. ARP spoofing

B. Pharming attacks

C. Cross-site scripting (XSS)

D. DNS poisoning

Answer: (SHOW ANSWER)

Cross-site scripting (XSS) attacks exploitinput validation vulnerabilitiesin web applications. These vulnerabilities occur when an application fails to properly validate, sanitize, or encode user-supplied input before including it in web pages. As a result, attackers can inject malicious scripts that are executed in the browsers of other users.

XSS attacks commonly occur through form fields, URL parameters, cookies, or HTTP headers. Once executed, malicious scripts can steal session cookies, capture keystrokes, redirect users to malicious sites, or perform actions on behalf of the victim.

ARP spoofing and DNS poisoning target network-level trust relationships, not application input validation.

Pharming redirects users to fake websites by manipulating DNS or host files, again unrelated to input validation.

Preventing XSS relies heavily on strong input validation, output encoding, content security policies (CSP), and secure coding practices. OWASP and NIST explicitly identify XSS as a validation-related vulnerability and emphasize defensive coding as the primary mitigation.

NEW QUESTION: 12

Scans networks to determine connected devices and services:

A. Burp Suite

B. Wireshark

C. Fiddler

D. Zenmap
Answer: (SHOW ANSWER)
Zenmap is the graphical front end for Nmap. It performs host discovery, port scanning, service enumeration, and OS fingerprinting.

NEW QUESTION: 13
What is the focus of disaster recovery planning after a data center failure?
A. Maintain business functions
B. Fix hardware
C. Restore IT and communications
D. Guide emergency responders
Answer: C (LEAVE A REPLY)
DRP focuses on restoring IT infrastructure, applications, and communications to operational status.

NEW QUESTION: 14
An entity that exploits system vulnerabilities is known as a:
A. Attacker
B. Threat vector
C. Threat
D. Threat actor
Answer: (SHOW ANSWER)
A threat actor is the individual or group responsible for carrying out attacks. Threat vectors describe methods, not entities.

NEW QUESTION: 15
Who must follow HIPAA compliance?
A. Energy sector
B. Health care
C. Finance sector
D. All
Answer: (SHOW ANSWER)
HIPAA applies to healthcare providers, insurers, and their business associates to protect patient health information (PHI).

NEW QUESTION: 16
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: (SHOW ANSWER)

A user ID provides identification-it claims an identity. Authentication verifies that claim using credentials like a password.

NEW QUESTION: 17
Which is the first step in the risk management process?
A. Risk response
B. Risk mitigation
C. Risk identification
D. Risk assessment
Answer: (SHOW ANSWER)
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: 18
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: 19
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: 20
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: (SHOW ANSWER)
The ISC2 Code of Ethics requires members to act lawfully and ethically. Accepting pirated material violates this obligation.

NEW QUESTION: 21
Which is a component of a Business Continuity (BC) plan?
A. Immediate response procedures
B. Notification systems and call trees
C. Management authority guidance
D. All
Answer: (SHOW ANSWER)
A complete BCP includes response procedures, communication plans, and management authority to ensure coordinated recovery.

NEW QUESTION: 22
A hacker launches a specific attack to exploit a known vulnerability. This is called:
A. Breach
B. Event
C. Exploit
D. Intrusion
Answer: (SHOW ANSWER)
An exploit is the method or code used to take advantage of a known vulnerability. Successful exploitation may result in an intrusion or breach.

NEW QUESTION: 23
Which one of the following cryptographic algorithms does NOT depend upon the prime factorization problem?

A. RSA - Rivest-Shamir-Adleman
B. GPG - GNU Privacy Guard
C. ECC - Elliptic Curve Cryptosystem
D. PGP - Pretty Good Privacy
Answer: (SHOW ANSWER)
Elliptic Curve Cryptography (ECC) does not rely on the prime factorization problem. Instead, ECC is based on the mathematical difficulty of solving elliptic curve discrete logarithm problems.
RSA relies directly on the difficulty of factoring large prime numbers. GPG and PGP are encryption tools and standards that may use RSA or other algorithms internally.
ECC provides equivalent security with much smaller key sizes, making it efficient for mobile devices, embedded systems, and environments with limited processing power.
Modern security standards increasingly recommend ECC due to its performance and strong security properties.

NEW QUESTION: 24
A company wants to prevent employees from bringing unauthorized electronic devices into the workspace.
Which physical control is best?
A. Metal detectors
B. Security guards
C. RFID scanners
D. Baggage X-ray machines
Answer: (SHOW ANSWER)
Metal detectors are effectivepreventive physical controlsthat detect electronic devices and storage media.
They are commonly used in high-security environments to enforce device restrictions.

NEW QUESTION: 25
What cybersecurity principle focuses on granting users only the privileges necessary to perform their job functions?
A. Least privilege
B. Defense in depth
C. Separation of duties
D. Need-to-know basis
Answer: (SHOW ANSWER)
The principle of least privilege ensures users have only the minimum permissions necessary to perform their tasks. This limits damage from compromised accounts and insider threats.
It is foundational to access control, IAM, and zero trust architectures and is recommended by all major security frameworks.

NEW QUESTION: 26

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: 27
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: (SHOW ANSWER)
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: 28
Which layer provides services directly to the user?
A. Application Layer
B. Session Layer
C. Presentation Layer
D. Physical Layer

Answer: A (LEAVE A REPLY)

TheApplication Layer (Layer 7)of the OSI model provides services directly to the user and user-facing applications. This layer supports protocols such as HTTP, HTTPS, SMTP, FTP, and DNS, which enable web browsing, email, file transfers, and name resolution.

While users interact with applications rather than the OSI model itself, the Application Layer is responsible for enabling those interactions. The Session Layer manages session establishment, the Presentation Layer handles data formatting and encryption, and the Physical Layer transmits raw bits over physical media.

From a security perspective, many attacks target the Application Layer, including SQL injection, cross-site scripting (XSS), and authentication bypasses. As a result, application-layer security controls such as WAFs, secure coding practices, and input validation are critical.

Understanding OSI layers helps security professionals design layered defenses and properly place controls.

NEW QUESTION: 29

Which phase of the access control process (AAA) does a user prove his/her identity?

A. Authentication

B. Authorization

C. Identification

D. Accounting

Answer: A (LEAVE A REPLY)

Authentication is the phase of the AAA (Authentication, Authorization, Accounting) model in which a user proves their identity. During authentication, the system verifies that the user is who they claim to be by validating credentials such as passwords, biometrics, smart cards, or cryptographic keys.

Identification occurs first, when a user claims an identity (for example, entering a username). Authentication then confirms that claim. Authorization follows authentication and determines what actions the authenticated user is permitted to perform. Accounting tracks and logs user activities for auditing and monitoring purposes.

Strong authentication is critical to system security because all subsequent access control decisions depend on its accuracy. Weak authentication mechanisms increase the risk of unauthorized access, credential theft, and impersonation attacks.

Modern security frameworks emphasize multi-factor authentication (MFA) to strengthen this phase.

NIST SP

800-63 highlights authentication as a core security function essential to protecting systems, data, and services from unauthorized access.

NEW QUESTION: 30

Removing the belief that a network has any trusted space and enforcing security at the most granular level is known as:

A. Zero Trust

B. Defense in Depth

C. Least Privilege
D. All
Answer: (SHOW ANSWER)
Zero Trust assumes no implicit trust and requires continuous verification of every access request. Microsegmentation is a core Zero Trust technique that limits lateral movement.

NEW QUESTION: 31
Which type of risk involves unauthorized use or disclosure of confidential information such as passwords, financial data, or personal information?
A. Compliance risk
B. Reputational risk
C. Operational risk
D. Information risk
Answer: (SHOW ANSWER)
Information riskrefers to the potential harm arising from the unauthorized access, disclosure, modification, or destruction of sensitive information. This includes credentials, financial records, intellectual property, and personally identifiable information (PII).
Information risk directly impacts theconfidentiality, integrity, and availability (CIA triad)of data. While such incidents may also lead to reputational damage or compliance violations, the primary category describing the exposure of sensitive data itself is information risk.
NIST SP 800-30 emphasizes information risk as a core component of enterprise risk management, especially in organizations that rely heavily on digital data for operations and decision-making.

NEW QUESTION: 32
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: (SHOW ANSWER)
Internal consistency ensures that all copies of data remain identical in content and meaning.

NEW QUESTION: 33

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

NEW QUESTION: 34
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: (SHOW ANSWER)
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: 35
A type of malware capable of self-propagation and infecting multiple systems without human intervention is called:
A. Worm
B. Spyware
C. Adware
D. Virus
Answer: (SHOW ANSWER)
Worms are self-propagating malware that spread automatically across networks by exploiting vulnerabilities.
Unlike viruses, worms do not require user interaction.

NEW QUESTION: 36
Which uses encrypted, machine-generated codes to verify a user's identity?
A. Basic authentication
B. Form-based authentication
C. Token-based authentication
D. All
Answer: (SHOW ANSWER)

Token-based authentication relies on encrypted, machine-generated tokens to verify a user's identity. After successful authentication, the system issues a token (often a JSON Web Token or OAuth token) that represents the user's session or authorization claims. This token is then presented with each request instead of repeatedly transmitting credentials.
Unlike basic or form-based authentication, token-based methods reduce exposure of usernames and passwords, improve scalability, and support modern distributed architectures such as APIs, cloud services, and mobile applications. Tokens can also include expiration times and scopes, improving security control.

NEW QUESTION: 37
A backup is which type of security control?
A. Preventive
B. Deterrent
C. Recovery
D. Corrective
Answer: (SHOW ANSWER)
Backups are recovery controls because they restore data and systems after failures, attacks, or disasters.

NEW QUESTION: 38
What doescriticalityrepresent?
A. Consultation needs
B. The importance of data or systems to mission success
C. Availability requirements
D. All of the above
Answer: (SHOW ANSWER)
Criticality reflects how essential an asset is to business operations or mission success. It influences prioritization, recovery planning, and protection strategies.

NEW QUESTION: 39
The first phase of the System Development Life Cycle (SDLC) is:
A. Requirements analysis
B. Feasibility study
C. Design
D. Development
Answer: (SHOW ANSWER)
The feasibility study determines whether a project is technically, economically, and operationally viable before development begins.

NEW QUESTION: 40
Why is the recovery of IT often crucial to the recovery and sustainment of business operations?

A. IT is not important to business operations
B. IT is often the cause of disasters
C. IT can be easily recovered without impact
D. Many businesses rely heavily on IT for operations
Answer: (SHOW ANSWER)
Modern organizations depend on IT systems for communication, data processing, transactions, and service delivery. Without IT, critical business functions often cannot operate, making IT recovery essential to business continuity.

NEW QUESTION: 41
What security feature is used in HTTPS?
A. IPSec
B. SSH
C. ICMP
D. SSL/TLS
Answer: (SHOW ANSWER)
HTTPS uses SSL/TLS to provide encryption, authentication, and integrity for web communications.

NEW QUESTION: 42
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: (SHOW ANSWER)
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: 43
What kind of control is it when we add a backup firewall that takes over if the main one stops working?
A. Clustering
B. High availability (HA)
C. Load balancing
D. Component redundancy
Answer: (SHOW ANSWER)

High availability (HA) refers to system designs that ensure continuous operation by minimizing downtime in the event of component failures. Adding a backup firewall that automatically takes over when the primary firewall fails is a classic example of high availability.
HA solutions often use failover mechanisms, heartbeat monitoring, and redundancy to ensure seamless service continuity. The goal is to maintain availability, which is a core pillar of the CIA triad.
Component redundancy describes duplicated parts, but high availability focuses on the operational outcome- continued service. Load balancing distributes traffic, not failover. Clustering involves multiple systems working together, but HA specifically emphasizes fault tolerance and uptime.
High availability is critical for security infrastructure such as firewalls, authentication servers, and monitoring tools. NIST and ISO frameworks stress HA as essential for business continuity, disaster recovery, and resilient security operations.

NEW QUESTION: 44
Which element of the security policy framework includes recommendations that are NOT binding?
A. Procedures
B. Guidelines
C. Standards
D. Policies
Answer: (SHOW ANSWER)
Guidelines are non-binding recommendations within a security policy framework. They provide best practices, suggestions, and advice to help users and administrators make informed decisions, but they do not require mandatory compliance.
Policies are high-level, mandatory statements approved by senior management. Standards define specific, mandatory requirements that must be followed to comply with policies. Procedures provide step-by-step instructions for implementing policies and standards.
Guidelines offer flexibility and allow organizations to adapt recommendations to different environments, technologies, or risk levels. Because they are not enforceable, guidelines are often used to encourage secure behavior without imposing strict controls.
For example, a guideline might recommend using a password manager, while a standard would require minimum password length. Security frameworks such as ISO/IEC 27001 and NIST distinguish clearly between mandatory controls and advisory guidance to balance security with operational flexibility.

NEW QUESTION: 45
Which access control method uses attributes and rules evaluated by a central Policy Decision Point (PDP)?
A. DAC
B. RBAC
C. MAC
D. ABAC

Answer: (SHOW ANSWER)
ABAC uses centralized policy engines (PDPs) to evaluate attributes and enforce fine-grained access control decisions dynamically.

NEW QUESTION: 46
A method for risk analysis that is based on the assignment of a descriptor such as low, medium, or high.
A. Quantitative Risk Analysis
B. Risk Assessment
C. Risk Mitigation
D. Qualitative Risk Analysis
Answer: (SHOW ANSWER)
Qualitative risk analysis evaluates risk using descriptive categories such aslow,medium, andhighinstead of numerical values. This approach relies on expert judgment, experience, and contextual understanding rather than precise financial or statistical calculations. According to NIST SP 800-30, qualitative analysis is especially useful when numerical data is unavailable or when rapid risk prioritization is required.
Unlike quantitative risk analysis, which assigns monetary values and probabilities, qualitative analysis focuses on relative severity and likelihood. It is commonly used during early stages of risk management, policy development, and executive decision-making. While less precise, qualitative risk analysis is easier to communicate to stakeholders and helps organizations focus resources on the most critical risks.

NEW QUESTION: 47
Which document identifies the principles and rules governing an organization's protection of information systems and data?
A. Procedure
B. Guideline
C. Policy
D. Standard
Answer: (SHOW ANSWER)

Security policies are high-level, mandatory statements approved by management that define security objectives, principles, and rules. Procedures and standards support policies but do not establish overarching intent.

NEW QUESTION: 48
The means by which a threat actor carries out their objectives.
A. Threat
B. Threat Vector
C. Exploit
D. Intrusion
Answer: (SHOW ANSWER)
Athreat vectoris the path or method used by a threat actor to exploit vulnerabilities, such as phishing, malware, or network attacks.

NEW QUESTION: 49
Which IR phase involves identifying critical data and systems?
A. Detection and analysis
B. Preparation
C. Containment
D. Eradication
Answer: (SHOW ANSWER)
Preparation includes asset identification, system classification, and readiness planning.

NEW QUESTION: 50
Which regulation addresses personal privacy?
A. HIPAA
B. GDPR
C. NIST
D. ISO
Answer: (SHOW ANSWER)
GDPR is a privacy regulation governing the protection of personal data for individuals in the EU.

NEW QUESTION: 51
Information should be consistently and readily accessible for authorized parties.
A. Confidentiality
B. Authentication
C. Availability
D. Non-repudiation
Answer: (SHOW ANSWER)
Availabilityensures that authorized users can access information and systems when needed, a core element of the CIA triad.

NEW QUESTION: 52
A measure of the degree to which an organization depends on information or systems to achieve its mission is called:
A. Availability
B. Criticality
C. Authorization
D. Confidentiality
Answer: (SHOW ANSWER)
Criticality reflects how essential an asset or system is to business success or mission accomplishment. It is commonly determined during a Business Impact Analysis (BIA) and influences recovery priorities.

NEW QUESTION: 53
Malware that disguises itself as legitimate software is called:
A. Worm
B. Trojan
C. Virus
D. Ransomware
Answer: (SHOW ANSWER)
ATrojandeceives users into executing it by appearing legitimate while performing malicious actions.

NEW QUESTION: 54
An event that jeopardizes confidentiality, integrity, or availability is called:
A. Breach
B. Event
C. Incident
D. Exploit
Answer: C (LEAVE A REPLY)
A security incident is an event that threatens or violates CIA principles. Not all incidents result in breaches.

NEW QUESTION: 55
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: (SHOW ANSWER)

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: 56
The common term for systems that control temperature and humidity in a data center is:
A. VLAN
B. STAT
C. TAWC
D. HVAC
Answer: (SHOW ANSWER)
HVAC (Heating, Ventilation, and Air Conditioning)systems regulate temperature, humidity, and airflow in data centers. Proper environmental controls are critical to prevent equipment failure and ensure system reliability.

NEW QUESTION: 57
Which of the following is a characteristic of cloud computing?
A. Broad network access
B. Rapid elasticity
C. Measured service
D. All
Answer: (SHOW ANSWER)
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: 58
Which access control model grants permissions based ondata sensitivityanduser job functions?
A. DAC
B. RBAC
C. MAC
D. RuBAC
Answer: (SHOW ANSWER)
Mandatory Access Control (MAC) usesdata classification (sensitivity)anduser clearances, which are often tied to job roles. Access decisions are centrally enforced and cannot be changed by users or data owners.

NEW QUESTION: 59
Which access control model can grant access to a given object based on complex rules?
A. ABAC
B. DAC
C. MAC

D. RBAC

Answer: (SHOW ANSWER)

Attribute-Based Access Control (ABAC) grants access based on complex logical rules that evaluate attributes of the user, resource, action, and environment. Examples include user role, department, time of day, device type, and data sensitivity. These attributes are evaluated dynamically, allowing fine-grained and context- aware access decisions.

DAC allows owners to grant permissions, MAC uses labels and classifications, and RBAC assigns permissions based on roles. None of these provide the same level of flexibility as ABAC. Because ABAC supports complex, rule-based decisions, it is widely used in modern cloud environments and zero trust architectures.

NEW QUESTION: 60

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: (SHOW ANSWER)

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: 61

Representation of data at OSI Layer 3 is called a:

A. Segment

B. Packet

C. Frame

D. None of the above

Answer: (SHOW ANSWER)

At Layer 3 (Network Layer), data is encapsulated intopacketsfor routing across networks.

NEW QUESTION: 62
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: (SHOW ANSWER)
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: 63
An unknown person obtains unauthorized access to the company file system. This is an example of:
A. Intrusion
B. Breach
C. Exploit
D. Incident
Answer: (SHOW ANSWER)
Unauthorized access that compromises confidentiality constitutes abreach. Intrusions become breaches when access is successful.

NEW QUESTION: 64
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: 65
Difference between sniffing and spoofing:
A. Sniffing intercepts traffic; spoofing disguises identity
B. Snooping intercepts traffic; sniffing disguises identity
C. Both are the same
D. Sniffing is not a threat
Answer: (SHOW ANSWER)

Sniffing captures network traffic, while spoofing impersonates trusted sources.

NEW QUESTION: 66
Created by switches to logically segment a network without changing physical topology:
A. LAN
B. WAN
C. VLAN
D. MAN
Answer: C (LEAVE A REPLY)
VLANslogically separate networks at Layer 2 while sharing the same physical infrastructure.

NEW QUESTION: 67
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: 68
XenServer, LVM, Hyper-V, and ESXi are:
A. Type 2 hypervisors
B. Type 1 hypervisors
C. Both
D. None
Answer: B (LEAVE A REPLY)
These areType 1 (bare-metal) hypervisors, running directly on hardware without a host operating system, offering higher performance and security.

NEW QUESTION: 69
What is the most important aspect of security awareness and training?
A. Maximizing business capabilities
B. Protecting assets
C. Protecting health and human safety
D. Ensuring confidentiality of data

Answer: (SHOW ANSWER)
Human life and safety always take precedence over systems, data, and business operations. Security awareness ensures employees know how to act safely during incidents such as fires, active threats, or infrastructure failures.

NEW QUESTION: 70
Which activity is often associated with Disaster Recovery efforts?
A. Running anti-malware
B. Vulnerability scanning
C. Zero-day exploits
D. Employees returning to the primary production location
Answer: (SHOW ANSWER)
Disaster Recovery includes restoring systems and returning operations to normal, which may involve staff moving back to the primary site after temporary relocation.

NEW QUESTION: 71
A curated knowledge base modeling adversary behavior across attack phases is:
A. MITRE ATTandCK
B. CVE
C. RMF
D. Security Management
Answer: (SHOW ANSWER)
MITRE ATTandCK maps adversary tactics, techniques, and procedures (TTPs) across the attack lifecycle.

NEW QUESTION: 72
Which prevents threats?
A. Antivirus
B. IDS
C. SIEM
D. HIDS
Answer: (SHOW ANSWER)
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: 73
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: (SHOW ANSWER)
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: 74
How do IT professionals differentiate between IT problems and security incidents?
A. Medical assistance
B. Evidence collection only
C. Specialized incident response training
D. Lessons learned participation
Answer: (SHOW ANSWER)
Incident response training enables professionals to recognize malicious activity versus routine IT failures and respond appropriately.

NEW QUESTION: 75
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: 76
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: 77
A way to prevent unwanted devices from connecting to a network is:
A. DMZ
B. VPN
C. VLAN
D. NAC
Answer: (SHOW ANSWER)
Network Access Control (NAC) enforces policies that determine whether devices can connect to a network based on posture, identity, and compliance.

NEW QUESTION: 78
Who is responsible for publishing and signing the organization's policies?
A. The security office
B. Human resources
C. Senior management
D. The legal department
Answer: (SHOW ANSWER)
Senior management is ultimately responsible for approving, signing, and publishing organizational policies.
While departments such as security, HR, and legal may draft, review, or advise on policies, executive leadership provides formal authorization and accountability.
This responsibility aligns with governance principles outlined in frameworks like ISO/IEC 27001 and NIST, which emphasize management commitment to information security. Policies require executive endorsement to ensure they are enforceable, aligned with business objectives, and supported with appropriate resources.
Senior management's involvement demonstrates organizational commitment, establishes authority, and ensures compliance across all departments. Without leadership approval, policies lack legitimacy and may not be consistently followed.
Security operations rely on clear, management-approved policies to guide procedures, incident response, and compliance activities. Executive sponsorship also enables enforcement and disciplinary actions when policies are violated.

NEW QUESTION: 79
Which OSI layer associates MAC addresses with network devices?
A. Physical layer
B. Network layer
C. Data Link layer
D. Transport layer
Answer: (SHOW ANSWER)
The Data Link layer (Layer 2) handles MAC addressing and frame delivery within local networks.

NEW QUESTION: 80
Which protocol is used for secure email?
A. POP3S
B. IMAPS
C. SMTPS
D. All
Answer: (SHOW ANSWER)
All listed protocols provide encrypted email communication using SSL/TLS for sending or retrieving email securely.

NEW QUESTION: 81
The practice of sending fraudulent communications that appear to come from a reputable source is known as:
A. DoS
B. Virus
C. Spoofing
D. Phishing
Answer: (SHOW ANSWER)
Phishing uses deceptive messages-often emails or websites-to trick users into revealing sensitive information. Spoofing is often used as a technique within phishing attacks.

NEW QUESTION: 82
A team activates procedures to mitigate a cyberattack. What plan is this?
A. Business Continuity Plan
B. Incident Response Plan
C. Disaster Recovery Plan
D. Security Operations Plan
Answer: (SHOW ANSWER)
An Incident Response Plan (IRP) defines how to detect, analyze, contain, eradicate, and recover from security incidents.

NEW QUESTION: 83
In incident terminology, a zero-day is:
A. Days with a cybersecurity incident
B. A previously unknown system vulnerability
C. Days without a cybersecurity incident
D. Days to solve a previously unknown system vulnerability
Answer: (SHOW ANSWER)
A zero-day vulnerability is a security flaw that is unknown to the vendor and defenders at the time it is discovered or exploited. Because there is no patch available, organizations have "zero days" to fix it.

NEW QUESTION: 84
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: 85
A company's governing board decides that only legal services may review third-party contracts. They create a document stating that no other department has permission to do so. This document is a:
A. Procedure
B. Policy
C. Standard
D. Law
Answer: (SHOW ANSWER)
Apolicyis a high-level, mandatory statement approved by senior management that defines what is allowed or required within an organization. In this scenario, the governing board establishes a rule that only the legal department may review third-party contracts, making it a policy decision.
Procedures provide step-by-step instructions, standards define specific technical or operational requirements, and laws are external legal mandates imposed by governments. None of those best describe this situation.
Policies establish authority, accountability, and organizational intent. They are enforceable and form the foundation for standards and procedures. Governance frameworks emphasize management-approved policies as essential for consistent and compliant operations.

NEW QUESTION: 86
Which version of TLS is considered the most secure and recommended for use?
A. TLS 1.0
B. TLS 1.1
C. TLS 1.2
D. TLS 1.3
Answer: (SHOW ANSWER)
TLS 1.3 is the most secure and currently recommended version of the Transport Layer Security protocol. It removes outdated cryptographic algorithms, simplifies the handshake process, and provides stronger security guarantees than earlier versions.
TLS 1.3 eliminates insecure features such as static RSA key exchange and weak cipher suites. It enforces forward secrecy by default and significantly reduces handshake latency, improving both security and performance.
TLS 1.0 and TLS 1.1 are deprecated due to known vulnerabilities. TLS 1.2 is still secure when properly configured but is being phased out in favor of TLS 1.3.
Security frameworks and regulatory standards strongly recommend TLS 1.3 for protecting sensitive data in transit, especially for public-facing services.

NEW QUESTION: 87
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: (SHOW ANSWER)
Anintrusionis an unauthorized attempt to access systems or resources, whether successful or not.

NEW QUESTION: 88
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: (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: 89
David's team recently implemented a new system that gathers information from a variety of different log sources, analyzes that information, and then triggers automated playbooks in response to security events.
What term BEST describes this technology?
A. SIEM
B. Log Repository
C. IPS
D. SOAR
Answer: D (LEAVE A REPLY)
SOAR (Security Orchestration, Automation, and Response) platforms are designed to collect security data from multiple tools, analyze events, and automatically execute response actions using predefined playbooks.
This automation allows security teams to respond quickly and consistently to incidents.
While SIEM systems collect and correlate logs and generate alerts, they typically require manual analyst intervention for response. SOAR extends SIEM capabilities by orchestrating workflows

across tools such as firewalls, endpoint protection, ticketing systems, and threat intelligence platforms.
Log repositories store logs without analysis or response capabilities. Intrusion Prevention Systems (IPS) focus on blocking malicious traffic in real time but do not coordinate broader incident response actions.
SOAR solutions reduce alert fatigue, improve response time, and standardize incident handling procedures.
They are a key component of mature Security Operations Centers (SOCs) and are strongly recommended by modern security operations frameworks.

NEW QUESTION: 90

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: (SHOW ANSWER)
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: 91
Which authentication enables automatic identification across multiple service providers?
A. Basic
B. Kerberos
C. Token-based
D. Federated
Answer: (SHOW ANSWER)
Federated authentication enables single identity across trusted organizations, supporting single sign-on (SSO) and eliminating repeated credential entry.

NEW QUESTION: 92
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: (SHOW ANSWER)
A Disaster Recovery Plan (DRP) provides procedures to restore IT systems, applications, and infrastructure after an outage.

NEW QUESTION: 93
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: (SHOW ANSWER)
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: 94
Which security measure helps prevent Cross-Site Scripting (XSS) attacks?
A. Strong password policies
B. Firewall blocking
C. Validating and sanitizing user input
D. Encrypting data
Answer: C (LEAVE A REPLY)
Validating and sanitizing user input prevents malicious scripts from being injected and executed in a user's browser. Input validation is the primary defense against XSS.

NEW QUESTION: 95
A tool used to inspect outbound traffic to reduce threats:
A. Anti-malware
B. NIDS
C. DLP

D. Firewall

Answer: (SHOW ANSWER)

Data Loss Prevention (DLP) tools inspect outbound traffic to prevent unauthorized data exfiltration.

NEW QUESTION: 96

A popular way of implementing the principle of least privilege is:

A. MAC

B. DAC

C. RBAC

D. ABAC

Answer: (SHOW ANSWER)

Role-Based Access Control (RBAC) enforces least privilege by assigning permissions based on job roles rather than individuals. Users receive only the permissions necessary for their role, reducing excess access.

RBAC is widely used in enterprises, cloud platforms, and operating systems due to its scalability and manageability.

NEW QUESTION: 97

A measure combining impact and likelihood is known as:

A. Impact

B. Risk

C. Threat

D. Threat vector

Answer: (SHOW ANSWER)

Risk is calculated by evaluating the likelihood of a threat exploiting a vulnerability and the resulting impact.

NEW QUESTION: 98

The documented set of procedures to detect, respond to, and limit the consequences of cyberattacks is called:

A. IR

B. IRP

C. BCP

D. DRP

Answer: (SHOW ANSWER)

An Incident Response Plan (IRP) outlines roles, responsibilities, and procedures for handling security incidents and minimizing damage.

NEW QUESTION: 99

Which is the most efficient and effective way to test a business continuity plan?

A. Simulations

B. Discussions
C. Walkthroughs
D. Reviews
Answer: (SHOW ANSWER)
Simulations provide realistic testing by executing scenarios that closely mirror real disruptions, revealing gaps and readiness levels better than discussions or reviews.

NEW QUESTION: 100
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: (SHOW ANSWER)
Recovery controls restore systems and data after an incident. Examples include backups, failover systems, and disaster recovery procedures.

NEW QUESTION: 101
The concept of integrity applies to:
A. Organization
B. Information systems and business processes
C. People
D. All
Answer: (SHOW ANSWER)
Integrity applies broadly-to data, systems, processes, and organizational operations-ensuring accuracy, completeness, and trustworthiness.

NEW QUESTION: 102
Which organization defines Internet protocol standards?
A. ISO
B. NIST
C. IETF
D. GDPR
Answer: C (LEAVE A REPLY)
The Internet Engineering Task Force (IETF) develops and maintains Internet standards through RFCs.

NEW QUESTION: 103
Limiting access based on data sensitivity and user authorization is known as:
A. DAC

B. MAC
C. RuBAC
D. RBAC
Answer: (SHOW ANSWER)
MAC enforces access based on classification labels and user clearances, commonly used in military and government systems.

NEW QUESTION: 104
Which provides integrity services that allow a recipient to verify that a message has not been altered?
A. Hashing
B. Encryption
C. Decryption
D. Encoding
Answer: A (LEAVE A REPLY)
Hashing produces a fixed-length value that uniquely represents data. Any modification to the data changes the hash, allowing integrity verification. Hashing does not provide confidentiality but is critical for detecting tampering.

NEW QUESTION: 105
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: (SHOW ANSWER)
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: 106
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: 107
During an ISC2 CC exam, you observe another candidate cheating. What should you do?
A. Yell at them
B. Do nothing
C. Report the candidate to ISC2
D. Call law enforcement
Answer: (SHOW ANSWER)
ISC2's Code of Ethics requires candidates to report violations through proper channels to preserve exam integrity.

NEW QUESTION: 108
A centralized organizational function that monitors, detects, and analyzes security events to prevent disruptions is called:
A. IRP
B. BCP
C. SOC
D. DRP
Answer: (SHOW ANSWER)
ASecurity Operations Center (SOC)is a centralized function responsible for continuous monitoring, detection, analysis, and response to cybersecurity events. SOC teams use tools such as SIEM, SOAR, IDS/IPS, and threat intelligence feeds to identify threats before they escalate into incidents.

NEW QUESTION: 109
Ping flood attacks target which OSI layer?
A. Layer 4
B. Layer 3
C. Layer 5

D. Layer 6

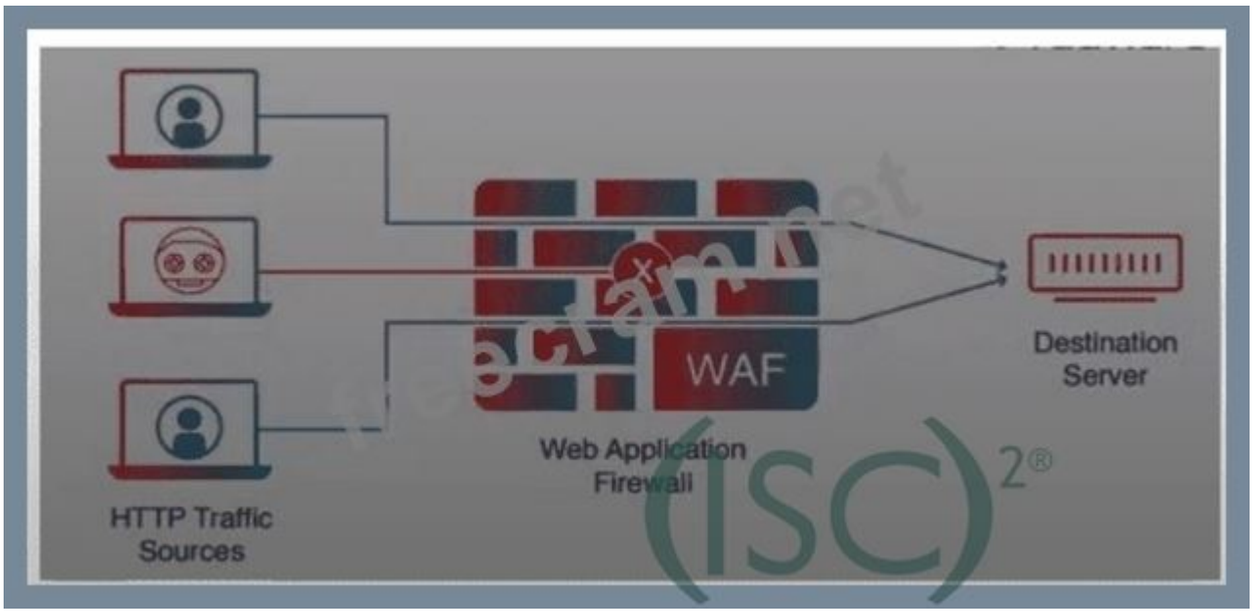
Answer: (SHOW ANSWER)

A ping flood attack exploits the Internet Control Message Protocol (ICMP), which operates atOSI Layer 3 (Network Layer). The attacker overwhelms a target system by sending a large volume of ICMP Echo Request (ping) packets, consuming bandwidth and processing resources.

Because ICMP is used for network diagnostics and error reporting, excessive ICMP traffic can prevent legitimate network communication, leading to a denial-of-service condition. Since IP and ICMP are Layer 3 protocols, ping flood attacks directly impact the network layer.

NEW QUESTION: 110

Exhibit.



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

A. To protect the web server from DDoS attacks

B. To monitor network traffic for intrusions

C. To filter and block malicious web traffic and requests

D. To manage SSL certificates

Answer: (SHOW ANSWER)

The primary purpose of aWeb Application Firewall (WAF)is tofilter, monitor, and block malicious HTTP

/HTTPS trafficdirected at web applications. A WAF operates at theapplication layer (Layer 7)of the OSI model and is specifically designed to protect web applications from common attacks such as SQL injection, cross-site scripting (XSS), command injection, and other OWASP Top 10 vulnerabilities.

Unlike traditional network firewalls, which focus on IP addresses, ports, and protocols, a WAF understands web-specific traffic patterns and inspects the content of HTTP requests and responses. This allows it to detect malicious payloads embedded in URLs, headers, cookies, and request bodies.

While some WAFs may offer limited protection against application-layer DDoS attacks, DDoS mitigation is not their primary function. Intrusion detection is typically handled by IDS/IPS solutions, and SSL certificate management is unrelated to WAF functionality.
Security frameworks such as NIST and OWASP recommend WAFs as a critical compensating control for protecting public-facing web applications, especially when secure coding fixes cannot be deployed immediately.

NEW QUESTION: 111
Common network device used to connect networks?
A. Server
B. Endpoint
C. Router
D. Switch
Answer: (SHOW ANSWER)
A router is a network device specifically designed to connect multiple networks and route traffic between them. Routers operate primarily at Layer 3 (the Network Layer) of the OSI model and use IP addresses to determine the best path for data packets.
Routers are commonly used to connect local area networks (LANs) to wide area networks (WANs), such as connecting an internal corporate network to the internet. They also play a role in enforcing network security by supporting access control lists (ACLs), network address translation (NAT), and routing policies.
Switches, while important, typically connect devices within the same network and operate at Layer 2. Servers and endpoints are hosts, not networking devices. Without routers, communication between separate networks would not be possible, severely limiting scalability and connectivity.
From a security perspective, routers help segment networks, reduce broadcast traffic, and control data flow, making them essential components in both performance and security architectures.

NEW QUESTION: 112
If a device is found to be non-compliant with the security baseline, what action should the security team take?
A. Report
B. Evaluate
C. Ignore
D. Disable or isolate it into a quarantine area until it can be checked and updated
Answer: (SHOW ANSWER)
When a device does not meet security baseline requirements, it poses a risk to the environment. Best practice is todisable or quarantine the deviceto prevent potential compromise or lateral movement. Network Access Control (NAC) solutions commonly automate this process.
Isolation ensures the device cannot interact with production systems until it is patched, configured correctly, and verified as compliant. This approach aligns with NIST and Zero Trust principles, emphasizing continuous compliance and containment.

NEW QUESTION: 113
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: 114
The last phase in the data security lifecycle is:
A. Encryption
B. Destruction
C. Archival
D. Backup
Answer: (SHOW ANSWER)
The final phase in the data security lifecycle isdestruction. After data is no longer required for business, legal, or regulatory purposes, it must be securely destroyed to prevent unauthorized recovery or misuse.
Encryption, backup, and archival are all earlier phases focused on protecting data during use, storage, and retention. Destruction ensures data is permanently removed through secure wiping, degaussing, or physical destruction of media.
Improper data disposal can lead to data breaches through remanence. NIST SP 800-88 provides detailed guidance on secure media sanitization and destruction methods. Secure destruction is especially critical for sensitive and regulated data such as PII, PHI, and financial records.

NEW QUESTION: 115
What is the first step in incident response planning?
A. Develop a management-approved policy
B. Identify critical systems
C. Train staff
D. Form the IR team
Answer: (SHOW ANSWER)
An incident response policy establishes authority, scope, and direction. Without management approval, IR activities lack legitimacy.

NEW QUESTION: 116
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: (SHOW ANSWER)
A complete BCP includes response procedures, communication plans, and management authority to ensure coordinated recovery.

NEW QUESTION: 117
A security model where no network is trusted by default is called:
A. Zero Trust
B. Trusted computing
C. TPM
D. TEE
Answer: (SHOW ANSWER)
Zero Trust assumes no implicit trust and requires continuous verification of users, devices, and access requests, regardless of location.

NEW QUESTION: 118
Methods or mechanisms used to gain unauthorized access are called:
A. Attacker
B. Threat vector
C. Threat
D. Threat actor
Answer: B (LEAVE A REPLY)
Threat vectors are the paths or techniques attackers use, such as phishing, malware, or exploitation.

NEW QUESTION: 119
Which cloud service model provides the most suitable environment for customers to build and operate their own software?
A. SaaS
B. IaaS
C. PaaS
Answer: (SHOW ANSWER)
Platform as a Service (PaaS) provides customers with an environment tobuild, deploy, and manage applicationswithout managing underlying infrastructure. PaaS includes operating systems, middleware, runtime environments, and development tools.
SaaS delivers fully managed applications, while IaaS provides raw infrastructure. PaaS best balances flexibility and operational efficiency for software development.

NEW QUESTION: 120

COVID-19 is an example where which plan sustains business?

A. IRP

B. DRP

C. BCP

D. All

Answer: (SHOW ANSWER)

Business Continuity Plans ensure operations continue during long-term disruptions.

NEW QUESTION: 121

A DDoS attack affects which OSI layers?

A. Network layer

B. Transport layer

C. Physical layer

D. Both A and B

Answer: (SHOW ANSWER)

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: 122

Access control used in high-security military and government environments:

A. DAC

B. MAC

C. RBAC

D. ABAC

Answer: (SHOW ANSWER)

Mandatory Access Control (MAC) enforces centrally managed security labels and clearances, making it suitable for classified and government systems.

NEW QUESTION: 123

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: 124

Networks that are heavily microsegmented with firewalls at connection points are characteristic of:

A. DMZ

B. VPN

C. VLAN

D. Zero Trust

Answer: (SHOW ANSWER)

Zero Trust architectures rely on microsegmentation and continuous enforcement to limit lateral movement.

NEW QUESTION: 125

Which addresses are reserved for internal network use and are not routable on the Internet?

A. ac00:: to adff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

B. fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

C. bc00:: to bdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

D. cc00:: to cdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Answer: (SHOW ANSWER)

The IPv6 address rangefc00::/7, which includesfc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, is reserved forUnique Local Addresses (ULAs). ULAs are the IPv6 equivalent of private IPv4 addresses (such as 10.0.0.0
/8 or 192.168.0.0/16). These addresses are intended for internal communications within an organization and arenot routable on the public Internet.
ULAs allow organizations to design internal IPv6 networks without relying on globally routable addresses.
This enhances security by reducing external exposure and simplifies internal network design.
According to RFC 4193, ULAs are designed to be globally unique within private networks while remaining isolated from the public Internet.

NEW QUESTION: 126

An organization develops procedures to restore critical business processes after a major disruption. What plan is this?

A. BCP

B. IRP

C. DRP

D. None

Answer: (SHOW ANSWER)

ABusiness Continuity Plan (BCP)ensures critical business functions continue or are restored during and after disruptions.

NEW QUESTION: 127
What is the difference between BCP and DRP?
A. BCP restores IT; DRP maintains business functions
B. DRP restores IT; BCP maintains business functions
C. They are the same
D. BCP is only before disasters
Answer: (SHOW ANSWER)
Disaster Recovery Planning (DRP) focuses on restoringIT systems and communications, while Business Continuity Planning (BCP) ensurescritical business functions continueduring disruptions. They are complementary but distinct disciplines.

NEW QUESTION: 128
The order of controls used in defense in depth:
A. Assets # Physical # Administrative # Technical
B. Assets # Administrative # Physical # Technical
C. Physical # Administrative # Technical # Assets
D. Assets # Administrative # Technical # Physical
Answer: (SHOW ANSWER)
Defense in depth begins by identifying assets, followed by administrative controls (policies), technical controls (logical), and physical controls to protect systems at multiple layers.

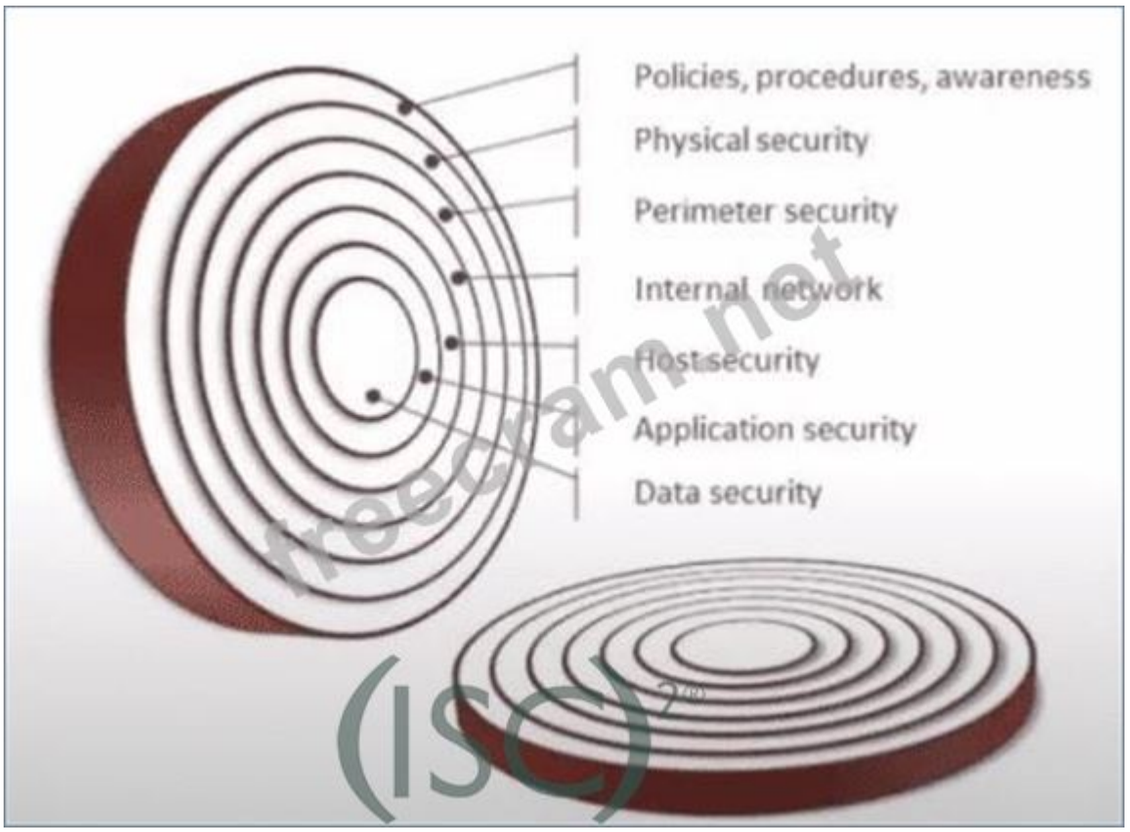
NEW QUESTION: 129
Port scanning attacks target which OSI layer?
A. Layer 4
B. Layer 3
C. Layer 5
D. Layer 6
Answer: (SHOW ANSWER)
Port scanning targetstransport-layer ports(TCP/UDP), making Layer 4 the correct answer.

NEW QUESTION: 130
The process of applying secure configurations to reduce the attack surface is known as:
A. Security assessment
B. Security evaluation
C. Security benchmark
D. Security hardening
Answer: (SHOW ANSWER)

Security hardening involves disabling unnecessary services, applying secure configurations, and reducing system exposure. It is a core preventative security practice recommended by NIST and CIS.

NEW QUESTION: 131
What is sensitivity in the context of confidentiality?
A. Harm caused to external stakeholders
B. Ability of information to be accessed only by authorized users
C. Need for protection assigned to information by its owner
D. Health status of individuals
Answer: (SHOW ANSWER)
Sensitivity refers to thedegree of protection required for information, as determined by its owner. Highly sensitive data requires stronger confidentiality controls because unauthorized disclosure could cause significant harm.

NEW QUESTION: 132
Exhibit.



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

A. File permissions

B. Buffer overflow

C. Zero-day vulnerability

D. Cross-site scripting

Answer: (SHOW ANSWER)

Azero-day vulnerabilityis typically not identifiable through a standard vulnerability assessment. Vulnerability scanners and routine assessments rely onknown vulnerability signatures, published advisories, and documented weaknesses. By definition, a zero-day vulnerability is unknown to vendors, defenders, and security tools at the time it exists or is exploited.

File permission issues, buffer overflows, and cross-site scripting (XSS) vulnerabilities are commonly detected through automated scans, configuration reviews, and application testing because they are well understood and documented classes of weaknesses. Scanners are specifically designed to identify these known issues.

Zero-day vulnerabilities, however, require alternative detection approaches such as behavioral monitoring, anomaly detection, threat intelligence, or post-exploitation forensics. This limitation is why vulnerability assessments alone are insufficient and must be complemented withdefense-in-depth, monitoring, and incident response capabilities.

Security frameworks consistently emphasize that organizations should not rely solely on vulnerability scanning, as it cannot detect unknown or newly emerging threats like zero-day vulnerabilities.

NEW QUESTION: 133

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: (SHOW ANSWER)

ADenial-of-Service (DoS)attack disrupts availability by overwhelming systems or resources, preventing legitimate access.

NEW QUESTION: 134

A device that forwards traffic to the port of a known destination device is a:

A. Switch

B. Hub

C. Router

D. Ethernet

Answer: (SHOW ANSWER)

A switch operates at Layer 2 and forwards traffic only to the destination port based on MAC address tables, unlike hubs which broadcast traffic.

NEW QUESTION: 135

Which is the loopback address?

A. ::1

B. 127.0.0.1

C. 255.255.255.0

D. Both A and B

Answer: (SHOW ANSWER)

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: 136

Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.

A. Zero Trust

B. DMZ

C. VLAN

D. Microsegmentation

Answer: (SHOW ANSWER)

Zero Trust is a security architecture that assumesno implicit trust-inside or outside the network perimeter.

Every access request must be continuously verified based on identity, device health, context, and policy.
Unlike traditional perimeter-based models, Zero Trust eliminates the concept of a "trusted internal network." Microsegmentation is a core Zero Trust technique that divides networks and workloads into highly granular security zones. Each zone enforces its own access controls, dramatically reducing lateral movement if an attacker gains access. This model aligns with NIST SP 800-207, which defines Zero Trust as a strategy to minimize attack surfaces and contain breaches.

NEW QUESTION: 137
After an earthquake disrupts business operations, which document contains the reactive procedures required to return business to normal operations?
A. Business Impact Analysis
B. Business Continuity Plan
C. Disaster Recovery Plan
D. Business Impact Plan
Answer: (SHOW ANSWER)
The Disaster Recovery Plan (DRP) contains step-by-step technical procedures to restore IT systems, data, and infrastructure after a disruptive event. While the BCP focuses on maintaining operations, the DRP focuses onrestoration.

NEW QUESTION: 138
Is defined as the process of identifying, estimating, and prioritizing risks.
A. Risk Assessment
B. Risk Treatment
C. Risk Mitigation
D. Risk Management
Answer: (SHOW ANSWER)
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: 139
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: (SHOW ANSWER)
ASHRAE recommends64°F-81°Ffor modern data centers to balance hardware longevity and energy efficiency.

NEW QUESTION: 140
An attack in which a user authenticated to a server unknowingly invokes unwanted actions after visiting a malicious website is known as:

A. XSS
B. CSRF
C. Spoofing
D. ALL
Answer: (SHOW ANSWER)
Cross-Site Request Forgery (CSRF) tricks an authenticated user's browser into sending unauthorized requests to a trusted server. Because the user is already authenticated, the server processes the request as legitimate.
XSS injects malicious scripts, while spoofing involves impersonation. CSRF exploits trust in an existing authenticated session. Defenses include CSRF tokens, same-site cookies, and proper request validation.

NEW QUESTION: 141
What is knowledge-based authentication?
A. Authentication based on a passphrase or secret code
B. Authentication based on a token or smart card
C. Authentication based on biometrics
D. Authentication based on behavior
Answer: (SHOW ANSWER)
Knowledge-based authentication relies onsomething the user knows, such as passwords, PINs, or answers to security questions. It is the most common but also the weakest form of authentication due to susceptibility to guessing, phishing, and brute-force attacks. For this reason, it is often combined with other factors in multi- factor authentication (MFA).

NEW QUESTION: 142
Events with negative consequences such as crashes, floods, defacement, or malicious code execution are called:
A. Breach
B. Incident
C. Adverse event
D. Exploit
Answer: (SHOW ANSWER)
Anadverse eventis a harmful occurrence that may or may not constitute a security incident or breach.

NEW QUESTION: 143
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: 144
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: (SHOW ANSWER)
ABAC supports dynamic, context-aware access decisions based on attributes such as location, device, and time-ideal for global access scenarios.

NEW QUESTION: 145
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: (SHOW ANSWER)
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: 146
Which document provides a high-level overview of a Disaster Recovery Plan?
A. Technical guides
B. Department-specific plans
C. Full plan copies for team members
D. Executive summary
Answer: (SHOW ANSWER)
Anexecutive summarygives leadership a concise overview of objectives, scope, and recovery strategies without technical detail.

NEW QUESTION: 147
Port used by DNS.
A. 53
B. 80
C. 45
D. 54
Answer: (SHOW ANSWER)
DNS primarily usesport 53over UDP and TCP for name resolution.

NEW QUESTION: 148
Dylan is creating a cloud architecture that requires connections between systems in two different private VPCs. What is the BEST way to enable this access?
A. VPN connection
B. Internet gateway
C. Public IP address
D. VPC endpoint
Answer: D (LEAVE A REPLY)
A VPC endpoint is the best solution for enabling secure, private connectivity between systems in different virtual private clouds (VPCs) without traversing the public internet. VPC endpoints allow private communication using the cloud provider's internal network.
VPNs introduce additional overhead and complexity, while internet gateways and public IP addresses expose systems to the public internet, increasing attack surface.

VPC endpoints provide strong security, reduced latency, and simplified architecture. They are recommended by cloud providers and security frameworks for private, internal cloud communication.

NEW QUESTION: 149
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: (SHOW ANSWER)
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: 150
What is the primary factor in the reliability of information and systems?
A. Authenticity
B. Confidentiality
C. Integrity
D. Availability
Answer: (SHOW ANSWER)
Integrityis the primary factor in system and information reliability. Reliable systems must ensure that data is accurate, complete, and protected from unauthorized modification. If integrity is compromised, decisions based on the data become unreliable-even if systems are available or confidential. NIST and ISO frameworks emphasize integrity as essential to trustworthiness and operational reliability.

NEW QUESTION: 151
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: 152
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: 153
Faking the sender address of a transmission to gain illegal entry is called:
A. Phishing
B. ARP
C. Spoofing
D. All
Answer: (SHOW ANSWER)
Spoofing involves falsifying identity information (IP, MAC, email headers) to appear as a trusted source and bypass controls.

NEW QUESTION: 154
Configuration settings or parameters stored as data and managed through a GUI are examples of:
A. Logical access control
B. Physical access control
C. Administrative access control

Answer: (SHOW ANSWER)
Logical access controls enforce security through software-based mechanisms such as access control lists, authentication systems, and configuration settings.

NEW QUESTION: 155
What is the highest priority during incident response?
A. Protect mission
B. Reduce impact
C. Protect life, health, and safety
D. Resume operations
Answer: (SHOW ANSWER)
Human safety always takes precedence over systems, data, and business operations.

NEW QUESTION: 156
Which fire suppression system is more friendly to electronics?
A. Carbon dioxide-based
B. Chemical-based
C. Water-based
D. Foam-based
Answer: (SHOW ANSWER)
Carbon dioxide (CO#) systems suppress fire without leaving residue or damaging electronic equipment.
While they pose risks to people, they are effective for protecting electronics compared to water or foam.

NEW QUESTION: 157
Activities necessary to restore IT and communications services are known as:
A. Incident response
B. Business continuity
C. Risk management
D. Disaster recovery
Answer: (SHOW ANSWER)
Disaster Recovery (DR)focuses specifically on restoring IT systems and communications following outages.

NEW QUESTION: 158
Which document serves as specifications for implementing policy and dictates mandatory requirements?
A. Policy
B. Guideline
C. Standard

D. Procedure

Answer: (SHOW ANSWER)

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: 159

Which of the following best describes a zero-day vulnerability?

A. A vulnerability that has been identified and patched

B. A vulnerability that has not yet been discovered or publicly disclosed

C. A vulnerability exploitable only by experts

D. A vulnerability that affects only legacy systems

Answer: (SHOW ANSWER)

A zero-day vulnerability is one that is unknown to the vendor and has no available patch at the time it is exploited. Attackers take advantage of the fact that defenders have "zero days" to fix the issue. Routine vulnerability scans cannot detect zero-days because scanners rely on known signatures. This is why defense-in-depth, monitoring, and anomaly detection are critical security strategies.

NEW QUESTION: 160

A _____ creates an encrypted tunnel to protect your personal data and communications.

A. HTTPS

B. VPN

C. Anti-virus

D. IDS

Answer: (SHOW ANSWER)

A Virtual Private Network (VPN) creates an encrypted tunnel between a user's device and a remote network or server. This tunnel protects data confidentiality and integrity by encrypting all traffic passing through it, even when using untrusted networks such as public Wi-Fi.

HTTPS encrypts only web traffic, antivirus detects malware, and IDS monitors for suspicious activity. Only a VPN provides full-tunnel encryption for all network communications. VPNs are commonly implemented using protocols such as IPSec or SSL/TLS and are widely recommended for secure remote access.

NEW QUESTION: 161

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: 162
What is the main objective of DRP after a breach shuts down systems?
A. Relocation
B. Employee safety
C. Prosecution
D. Restore systems
Answer: (SHOW ANSWER)
The primary objective of DRP is restoring IT systems to a reliable operational state.

NEW QUESTION: 163
VLAN hopping belongs to which OSI layer?
A. Layer 3
B. Layer 4
C. Layer 7
D. Layer 2
Answer: (SHOW ANSWER)
VLAN hopping exploits weaknesses in Layer 2 switching mechanisms such as trunking and tagging.

NEW QUESTION: 164
How many bits represent the Organizationally Unique Identifier (OUI) in MAC addresses?
A. 16 bits
B. 48 bits
C. 24 bits
D. 32 bits
Answer: (SHOW ANSWER)
A MAC (Media Access Control) address is 48 bits long and is divided into two main parts. The first24 bitsrepresent theOrganizationally Unique Identifier (OUI), which is assigned by IEEE to hardware manufacturers.
The remaining 24 bits are assigned by the manufacturer to uniquely identify individual network interfaces.
The OUI allows network administrators and tools to identify the vendor of a network device. Understanding MAC addressing is important for network security, device identification, and troubleshooting.

MAC addresses are commonly used in access control mechanisms such as MAC filtering, although they should not be relied upon as a strong security control due to spoofing risks.

NEW QUESTION: 165
David is worried about distributed denial-of-service (DDoS) attacks against his company's primary web application. Which option will provide the MOST resilience against large-scale DDoS attacks?
A. Implement a CDN
B. Increase the number of servers in the web application cluster
C. Contract for DDoS mitigation services via the company's IPS
D. Increase bandwidth from one or more ISPs
Answer: (SHOW ANSWER)
A Content Delivery Network (CDN) provides the greatest resilience against large-scale DDoS attacks by distributing traffic across a globally dispersed network of edge servers. CDNs absorb and filter malicious traffic before it reaches the origin infrastructure.
Increasing servers or bandwidth helps only to a limited extent and can still be overwhelmed by volumetric attacks. IPS-based mitigation is effective for smaller attacks but is not designed to handle massive distributed floods. CDNs combine traffic absorption, rate limiting, caching, and threat filtering at scale.
Major CDNs operate with terabits of capacity and specialized DDoS defenses, making them highly effective against attacks that would cripple individual organizations.
For public-facing applications, CDNs are considered a best-practice defensive control against availability attacks.

NEW QUESTION: 166
Flooding a server with traffic to make services unavailable is called:
A. Phishing
B. Virus
C. Spoofing
D. DDoS
Answer: (SHOW ANSWER)
Distributed Denial-of-Service (DDoS) attacks overwhelm targets with traffic from multiple sources, disrupting availability.

NEW QUESTION: 167
Juli is listening to network traffic and capturing passwords as they are sent to the authentication server. She plans to use the passwords as part of a future attack. What type of attack is this?
A. Brute-force attack
B. Dictionary attack
C. Social engineering attack
D. Replay attack
Answer: (SHOW ANSWER)
This scenario describes areplay attack, in which an attacker captures valid authentication data and reuses it later to gain unauthorized access. Juli is passively monitoring network traffic, capturing credentials as they are transmitted, and planning to reuse them in a future attack.
Replay attacks often occur when authentication mechanisms do not use protections such as encryption, nonces, timestamps, or session tokens. If credentials are transmitted in clear text or without replay protection, attackers can intercept and reuse them without needing to crack passwords.
Brute-force and dictionary attacks involve guessing credentials, not capturing them. Social engineering relies on human manipulation rather than technical interception.
Replay attacks highlight the importance of secure protocols such as TLS, encrypted authentication exchanges, challenge-response mechanisms, and one-time passwords. NIST authentication guidance explicitly identifies replay resistance as a critical requirement for secure authentication systems.

NEW QUESTION: 168
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: 169
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: 170
Mark is configuring an automated data transfer between two hosts and needs an authentication method. What approach is best suited?

A. Biometric
B. Smart Card
C. SSH Key
D. Hard-coded Password
Answer: (SHOW ANSWER)
SSH key-based authentication is ideal for automated system-to-system communication. It allows secure, passwordless authentication using cryptographic key pairs.
Biometrics and smart cards require human interaction, and hard-coded passwords are insecure and difficult to rotate. SSH keys provide strong authentication, automation support, and secure key management.
This approach is widely recommended for scripts, automation, and DevOps pipelines.

NEW QUESTION: 171
Security controls protecting against fire, floods, and earthquakes are:
A. Physical controls
B. Logical controls
C. Administrative controls
D. Technical controls
Answer: (SHOW ANSWER)
Physical controls such as fire suppression systems, flood barriers, and seismic bracing protect facilities and equipment from environmental threats.

NEW QUESTION: 172
Exhibit.

information security is not built on which of the following?

A. Confidentiality

B. Availability

C. Accessibility

D. Integrity

Answer: (SHOW ANSWER)

Information security is fundamentally built on theCIA triad:Confidentiality, Integrity, and Availability. These three principles form the cornerstone of nearly all cybersecurity frameworks, including NIST, ISO/IEC

27001, and CIS controls.

* Confidentialityensures that information is accessible only to authorized individuals and systems.

* Integrityensures that data remains accurate, complete, and unaltered except by authorized actions.

* Availabilityensures that systems and data are accessible to authorized users when needed.

Accessibility, while related to usability and system design, isnota core pillar of information security. In fact, security controls often intentionallylimitaccessibility to protect systems and data. Accessibility focuses on ensuring ease of access (often in the context of user experience or disability access), whereas security focuses oncontrolled access.

Confusing accessibility with availability is common, but they are not the same. Availability is about reliable access forauthorized users, while accessibility is about ease of access in general. Therefore, accessibility is not one of the foundational elements upon which information security is built.

This distinction is critical for understanding security architecture and governance.