GIAC.GDSA.v2025-09-16.q89

Exam Code:	GDSA
Exam Name:	GIAC Defensible Security Architect
Certification Provider:	GIAC
Free Question Number:	89
Version:	v2025-09-16
# of views:	111
# of Questions views:	890
https://www.freecram.net/torrent/GIAC.GDSA.v2025-09-16.q89.html	

NEW QUESTION: 1
Which of the following is true regarding the deployment of Network Access Control (NAC)?
Response:
A. It is used to provide high bandwidth to critical applications.
B. It can prevent endpoints that do not comply with policy from accessing the network.
C. It allows all devices onto the network without any form of authentication.
D. It decreases network visibility and control.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
In a data-centric security model, reverse proxies are primarily used to:
Response:
A. Authenticate users across multiple cloud services
B. Manage and filter incoming client requests before they reach the backend server
C. Provide automatic backup for database transactions
D. Encrypt data at rest
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Your security operations team has detected unusual activity on your organization's network, suggesting a DDoS attack is underway. Multiple external IP addresses are sending excessive amounts of traffic to your web server.
What immediate steps should you take to mitigate the attack and protect your infrastructure?
Response:
A. Block all outbound network traffic and initiate a full system scan
B. Migrate all services to a backup data center and restore data from backups

C. Enable rate-limiting and deploy a Web Application Firewall (WAF) to filter traffic from malicious IPs
D. Disconnect the web server from the internet to stop all incoming traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 4
What is the role of next-generation firewalls (NGFWs) in modern network security architectures?
Response:
A. Replacing the need for encryption technologies
B. Restricting access based solely on IP addresses
C. Providing signature-based malware detection only
D. Integrating deep packet inspection with advanced threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 5
What is the primary focus of container security in cloud environments?
Response:
A. Data encryption
B. Isolating applications
C. User authentication
D. Bandwidth optimization
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which of the following is not a typical cloud service model?
Response:
A. CaaS
B. SaaS
C. PaaS
D. IaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Within a Zero Trust model, which actions help mitigate the risk of insider threats?
(Choose two)
Response:
A. Mandatory vacation policies
B. Regular user behavior analytics
C. Frequent change of user roles and responsibilities
D. Implementation of least privilege access
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which of the following is the primary function of a web proxy?
Response:
A. Filtering and managing web traffic between users and the internet
B. Encrypting all data in transit
C. Monitoring and blocking email-based phishing attacks
D. Preventing unauthorized users from accessing the network
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which defenses can help mitigate the risk of Distributed Denial of Service (DDoS) attacks? (Choose two)
Response:
A. Deploying a Web Application Firewall (WAF)
B. Isolating internal networks using VLANs
C. Implementing Network Address Translation (NAT)
D. Using rate-limiting to control incoming traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 10
Which of the following techniques is used to authenticate and encrypt endpoint traffic in Zero Trust Networking?

Response:
A. Single Packet Authentication
B. Domain Isolation
C. Red herring defenses
D. Transport Layer Security (TLS)
Answer: (SHOW ANSWER)

NEW QUESTION: 11
What are the purposes of using a sandbox in network defense?
Response:
A. Enhancing user experience
B. Storing sensitive information
C. Analyzing malware behavior
D. Testing untrusted programs
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 12
What are the primary security benefits of implementing 802.1X on a network?

(Choose two)
Response:
A. It ensures data encryption across the network.
B. It provides automatic routing optimization.
C. It establishes identity-based network access control.
D. It prevents unauthorized network access at the port level.
Answer: (SHOW ANSWER)

NEW QUESTION: 13
The Intrusion Kill Chain model helps in understanding an attacker's actions by dividing the attack process into distinct phases. Which of the following is NOT a phase in this model?
Response:
A. Reconnaissance
B. Patch Management
C. Delivery
D. Exploitation
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which techniques can be used to prevent ARP cache poisoning attacks on a network?
(Choose two)
Response:
A. Disabling network segmentation
B. Enabling Dynamic ARP Inspection (DAI)
C. Implementing static ARP entries for critical devices
D. Increasing the number of VLANs
Answer: (SHOW ANSWER)

NEW QUESTION: 15
Why is credential rotation important in a Zero Trust framework?
Response:
A. It simplifies the user authentication process
B. It reduces the risk of credential compromise over time
C. It increases the complexity for users, enhancing security
D. It ensures that passwords are easy to remember
Answer: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following is the primary role of database firewalls in data-centric security?
Response:
A. Encrypting data during transmission

B. Backing up databases in real time
C. Protecting databases from unauthorized access and SQL injection attacks
D. Monitoring network traffic for anomalies
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following statements accurately describe IPv6 addressing?
(Choose two)
Response:
A. IPv6 allows for a significantly larger number of addresses compared to IPv4.
B. IPv6 uses dot-decimal notation.
C. IPv6 addresses are primarily used for network devices only.
D. IPv6 addresses are 128 bits in length.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which encryption protocol is commonly used to secure VPN connections over the internet?
Response:
A. SMTP
B. SNMP
C. TLS
D. IPsec
Answer: (SHOW ANSWER)

NEW QUESTION: 19
What is the primary purpose of a dual-stack system in IPv6 deployment?
Response:
A. To double the network speed by utilizing both IPv4 and IPv6
B. To provide redundancy in case one of the stacks fails
C. To support both IPv4 and IPv6 traffic simultaneously
D. To transition all network traffic from IPv4 to IPv6 immediately
Answer: (SHOW ANSWER)

NEW QUESTION: 20

Which is NOT a typical feature of a web application firewall (WAF)?

Response:

A. Direct access to user credentials

B. Customizable rule sets

C. Traffic monitoring and logging

D. Blocking of suspicious requests

Answer: A (LEAVE A REPLY)

NEW QUESTION: 21

Which of the following is a recommended mitigation for IPv6 router advertisement attacks?

Response:

A. Enabling MAC address filtering

B. Enabling router advertisement protection features on network devices

C. Increasing the number of subnets in the network

D. Disabling all IPv6 traffic on the network

Answer: (SHOW ANSWER)

NEW QUESTION: 22

How does software-defined networking (SDN) contribute to security architecture?

(Choose two)

Response:

A. By fixing all network vulnerabilities

B. By making network control more dynamic

C. By decreasing network visibility

D. By allowing centralized network policy management

Answer: (SHOW ANSWER)

NEW QUESTION: 23

How does a host-based Intrusion Detection System/Intrusion Prevention System (IDS/IPS) contribute to the security of Zero Trust Endpoints?

Response:

A. By encrypting data at rest and in transit

B. By serving as the primary firewall at the network perimeter

C. By generating excessive logs to deter attackers

D. By monitoring and analyzing system activities for signs of malicious actions

Answer: (SHOW ANSWER)

NEW QUESTION: 24

Perimeter-focused deficiencies highlight which of the following issues?

(Choose two)
Response:
A. Underestimating the importance of user awareness training
B. Overreliance on physical security measures
C. Ignoring the potential for insider threats
D. Excessive trust in perimeter security to block all attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 25
What is data discovery in the context of data governance?
Response:
A. Ignoring data privacy regulations
B. Removing all data from the network
C. Identifying and classifying data stored in various locations within an organization
D. Migrating all company data to the cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What role does mobility management play in data governance?
Response:
A. Manages the physical movement of data servers
B. Focuses only on data stored on desktop computers
C. Controls access to data through mobile devices and ensures data protection regardless of location
D. Ensures that mobile applications are entertaining
Answer: (SHOW ANSWER)

NEW QUESTION: 27
Which of the following is a key challenge in implementing Mobile Device Management (MDM) solutions?
Response:
A. Ensuring secure access to data from both managed and unmanaged devices
B. Managing data loss through email servers
C. Providing automatic encryption of all cloud data
D. Performing regular data audits on-premises
Answer: (SHOW ANSWER)

NEW QUESTION: 28
How does a Web proxy contribute to network security?
Response:
A. By allowing all traffic without inspection

B. By increasing the data transfer speeds
C. By providing a backup connection method
D. By filtering and monitoring internet traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 29
What is an IPv6 router advertisement attack?
Response:
A. An attack where an unauthorized node sends router advertisements to redirect IPv6 traffic
B. A type of network scan to discover hidden IPv6 routers
C. An attack that only affects dual-stack systems, leaving IPv6-only networks secure
D. An attack that targets the routing table of IPv4 routers exclusively
Answer: (SHOW ANSWER)

NEW QUESTION: 30
What is the primary function of Host Intrusion Detection Systems (HIDS) in endpoint security?
Response:

A. Detecting and alerting on potential threats and unauthorized changes to the endpoint
B. Monitoring network traffic for suspicious activity
C. Managing user authentication across the network
D. Encrypting data at rest on the endpoint
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Your organization has implemented a Zero Trust architecture to enhance network security. However, several systems are still relying on traditional perimeter defenses, which have become ineffective against advanced threats. To comply with the Zero Trust model, what immediate actions should your team prioritize to protect the organization's critical assets?
Response:
A. Implement micro-segmentation, enforce strong identity verification, and adopt the principle of least privilege
B. Upgrade perimeter firewalls and focus on reducing network traffic
C. Disable all access to internal systems and require manual approvals for every request
D. Decrease logging activities to focus on higher-priority events only
Answer: (SHOW ANSWER)

NEW QUESTION: 32
Your network team has detected unusual traffic between VLANs that should be isolated. After further investigation, they suspect a VLAN hopping attack. What immediate steps should you take to mitigate the attack and secure the network?
Response:
A. Perform a full network reboot to eliminate any lingering attack traces
B. Set up a new VLAN for all critical devices
C. Disable trunking on all unnecessary ports and configure unused ports as access ports
D. Allow unrestricted access to all VLANs for better monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 33
SMTP proxies are specifically used to secure which type of network traffic?
Response:
A. HTTP
B. Email
C. DNS
D. FTP
Answer: (SHOW ANSWER)

NEW QUESTION: 34
What is the purpose of 802.1X in securing Layer 2 networks?
Response:
A. Ensuring high network bandwidth
B. Preventing Distributed Denial of Service (DDoS) attacks
C. Authenticating devices trying to access the network
D. Encrypting all network traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 35
What is the primary purpose of a Data Loss Prevention (DLP) solution in a corporate environment?
Response:
A. Monitoring network traffic for anomalies
B. Detecting and preventing unauthorized data transfer
C. Encrypting sensitive data in transit
D. Automatically backing up critical files

Answer: (SHOW ANSWER)

NEW QUESTION: 36
In the context of Zero Trust, which of the following measures are effective in responding to pivoting adversaries?
(Select all that apply)
Response:
A. Isolating infected systems
B. Continuous monitoring of network activities
C. Regularly updating firewall rules
D. Implementing strict network access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which OSI model layer is synonymous with Layer 3 defense?
Response:
A. Managing application-specific communications over the network efficiently.
B. Facilitating data packet routing based on logical addressing and path determination.
C. Establishing network connections and providing error detection at the data link level.
D. Ensuring reliable data transfer with proper sequencing and error control mechanisms.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
What is the role of red herring defenses in Zero Trust Networking?
Response:
A. To confuse attackers by presenting false targets or information
B. To isolate domains within the network
C. To encrypt all network traffic
D. To provide authentication for endpoint traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 39
Which security controls help reduce the attack surface on endpoints in a Zero Trust environment?
(Choose two)
Response:
A. Applying regular security patches and updates
B. Implementing host-based firewalls
C. Allowing administrator access for all users
D. Disabling encryption to improve performance
Answer: (SHOW ANSWER)

NEW QUESTION: 40

Which of the following is a core benefit of using Network Intrusion Prevention Systems (NIPS)?
Response:

A. They are primarily used for data recovery.
B. They primarily focus on outbound traffic.
C. They can replace the need for traditional firewalls.
D. They can take direct action to block or prevent malicious activity.
Answer: (SHOW ANSWER)

NEW QUESTION: 41

Which techniques are effective for enhancing network security monitoring?
(Choose two)
Response:
A. Implementing deep packet inspection for detailed traffic analysis
B. Deploying Network Intrusion Prevention Systems (NIPS)
C. Using encryption for all inbound connections
D. Disabling all outbound traffic to prevent data leakage
Answer: (SHOW ANSWER)

NEW QUESTION: 42

Your organization is implementing Zero Trust Networking. During an internal audit, your team identifies a critical flaw in how endpoint traffic is authenticated before accessing sensitive resources. Several devices have bypassed authentication and are communicating with internal systems.
What immediate actions should you take to align with the Zero Trust Networking model and secure the network?
Response:
A. Implement Single Packet Authentication (SPA) for all devices and enforce endpoint traffic encryption
B. Allow unauthenticated devices to access non-critical systems while reviewing network configurations
C. Restrict all external traffic and allow internal traffic to continue without further verification
D. Disable all network traffic until a full security audit is completed
Answer: (SHOW ANSWER)

NEW QUESTION: 43

Zero Trust fundamentals include measures against insider threats, such as:
Response:
A. Allowing unrestricted data access
B. Ignoring abnormal access patterns
C. Conducting regular user activity reviews

D. Decreasing the use of encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 44
What is the primary goal of Zero Trust Networking?
Response:
A. To limit access to network resources based on predefined trust levels
B. To allow unrestricted access to devices once authenticated
C. To reduce encryption overhead on the network
D. To minimize the number of connected devices
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following is a core component of Zero Trust Architecture?
Response:
A. Network segmentation using firewalls
B. Credential rotation to reduce the risk of compromised credentials
C. Network perimeter security
D. Packet filtering based on port numbers
Answer: (SHOW ANSWER)

NEW QUESTION: 46
In the context of Zero Trust Endpoints, why is end-user privilege reduction considered a critical practice?
Response:
A. It reduces the attack surface by limiting access to critical resources
B. It ensures all users have admin privileges for transparency
C. It allows users to install any required software without IT intervention
D. It minimizes the risk of accidental data deletion by users
Answer: (SHOW ANSWER)

NEW QUESTION: 47

What aspects are crucial in a cloud-based security architecture for protecting data?
(Select all that apply)
Response:
A. Frequent password changes
B. Network traffic analysis
C. User education and awareness
D. Regular data backup
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which protocol is often targeted in Layer 3 attacks due to its use in time synchronization across networks?
Response:
A. HTTP
B. NTP
C. SNMP
D. SMTP
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Your organization has implemented a Zero Trust Architecture and is now focusing on protecting against insider threats. The security team has identified an employee using elevated privileges to access sensitive data they should not have.
What immediate steps should you take to comply with Zero Trust principles and prevent further unauthorized access?
Response:
A. Allow the employee continued access while performing a full security audit
B. Revoke the employee's elevated privileges, implement least privilege access, and monitor their activity for any further violations
C. Disable multi-factor authentication to simplify monitoring
D. Block all user traffic and disable access to the sensitive data for all employees
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which are valid approaches to implement NIDS?
(Choose two)
Response:

A. Disabling all network protocols
B. Anomaly-based detection
C. Signature-based detection
D. Ignoring all alerts

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 51
What is the primary benefit of implementing automated patch management within a Zero Trust Endpoint strategy?
Response:
A. Ensures timely application of patches, reducing the window of vulnerability
B. Automates backup processes only
C. Reduces the need for IT staff
D. Increases the complexity of the system, enhancing security through obscurity
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which strategies are effective for responding to pivoting adversaries in a Zero Trust model? (Choose two)
Response:
A. Disabling all network monitoring to avoid false positives
B. Enforcing strict credential rotation policies
C. Automatically trusting all previously authenticated devices
D. Implementing micro-segmentation to limit lateral movement
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Which of the following are effective measures to mitigate IPv6 router advertisement attacks? (Choose two)
Response:
A. Using digital signatures with router advertisements
B. Implementing RA Guard to validate router advertisement messages
C. Disabling IPv6 across the network
D. Isolating IPv6 traffic from IPv4 traffic
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 54
Which security mechanisms are used to mitigate VLAN hopping attacks? (Choose two)
Response:
A. Using ARP poisoning detection tools
B. Disabling unused ports and configuring them as access ports
C. Enforcing VLAN tagging
D. Allowing trunk ports on all switches
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 55
How does MAC spoofing pose a threat to network security?
Response:
A. It facilitates the unauthorized interception of network traffic.
B. It can disrupt the availability of network services.
C. It enhances the bandwidth allocation for an attacker's machine.
D. It directly compromises the encryption algorithms used on the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Your organization is planning to migrate several critical applications to a public cloud provider. You are tasked with ensuring security during and after the migration. What immediate steps should you take to secure the cloud-based infrastructure and protect your organization's data?
Response:
A. Focus only on encrypting data at rest, and leave IAM configuration for later
B. Establish Identity and Access Management (IAM) policies and enable encryption for all data
C. Disable multi-factor authentication to simplify access for employees
D. Rely on the cloud provider to secure the infrastructure entirely
Answer: (SHOW ANSWER)

NEW QUESTION: 57
Which of the following elements are fundamental to data-centric security?
(Choose two)
Response:
A. Conducting user awareness training to mitigate human error and enhance security culture.
B. Masking data to obscure sensitive information from unauthorized personnel.
C. Encrypting data to prevent unauthorized access and ensure its confidentiality.
D. Updating software regularly to defend against the latest cybersecurity threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
What is a primary security feature of next-generation firewalls?
Response:
A. They include integrated intrusion prevention.
B. They can only filter traffic based on IP addresses and ports.
C. They support only static routing.
D. They function identically to traditional stateful firewalls but are faster.
Answer: (SHOW ANSWER)

NEW QUESTION: 59

Which of the following are key features of a next-generation firewall (NGFW)?
(Choose two)
Response:
A. Application awareness and control
B. IP address filtering only
C. Deep packet inspection
D. Full disk encryption for all network devices
Answer: (SHOW ANSWER)

NEW QUESTION: 60
In cloud security, the shared responsibility model implies that:

Response:
A. Third-party providers take care of security
B. Customers are responsible for managing physical security
C. Cloud service providers handle the security of the infrastructure, while customers manage their own data
D. Cloud service providers manage all security responsibilities
Answer: (SHOW ANSWER)

NEW QUESTION: 61
Which of the following are best practices for securing remote access to corporate networks?
(Choose two)
Response:
A. Using multi-factor authentication (MFA) for all remote connections
B. Allowing unrestricted access to the network from personal devices
C. Disabling VPN encryption to reduce latency
D. Implementing a Jump Box for managing remote access
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 62
Which of the following are effective components of network security monitoring?
(Choose two)

Response:
A. Using only signature-based detection methods
B. Analyzing encrypted traffic without decryption
C. Continuously monitoring network traffic for suspicious activities
D. Identifying trends and patterns indicative of potential threats
Answer: (SHOW ANSWER)

NEW QUESTION: 63
In the context of DDOS protections, what is the purpose of rate limiting?
Response:
A. To restrict the number of requests a server accepts over a certain period
B. To allocate more resources to privileged users
C. To enhance the transmission speed
D. To ensure equal bandwidth distribution
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which of the following are considered best practices for secure remote access?
Response:
A. Using outdated encryption standards
B. Allowing unlimited access attempts
C. Enforcing strong authentication mechanisms
D. Regularly updating access policies
Answer: (SHOW ANSWER)

NEW QUESTION: 65
What is a Jump Box in the context of secure remote access?
Response:
A. A type of encryption software used to secure VPNs
B. A tool used to perform load balancing across multiple servers
C. A firewall used to protect internal network segments
D. A centralized server used to access and manage devices within a secure network
Answer: (SHOW ANSWER)

NEW QUESTION: 66
In a cloud-based security architecture, what is the role of network segmentation?
Response:
A. To enhance network bandwidth
B. To monitor web traffic for malicious activity
C. To separate sensitive workloads from less critical workloads, reducing the risk of lateral movement

D. To encrypt all data stored in the cloud
Answer: (SHOW ANSWER)

NEW QUESTION: 67
In the context of network proxies and firewalls, what is an essential characteristic of SMTP proxies?
Response:
A. They are primarily used to enhance the user interface of email applications.
B. They should enable all email attachments without scanning.
C. They increase the speed of email delivery.
D. They provide detailed analysis and filtering of email traffic to identify threats.
Answer: (SHOW ANSWER)

NEW QUESTION: 68
What does securing on-premise hypervisors help prevent in a cloud architecture?
Response:
A. Data breaches
B. Subscription fraud
C. Overprovisioning
D. Internet downtime
Answer: (SHOW ANSWER)

NEW QUESTION: 69
In the context of threat vector analysis, which of the following is true?
Response:
A. It ignores insider threats
B. It focuses exclusively on software vulnerabilities
C. It only considers external threats
D. It assesses the paths through which an organization could be attacked
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following is a core concept of Domain Isolation in Zero Trust Networking?

Response:
A. Segmenting networks based on geographical locations
B. Preventing unauthorized devices from communicating with sensitive resources
C. Increasing network speed by limiting encryption
D. Limiting internet access to specific domains
Answer: (SHOW ANSWER)

NEW QUESTION: 71

Which technique aims to authenticate users or devices based on individual packets rather than sessions?
Response:
A. Red herring defenses
B. Domain Isolation
C. Transport Layer Security (TLS)
D. Single Packet Authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 72
What is the primary purpose of Domain Isolation in Zero Trust Networking?
Response:
A. To consolidate all domains into a single management domain
B. To enhance the speed of network connectivity
C. To isolate and segment network resources based on trust levels
D. To unify different network domains for easier access
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Your organization has detected that several employees are accessing sensitive data on their mobile devices outside of approved locations. As the security architect, you need to address the governance and mobility management issues. What is the best course of action to protect the data while maintaining employee productivity?
Response:
A. Implement Mobile Device Management (MDM) with geofencing to restrict access to specific locations and enforce encryption policies on mobile devices
B. Ban all mobile devices from accessing company networks until further notice
C. Install antivirus software on all employee devices and monitor their data usage
D. Set up a network access control (NAC) solution to block all devices accessing corporate data remotely
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Encryption in network security serves to:
Response:
A. Prevent unauthorized data manipulation and eavesdropping.
B. Slow down the network.
C. Increase the network's latency.
D. Replace the need for a firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which of the following best defines the Zero Trust Model in security architecture?
Response:
A. Assuming every request is a potential security threat, even from within the network
B. Allowing all traffic from trusted devices without further checks
C. Prioritizing external threats over internal ones
D. Granting users full access to network resources once authenticated
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following are considered best practices when implementing secure remote access? (Choose two)
Response:
A. Ensuring end-to-end encryption
B. Using shared passwords for convenience
C. Allowing unlimited access from any location
D. Employing multi-factor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 77
What is the primary purpose of dual factor authentication for remote access VPNs?
Response:
A. To verify user identity with two different forms of authentication
B. To double the VPN throughput
C. To provide backup connectivity options
D. To allow twice as many users to connect
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Which principles are fundamental to data governance?
(Select all that apply)
Response:

A. Data Availability
B. Data Deletion after a set period
C. Data Consistency
D. Data Quality
Answer: (SHOW ANSWER)

NEW QUESTION: 79
What practices are vital for effective Layer 3 defense?
(Choose two)
Response:
A. Applying rigorous network monitoring to detect and respond to unusual traffic patterns swiftly.
B. Implementing access control lists (ACLs) to restrict unauthorized network traffic and enhance security.
C. Employing stateful packet inspection to analyze and filter packets based on established connections.
D. Designing a segmented network architecture to limit the spread of security breaches within the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which type of encryption is typically used to protect data in transit across a network?

Response:
A. AES-256 for database storage
B. SHA-256 for hashing
C. MD5 for verifying file integrity
D. TLS/SSL for securing communication channels
Answer: (SHOW ANSWER)

NEW QUESTION: 81
Which of the following is a security concern unique to IPv6 networks?
Response:
A. IP address exhaustion
B. Limited bandwidth
C. IPv6 address spoofing
D. Lack of subnetting capabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 82
When considering remote access security, why is it important to use dual factor authentication along with VPNs?
Response:

A. It provides a faster connection to the network.
B. It eliminates the need for encryption.
C. It simplifies the user login process.
D. It ensures that the user's device also participates in the authentication process.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
When securing network protocols like SNMP and NTP, it is crucial to:
Response:
A. Configure them with public access
B. Utilize the least secure versions
C. Ensure they are unmonitored
D. Apply strong authentication and encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 84
What are the key benefits of implementing Single Packet Authentication in Zero Trust Networking?
(Choose two)
Response:
A. It simplifies the credential management process
B. It minimizes the network's exposure to reconnaissance activities
C. It allows only authenticated packets to initiate connections
D. It enables the network to respond to authentication requests more slowly
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 85
In a Zero Trust Networking model, what is the primary role of Single Packet Authentication (SPA)?
Response:
A. Reducing the number of available IP addresses
B. Verifying and authenticating a device before allowing network access
C. Monitoring user behavior across the network
D. Encrypting data at rest
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which type of attack involves exploiting vulnerabilities in VLAN configurations to gain unauthorized access to other VLANs?
Response:
A. VLAN hopping

B. DNS poisoning
C. ARP cache poisoning
D. MAC flooding
Answer: (SHOW ANSWER)

NEW QUESTION: 87
Which of the following are considered essential features of cloud-based security architecture? (Select all that apply)
Response:
A. Encryption of data at rest and in transit
B. Identity and access management (IAM)
C. Distributed Denial of Service (DDoS) mitigation
D. Physical security measures
Answer: (SHOW ANSWER)

NEW QUESTION: 88
What is the primary goal of file classification in data governance?
Response:
A. Improving data security and compliance
B. Enhancing data retrieval speed
C. Reducing the effectiveness of encryption
D. Increasing storage requirements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 89
How do jump boxes contribute to network security?
Response:
A. They provide direct Internet access.
B. They increase the network's attack surface.
C. They decrease the need for monitoring.
D. They offer a single point of access for administrative tasks.
Answer: (SHOW ANSWER)