ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

An organization is experiencing a high volume of phishing attacks and malware downloads. The cybersecurity team wants to deploy a firewall to enhance their threat prevention system. Which type of firewall deployment would provide the most effective protection against such threats?

A. Open-source firewall with no subscription to threat intelligence feeds
B. Host-based firewall on individual endpoints
C. Transparent firewall with minimal configuration
D. Network-based firewall with URL filtering

Answer: D

Question: 2

An organization is building a robust threat prevention system to protect its cloud environment. They are evaluating various tools and practices to detect and block advanced persistent threats (APTs) and ransomware attacks. Which two components should be included in their threat prevention system? (Choose two)

A. Endpoint Detection and Response (EDR) tools
B. Manually reviewing log files once a year
C. Web application firewalls (WAFs)
D. Disabling software updates for stability
E. Continuous monitoring of network traffic

Answer: A, C

Question: 3

Which of the following is an example of an effective practice to enhance end-user cybersecurity awareness?

A. Providing one-time training during employee onboarding with no follow-up.
B. Sending monthly cybersecurity newsletters highlighting recent incidents and prevention tips.
C. Requiring employees to memorize a list of known malware names.
D. Allowing employees to choose their own cybersecurity training schedule with no deadlines.

Answer: B

Question: 4

Which of the following best describes the role of Continuous Integration (CI) in the CI/CD pipeline for cloud security?

A. Monitoring runtime behavior of applications in production to identify security vulnerabilities.
B. Encrypting sensitive data during the software development process to prevent unauthorized access.
C. Ensuring that code changes are automatically built, tested, and integrated into a shared repository.
D. Automating the deployment of applications into production environments with minimal human intervention.

Answer: C

Question: 5

You are configuring a network for a medium-sized enterprise. The goal is to separate different departments (e.g., HR, IT, Sales) using network segmentation while ensuring efficient utilization of IP addresses and controlling traffic flow between segments. Which of the following methods is the most appropriate to achieve this goal?

A. Configure the network to use a flat IP addressing scheme, where all devices share the same subnet, and implement ACLs to control traffic.
B. Divide the network into multiple IP subnets, assigning a unique subnet to each department and using VLANs to implement segmentation.
C. Deploy a single large subnet for all departments and rely on firewalls to inspect and control inter-department traffic.
D. Create different IP subnets for each department and assign devices to subnets based on IP ranges but without VLANs.

Answer: B

Question: 6

Which of the following is a key characteristic of Software as a Service (SaaS)?

A. The customer is responsible for updating and patching the software.
B. The customer has complete control over the underlying infrastructure.
C. The service provider manages the application, infrastructure, and platform.
D. The service is installed on the customer's on-premises hardware.

Answer: C

Question: 7

A company network experiences a sudden spike in unusual network activity. Upon investigation, analysts discover an unauthorized proxy server that is intercepting employee traffic and decrypting HTTPS communications. What method might the attacker have used to facilitate this type of Man-in-the- Middle (MITM) attack?

A. SQL Injection
B. Brute force attack
C. SSL/TLS certificate spoofing
D. Cross-Site Scripting (XSS)

Answer: C

Question: 8

An organization using Kubernetes clusters for a microservices-based application has recently experienced a security breach. The security team identified that weak cluster configurations allowed attackers to exploit vulnerabilities in the environment. Which of the following actions best strengthens the security of a Kubernetes cluster?

A. Allowing pods to share service account credentials.
B. Restricting pod communication using network policies.
C. Deploying outdated versions of Kubernetes to maintain compatibility with legacy applications.
D. Disabling encryption for Kubernetes secrets to reduce overhead.

Answer: B

Question: 9

Which of the following is the primary focus of the "Actions on the Objective" stage in the cyberattack lifecycle?

A. Achieving the intended goal of the attack, such as data theft or disruption
B. Deploying the malicious payload onto the target system
C. Navigating through a compromised network to identify valuable assets
D. Establishing a persistent connection to the target system

Answer: A

Question: 10

You are configuring a Palo Alto Networks firewall for an organization. The goal is to allow inbound traffic from a trusted partner's IP range (192.168.10.0/24) to access the organization's web server on port 443 securely. At the same time, you must block all other traffic from untrusted external sources to the web server. Which two actions correctly configure the firewall rules to meet the requirements? (Choose two)

A. Enable bidirectional traffic for port 80 from all external IP addresses.
B. Create an inbound allow rule permitting traffic from 192.168.10.0/24 to the web server on port 443.
C. Set up a default deny-all inbound rule for all untrusted traffic to the web server.
D. Configure SSL decryption for all inbound traffic to the web server.
E. Enable NAT for the web server with a static one-to-one IP mapping.

Answer: B, C

Question: 11

Which of the following best describes the responsibilities of the cloud service provider (CSP) and the customer in the Infrastructure as a Service (IaaS) cloud service model?

A. The CSP takes full responsibility for all aspects of security, including operating systems,

applications, and customer data.
B. The CSP manages the underlying physical infrastructure, including networking and servers, while the customer is responsible for managing the operating system, middleware, and applications.
C. The CSP manages physical security and application security, while the customer is responsible for networking and hardware.
D. The CSP is responsible for securing the application data, while the customer is responsible for maintaining the physical hardware.

Answer: B

Question: 12

Which of the following capabilities is unique to next-generation firewalls (NGFWs) when compared to stateful firewalls?

A. Maintaining connection states for active sessions.
B. Performing NAT (Network Address Translation) to enable private IP communication.
C. Deep packet inspection to identify applications regardless of port number.
D. Packet filtering based on source and destination IPs and ports.

Answer: C

Question: 13

Which two components of endpoint security are essential for detecting and preventing advanced persistent threats (APTs) on a device? (Choose two)

A. Network Firewall
B. Behavioral Analysis Engine
C. Endpoint Detection and Response (EDR)
D. Spam Filtering
E. Signature-Based Antivirus

Answer: B, C

Question: 14

Which of the following terms is most accurately associated with the DevSecOps practice of integrating security into software development workflows?

A. Shift-Left Security, which incorporates security practices early in the development lifecycle.

B. Waterfall Model, focusing on security testing at the final stage of the development cycle.
C. Code Refactoring, which focuses solely on improving code readability and performance, not security.
D. Continuous Integration (CI) without security checks to ensure faster builds.

Answer: A

Question: 15

You are tasked with recommending a cloud deployment model for a new application that must run in an environment shared by multiple organizations but is not publicly accessible. Which of the following cloud deployment models best fits the requirement?

A. Private Cloud
B. Multicloud
C. Public Cloud
D. Community Cloud

Answer: D

Question: 16

Your organization is implementing URL filtering to enhance network security and prevent access to malicious or inappropriate websites. As a security administrator, you must configure URL filtering policies to meet the organization's requirements. Which of the following statements accurately describe the function of URL filtering in network security? (Choose two)

A. URL filtering helps enforce compliance by restricting access to websites that violate regulatory requirements.
B. URL filtering inspects the payload of HTTPS traffic to identify and block malicious files within the website.
C. URL filtering dynamically generates new URL categories based on machine learning models in real time.
D. URL filtering operates solely based on IP addresses and cannot analyze domain names or URLs.
E. URL filtering can block access to websites based on their content categories, such as gambling or adult content.

Answer: A, E

Question: 17

During a Security Operations Center (SOC) analysis, an analyst identifies an unusual outbound connection from a corporate endpoint to a suspicious IP address in a foreign country. What should be the first step the analyst takes as part of the incident response process?

A. Submit the suspicious IP address to a public malware database without internal escalation.
B. Immediately disconnect the endpoint from the network.
C. Block the suspicious IP address at the firewall without further analysis.
D. Validate the alert by correlating it with other logs and threat intelligence sources.

Answer: D

Question: 18

A medium-sized organization migrates its workloads to a public cloud provider. The IT manager is unsure about which security responsibilities remain with the organization and which are handled by the cloud provider. The manager seeks to clarify their responsibilities under the shared responsibility model. Under the shared responsibility model in a public cloud environment, which of the following is the organization's responsibility?

A. Maintaining the underlying hardware of the cloud infrastructure.
B. Ensuring the physical security of the cloud provider's data centers.
C. Managing identity and access policies for user accounts within the organization.
D. Configuring firewalls to secure their virtual machines.

Answer: D

Question: 19

A cybersecurity analyst is investigating a suspected breach. The analysis reveals that attackers exploited a misconfigured cloud storage bucket to upload malicious scripts, which subsequently allowed them to gain unauthorized access to sensitive data. Which of the following best describes the exploitation method used in this scenario?

A. Delivering a zero-day exploit to bypass endpoint defenses
B. Exploitation of a misconfigured cloud storage bucket
C. Establishing a Command and Control channel through malware
D. Phishing email containing a malicious link

Answer: B

Question: 20

A company is looking for a cloud service model where they can quickly adopt tools like email, customer relationship management (CRM), and collaboration platforms without investing in infrastructure or maintenance. Which cloud service model best fits their needs?

A. Database as a Service (DBaaS)
B. Infrastructure as a Service (IaaS)
C. Platform as a Service (PaaS)
D. Software as a Service (SaaS)

Answer: D

Question: 21

Which of the following statements correctly differentiates between routed protocols and routing protocols in the context of network communication?

A. Routing protocols enable routers to exchange information and determine optimal paths, whereas

routed protocols are the data-carrying protocols transmitted over the network.
B. Routed protocols determine the next-hop router for forwarding packets, while routing protocols are used to encapsulate data into packets.
C. Routed protocols dynamically adjust network paths during failures, whereas routing protocols establish static paths between devices.
D. Routed protocols are used to discover the best path for data transmission, while routing protocols define the structure and syntax of data packets.

Answer: A

Question: 22

Which of the following is a core feature of a Cloud Native Security Platform (CNSP)?

A. Direct integration with on-premises physical firewalls for cloud-based traffic routing.
B. Exclusive reliance on static rule-based policies for threat detection.
C. Automatic detection and remediation of security misconfigurations across cloud-native resources.
D. Limiting security coverage to virtual machines in multi-cloud environments.

Answer: C

Question: 23

A cybersecurity team is designing a network architecture based on the Zero Trust model. Which of the following principles is most fundamental to the Zero Trust framework?

A. Rely on endpoint antivirus software as the primary defense mechanism.
B. Allow all internal traffic by default and monitor external traffic closely.
C. Authenticate and authorize every request, regardless of its source.
D. Build trust by analyzing historical data and establishing traffic baselines.

Answer: C

Question: 24

Which of the following best describes an activity performed during the exploitation stage of the cyberattack lifecycle?

A. A zero-day vulnerability in the target system is leveraged to gain unauthorized access.
B. A backdoor is installed on a compromised host for persistent access.
C. The attacker analyzes the organization's publicly available DNS records to identify key systems.
D. A phishing email is sent to a user, tricking them into clicking on a malicious link.

Answer: A

Question: 25

Which of the following is the most accurate example of a "security event" in a typical network environment?

A. A firewall detects and blocks a brute-force attack attempt on a login portal.
B. A user accesses their email account using valid credentials.
C. A Distributed Denial of Service (DDoS) attack disrupts a company's public-facing website.
D. An attacker exfiltrates sensitive data from a database using a SQL injection vulnerability.

Answer: B

Question: 26

Which of the following best defines the term "API" in the context of cloud security?

A. A virtual network component that connects cloud resources securely across regions.
B. A set of programming interfaces that enable applications to interact with cloud services.
C. A secure communication protocol used exclusively for encrypting cloud-based data transfers.
D. A user interface that allows end-users to manage cloud services through graphical tools.

Answer: B

Question: 27

Which endpoint security technology is most effective in preventing zero-day malware attacks by monitoring and analyzing system behavior in real-time?

A. Intrusion Detection System (IDS)
B. Endpoint Detection and Response (EDR)
C. Antivirus Software
D. Network Access Control (NAC)

Answer: B

Question: 28

A computer in a local network is configured with an IP address of 192.168.1.10 and a subnet mask of 255.255.255.0. It attempts to communicate with a web server at 203.0.113.5. What role does the default gateway play in this communication?

A. The default gateway blocks packets that are not explicitly permitted by a local firewall rule.
B. The default gateway resolves the domain name of the web server into its IP address.
C. The default gateway forwards packets destined for IP addresses outside the local subnet.
D. The default gateway assigns a new IP address to the computer for external communication.

Answer: C

Question: 29

Which of the following best describes the primary characteristic of a Trojan in a cybersecurity context?

A. A program that disguises itself as legitimate software to perform malicious activities
B. A tool used for intercepting and logging keystrokes on a victim’s machine
C. A program that encrypts files on a system and demands payment for their release

D. A self-replicating program designed to spread across networks

Answer: A

Question: 30

A company is evaluating an antivirus solution for its hybrid environment, which includes on-premises systems and cloud-hosted workloads. The chosen antivirus must meet the following requirements: Detect known and unknown threats.
Minimize performance overhead.
Provide centralized management for all devices.
Which type of antivirus solution would best meet the company's needs?

A. A cloud-based antivirus solution with heuristic and behavioral analysis.
B. An antivirus solution that focuses solely on cloud-hosted workloads.
C. A traditional signature-based antivirus solution.
D. An open-source antivirus solution that offers manual configuration.

Answer: A

Question: 31

Which of the following statements best describes the role of a host-based firewall in endpoint security?

A. A host-based firewall is only effective if paired with an intrusion prevention system (IPS).
B. A host-based firewall only protects against malware infections on the endpoint by scanning downloaded files.
C. A host-based firewall filters traffic entering and leaving an individual endpoint based on predefined security rules.
D. A host-based firewall protects the entire network by analyzing and blocking malicious traffic at the network perimeter.

Answer: C

Question: 32

What is a common method attackers use to deliver a Trojan to unsuspecting users?

A. Exploiting an unpatched vulnerability in the target system
B. Sending a phishing email with a link to a fake login page
C. Performing a brute-force attack to guess user passwords
D. Embedding the Trojan in a seemingly legitimate software download

Answer: D

Question: 33

A company is concerned about employees accessing unauthorized websites during work hours, potentially exposing the organization to security risks or productivity loss. Which of the following best describes the primary function of URL filtering in a network security solution?

A. Monitoring user activity on the network without enforcing restrictions. B. Blocking all external traffic to the internet to prevent malware attacks.
C. Encrypting web traffic to ensure secure communication with websites. D. Allowing or denying access to websites based on their categorization.

Answer: D

Question: 34

Which of the following best describes the primary function of a Data Loss Prevention (DLP) system in network security?

A. Blocking malicious incoming traffic from reaching the organization's internal network.
B. Monitoring user activity to identify suspicious behavior based on login patterns.
C. Detecting and blocking unauthorized attempts to transmit sensitive data outside the organization.
D. Encrypting data at rest and in transit to protect it from unauthorized access.

Answer: C

Question: 35

Which of the following scenarios best demonstrates the use of NAT?

A. A web server hosting a public website is directly assigned a static public IP address for global access.
B. An organization uses a single public IP address for all employee devices to access the internet.
C. A firewall encrypts incoming and outgoing traffic to protect against external threats.
D. A private IP address is assigned to each employee device for local communication only, without internet access.

Answer: B

Question: 36

Which of the following is a key pillar of effective security operations and ensures that organizations can proactively identify and respond to potential threats?

A. Threat Intelligence Integration
B. Patch Management
C. Incident Response
D. Disaster Recovery Planning

Answer: A

Question: 37

Which of the following characteristics is most accurate in distinguishing Internet of Things (IoT) devices from traditional computing endpoints in the context of endpoint security?

A. IoT devices inherently include robust security features such as endpoint detection and response (EDR).
B. IoT devices are typically managed using standard operating systems like Windows or macOS.
C. IoT devices are primarily designed for specific, limited functions, unlike general-purpose endpoints.
D. IoT devices communicate exclusively over proprietary protocols, making them incompatible with standard network infrastructure.

Answer: C

Question: 38

A network administrator is configuring a corporate network and needs to implement both routed and routing protocols. Which of the following combinations of actions correctly demonstrates the roles of these protocols?

A. Using IP as the data-carrying protocol and EIGRP to determine the best path between network segments.
B. Using OSPF to encapsulate data and IP to determine the best path for delivery.
C. Configuring TCP/IP to establish routes and using MPLS as a routing protocol.
D. Configuring BGP to carry data between routers and TCP to exchange routing information.

Answer: A

Question: 39

Which of the following best describes cloud orchestration in the context of modern cloud security?

A. Automating the deployment, scaling, and management of cloud infrastructure across multiple environments using a single unified interface.
B. Provisioning cloud storage services manually for high-availability architectures.
C. Automating the detection of cloud security breaches without requiring manual intervention.
D. Synchronizing security policies across on-premise and cloud systems using manual configurations.

Answer: A

Question: 40

Which of the following is a key advantage of using syslog in a security operations center (SOC)?

A. It uses artificial intelligence to automatically correlate and prioritize security alerts.
B. It provides real-time detection and prevention of threats across the network.

C. It operates exclusively within a single operating system, offering highly specialized insights.
D. It enables centralized logging and standardizes log message formats from multiple devices.

Answer: D

Question: 41

Which two of the following statements accurately describe characteristics of network segmentation methods in securing an enterprise network? (Choose two)

A. Macrosegmentation divides the network into physical segments using firewalls for perimeter-level traffic inspection.
B. Macrosegmentation relies on virtual LANs (VLANs) to separate traffic within a single switch or router.
C. Microsegmentation requires software-defined networking (SDN) to implement granular traffic control.
D. Microsegmentation can only operate in on-premises environments and is not suited for hybrid cloud models.
E. Microsegmentation enforces security policies at the application layer for greater control over inter-host communication.

Answer: C, E

Question: 42

An organization experiences an attack in which an employee unknowingly downloads a malicious program disguised as a legitimate software update. Once installed, the program monitors the user's keystrokes, capturing sensitive information like login credentials and financial details. What type of malware is being described in this scenario?

A. Ransomware
B. Trojan
C. Spyware
D. Worm

Answer: C

Question: 43

A network administrator notices that devices within the same subnet (192.168.10.0/24) are unable to communicate directly with each other and instead route their traffic through the default gateway. What is

the most likely explanation for this behavior?

A. The devices have incorrect DNS server configurations, forcing traffic through the gateway.
B. The switch connecting the devices is operating at Layer 3 instead of Layer 2.
C. The default gateway is overriding all device communications, regardless of their destination.
D. The subnet mask is misconfigured, causing the devices to misidentify their network range.

Answer: D

Question: 44

Which of the following best describes the role of visibility as a pillar of effective security operations?

A. Ensuring that all logs and security events are collected and stored for compliance reporting.
B. Providing actionable insights by centralizing data from various security tools and environments.
C. Guaranteeing 24/7 staffing of a Security Operations Center (SOC).
D. Isolating critical servers from external networks for enhanced protection.

Answer: B

Question: 45

A financial institution discovers that one of its web applications does not validate user input correctly, allowing attackers to execute arbitrary SQL queries. Which of the following statements correctly identifies this issue and provides relevant details about vulnerabilities and exploits? (Choose two)

A. The issue is an example of a vulnerability because it represents a weakness in the application that could be exploited.
B. Such vulnerabilities are rare and unlikely to appear in modern web applications using frameworks.
C. An exploit for this vulnerability would involve using crafted SQL statements to bypass authentication mechanisms.
D. This issue is an exploit because it actively describes an attacker's use of SQL injection to extract sensitive data.

Answer: A, D

Question: 46

An organization stores sensitive customer data in a cloud storage service. The compliance officer is concerned about protecting this data against unauthorized access during both storage and transmission. Which method best ensures data security for sensitive information stored in a public cloud environment?

A. Using shared cloud storage buckets with public access for convenience.
B. Relying on the cloud provider's default security policies without additional configuration.
C. Storing sensitive data in plaintext for easy access and performance optimization.
D. Encrypting data at rest and using SSL/TLS for data in transit.

Answer: D

Question: 47

Which two stages of the cyberattack lifecycle involve gaining and maintaining unauthorized access to a target system? (Choose two)

A. Exploitation
B. Installation
C. Lateral Movement

D. Delivery
E. Reconnaissance

Answer: A, B

Question: 48

Which of the following activities is most representative of the installation stage of the cyberattack lifecycle?

A. Scanning a target network for open ports and vulnerable services.
B. Deploying a remote access Trojan (RAT) on a compromised system.
C. Exfiltrating sensitive data to an external attacker-controlled server.
D. Phishing a user to trick them into entering their login credentials.

Answer: B

Question: 49

A company is building a cloud-native application and wants to secure its infrastructure, software development practices, and containerized workloads. Which of the following combinations best represents the four Cs of cloud-native security?

A. Code, Containers, Cloud, Cluster
B. Cryptography, Cloud, Code, Configuration
C. Cloud, Containers, Configuration, Compliance
D. Cluster, Configuration, Cryptography, Containers

Answer: A

Question: 50

What is the primary role of APIs in cloud security?

A. To replace traditional firewalls in cloud-based environments.
B. To monitor real-time data flow between different cloud regions for anomalies.
C. To provide a method for applications to securely interact with cloud resources.
D. To create backup snapshots of critical cloud resources for disaster recovery.

Answer: C

Question: 51

A cybersecurity analyst is configuring a Security Information and Event Management (SIEM) solution for an organization. Which of the following best describes a primary function of a SIEM in security operations?

A. Automatically blocking malicious IP addresses in real time.
B. Performing vulnerability scans and generating patch recommendations.
C. Conducting penetration tests to assess the effectiveness of security controls.

D. Correlating and analyzing logs from multiple sources to detect potential threats.

Answer: D

Question: 52

Which of the following scenarios demonstrates the proper use of a host-based firewall in securing an endpoint?

A. Blocking unauthorized devices from connecting to the corporate Wi-Fi network.
B. Encrypting endpoint data before it is transmitted over the network.
C. Allowing only specific applications on the endpoint to access the internet based on security policies.
D. Preventing distributed denial-of-service (DDoS) attacks by analyzing traffic patterns across the network.

Answer: C

Question: 53

Which of the following best describes how a Security Information and Event Management (SIEM) system improves security operations?

A. SIEM tools replace the need for manual threat hunting by automating all security tasks.
B. SIEM tools passively collect logs without analyzing them, ensuring compliance.
C. SIEM tools provide log aggregation, correlation, and alerting to identify threats in real time.
D. SIEM tools detect malware and automatically remove infected files from endpoints.

Answer: C

Question: 54

Which of the following best describes the primary responsibility of securing "Code" in the context of the four Cs of cloud native security?

A. The customer ensures that the CSP scans the application code for vulnerabilities.
B. The customer writes secure code and integrates automated security checks into the CI/CD pipeline.
C. The CSP is responsible for encrypting the code and ensuring it is free of vulnerabilities.
D. The CSP patches the application code provided by the customer to resolve security issues.

Answer: B

Question: 55

A company wants to enhance its security posture by identifying malicious activities embedded in encrypted web traffic. Which firewall feature is required for this functionality, and which firewall type supports it?

A. Port-based traffic filtering supported by stateful firewalls.

B. URL filtering supported by stateful firewalls.
C. Deep packet inspection with SSL/TLS decryption supported by next-generation firewalls.
D. Session-based filtering supported by stateful firewalls.

Answer: C

Question: 56

You are configuring a DNS server and need to map a domain name (example.com) to its corresponding IP address (203.0.113.10). Which DNS record type should you use?

A. A Record
B. PTR Record
C. CNAME Record
D. MX Record

Answer: A

Question: 57

You are a cybersecurity apprentice tasked with identifying phishing variants during a simulated attack in your organization's email system. Below are descriptions of email-based attack types. Your task is to identify two correct examples of phishing variants. Which two of the following are examples of phishing? (Choose two)

A. Man-in-the-middle attack
C. Spear phishing
D. Vishing
E. Business Email Compromise (BEC)
F. Watering hole attack

Answer: B, D

Question: 58

What is the primary role of the "people" pillar in effective security operations?

A. To automate repetitive tasks and minimize manual effort in security operations
B. To ensure the deployment of advanced security tools and technologies
C. To exclusively focus on threat hunting and vulnerability assessments
D. To manage incident response workflows and enable collaboration across teams

Answer: D

Question: 59

In the Software as a Service (SaaS) cloud service model, which of the following best describes the customer's responsibilities?

A. The customer uses the application as provided by the CSP and is only responsible for managing user access and data input.
B. The customer is responsible for securing the application and managing the underlying operating system.
C. The customer is responsible for patching the operating system and ensuring the application meets regulatory compliance.
D. The customer uses the application provided by the CSP but must configure and manage the application's backend infrastructure.

Answer: A

Question: 60

Which two endpoint security components are crucial for preventing malware propagation and mitigating post-exploitation activities? (Choose two)

A. Privilege Management
B. Threat Intelligence Integration
C. Application Whitelisting
D. Host-Based Firewall
E. Intrusion Detection System (IDS)

Answer: A, C

Question: 61

Your company wants to deploy a cloud-based application that requires dynamic scalability for web traffic while maintaining sensitive customer data in an on-premises data center. Which deployment model should you recommend?

A. Hybrid Cloud
B. Multicloud
C. Private Cloud
D. Public Cloud

Answer: A

Question: 62

Which of the following best describes the primary function of a Network-Based Intrusion Detection System (NIDS) in a cybersecurity environment?

A. Blocking malicious IP addresses to prevent unauthorized access
B. Monitoring network traffic for malicious activity in real-time
C. Encrypting sensitive data for secure transmission
D. Preventing unauthorized changes to files on a server

Answer: B

Question: 63

Which of the following is not a key phase of an effective Incident Response (IR) plan?

A. Preparation
B. Detection and Analysis
C. Containment, Eradication, and Recovery
D. Asset Procurement

Answer: D

Question: 64

Which statement accurately describes the relationship between the TCP/IP model and the OSI model?

A. The OSI model's Transport layer is divided into two layers in the TCP/IP model: Connection layer and Flow layer.
B. The TCP/IP model has seven layers that directly correspond to the OSI model's layers.
C. The OSI model does not include a Network layer, while the TCP/IP model does.
D. The TCP/IP model's Application layer combines the OSI model's Application, Presentation, and Session layers.

Answer: D

Question: 65

An organization implementing Zero Trust finds it challenging to manage user and device access to sensitive applications. Which of the following best aligns with the Zero Trust purpose and practices for overcoming this challenge?

A. Grant all employees access to sensitive applications during business hours.
B. Use network segmentation to isolate sensitive applications from other traffic.
C. Deploy a VPN for employees to securely access all company resources.
D. Implement continuous monitoring and least privilege access controls.

Answer: D

Question: 66

A global manufacturing company has offices in multiple countries. They want to interconnect their sites to enable seamless communication and data sharing while ensuring high reliability and security. Which type of network best suits their needs?

A. Wide Area Network (WAN)
B. Metropolitan Area Network (MAN)
C. Personal Area Network (PAN)
D. Local Area Network (LAN)

Answer: A

Question: 67

An organization is implementing endpoint security for its remote workforce. The solution must include encryption, device compliance checks, and protection against phishing. Which solution best meets these requirements?

A. Security Information and Event Management (SIEM)
B. Next-Generation Firewall (NGFW)
C. Unified Threat Management (UTM)
D. Endpoint Protection Platform (EPP)

Answer: D

Question: 68

Which of the following best describes a primary objective of a ransomware attack?

A. To exfiltrate sensitive data without alerting the user
B. To secretly monitor user activity on a compromised system
C. To use compromised systems for sending phishing emails
D. To encrypt files on a victim's system and demand payment for decryption

Answer: D

Question: 69

Which of the following tools is most commonly used for cloud orchestration and aligns with cloud security best practices?

A. Postman
B. Splunk
C. Wireshark
D. Terraform

Answer: D

Question: 70

An organization implements IoT devices, such as smart thermostats and IP cameras, alongside traditional endpoints, like laptops and desktops. Which of the following best describes a primary security challenge unique to IoT devices compared to traditional endpoints?

A. IoT devices often lack direct update mechanisms, increasing their vulnerability to security exploits.
B. IoT devices are isolated from network traffic, eliminating risks from external threats.
C. IoT devices require user authentication for every operation, making them more secure than traditional endpoints.
D. IoT devices are protected by advanced encryption methods, unlike traditional endpoints.

Answer: A

Question: 71

Which of the following best describes a typical behavior of spyware?

A. Exploits vulnerabilities in a device to install additional malware without user consent.
B. Collects sensitive information from the victim's device and sends it to a third party.
C. Encrypts files on the victim's device and demands payment for their release.
D. Deletes critical system files to render the device inoperable.

Answer: B

Question: 72

You are troubleshooting a network issue where users are unable to access websites using domain names but can access them using IP addresses. Which function of DNS is most relevant to resolving this issue?

A. DNS is responsible for assigning IP addresses to devices.
B. DNS ensures encrypted communication between devices.
C. DNS provides domain-to-IP address resolution.
D. DNS converts IP addresses to MAC addresses.

Answer: C

Question: 73

A company has implemented a zone-based firewall to segment its network. Which traffic flow would most likely require a specific security policy to be defined?

A. Traffic between a trusted zone and an untrusted zone.
B. Traffic between devices within the same VLAN.
C. Traffic between endpoints on the same subnet.
D. Traffic between devices in the same zone.

Answer: A

Question: 74

An organization implements URL filtering to block high-risk websites. During a review of the network logs, the security team discovers users are accessing malicious websites via encrypted HTTPS connections. Which additional feature is critical to ensure effective URL filtering in this scenario?

A. Using intrusion detection systems (IDS) to monitor network traffic.
B. Configuring IP blacklists to block access to malicious IP addresses.
C. Implementing SSL/TLS decryption to inspect encrypted traffic.
D. Enabling DNS filtering to block domains before resolving IP addresses.

Answer: C

Question: 75

A company deploys a Data Loss Prevention (DLP) solution to secure sensitive data. Which of the following scenarios would trigger the DLP system to take action?

A. An employee attempts to upload a file containing customer PII to a personal cloud storage service.
B. An IT administrator encrypts a file containing sensitive information before transferring it internally.
C. An external hacker tries to exploit a vulnerability in the company's web server.
D. A marketing team member shares an internal campaign plan via the company's approved email system.

Answer: A

Question: 76

What is the primary purpose of a demilitarized zone (DMZ) in a network architecture?

A. To replicate a backup of the internal network for disaster recovery purposes.
B. To isolate internal systems from external systems while providing controlled access to public-facing services.
C. To enable unrestricted communication between internal and external networks.
D. To act as a secure area for storing sensitive data that must not be accessed externally.

Answer: B

Question: 77

A financial organization is developing its Security Operations strategy. They need to ensure it aligns with the key pillars of effective security operations while addressing business objectives. Which of the following measures best demonstrates aligning security operations with business priorities?

A. Implementing a threat intelligence system that focuses only on external attacks, disregarding internal risks.
B. Establishing a process for the Security Operations Center (SOC) to assess risks based on business-critical assets and prioritizing incident responses accordingly.
C. Conducting security drills with only the IT team and excluding non-technical business stakeholders.
D. Regularly updating firewalls to meet compliance requirements without engaging other business units.

Answer: B

Question: 78

What capability best describes the role of a Cloud Native Security Platform (CNSP) in enhancing security for cloud-native applications?

A. Providing security for containerized workloads, Kubernetes, and serverless functions across cloud environments.
B. Replacing endpoint detection and response (EDR) tools with cloud-native alternatives.
C. Offering manual tools for incident response without automation or orchestration.
D. Managing cloud provider billing for improved financial transparency.

Answer: A

Question: 79

A cybersecurity team deploys an Intrusion Prevention System (IPS) to enhance their threat prevention capabilities. Soon after deployment, they notice that legitimate traffic is being blocked. What is the most likely cause of this issue?

A. Incorrect user access permissions
B. Overly strict IPS signature rules
C. Firewall misconfigurations
D. Lack of encryption on the network

Answer: B

Question: 80

Which of the following best explains the primary difference between Continuous Delivery and Continuous Deployment (CD) in the context of cloud security?

A. Continuous Delivery ensures automated deployment into production, while Continuous Deployment requires manual approval before deployment.
B. Continuous Delivery includes security scanning of deployed applications, while Continuous Deployment automates security patching of infrastructure.
C. Continuous Delivery focuses on delivering changes to a staging environment, while Continuous Deployment automatically deploys changes into production.
D. Continuous Delivery is used exclusively in private clouds, while Continuous Deployment is specific to public clouds.

Answer: C

Question: 81

A company wants to secure remote access for its employees working from home by using a VPN. Which of the following best describes how a VPN provides security for remote communication?

A. Ensures all communications use a private IP addressing scheme, preventing exposure to public networks.
B. Blocks unauthorized access by configuring firewall rules on the client device.
C. Encrypts data between the client and the server, making it unreadable to attackers during transit.
D. Replaces the user's IP address with the IP address of the VPN server to anonymize traffic without encrypting it.

Answer: C

Question: 82

Which of the following best explains the role of a Security Orchestration, Automation, and Response (SOAR) platform in security operations?

A. Replacing human analysts entirely by using AI-driven automation.
B. Automating repetitive tasks such as phishing email triage to improve incident response efficiency.
C. Generating compliance reports by analyzing security device configurations.
D. Centralizing the storage of security logs for long-term retention.

Answer: B

Question: 83

Which of the following best describes a Wide Area Network (WAN)?

A. A network that connects devices wirelessly within a limited range, such as a home or office.
B. A network designed to connect devices within a single building or campus.
C. A network that spans large geographical areas, often connecting multiple local area networks (LANs).
D. A network limited to a specific metropolitan area, providing high-speed connections.

Answer: C

Question: 84

Which of the following correctly identifies a layer-specific function that differs between the TCP/IP and OSI models?

A. The TCP/IP model's Transport layer provides error detection, a function handled by the OSI model's Physical layer.
B. The OSI model's Session layer manages encryption and decryption, a function that is part of the TCP/IP Transport layer.
C. The TCP/IP model's Internet layer handles IP addressing and routing, which are functions of the OSI model's Network layer.
D. The TCP/IP model's Application layer performs packet sequencing, which is a function of the OSI model's Presentation layer.

Answer: C

Question: 85

A university needs to set up a network for its campus to connect various departments, dormitories, and libraries within a 10-square-kilometer area. What type of network is most appropriate for this setup?

A. Campus Area Network (CAN)
B. Local Area Network (LAN)

C. Metropolitan Area Network (MAN)
D. Wide Area Network (WAN)

Answer: A

Question: 86

During a cybersecurity investigation, analysts discover that a piece of malware has spread throughout the organization's network. The malware was initially introduced via an email attachment disguised as an invoice. Once executed, the malware replicated itself across the network without requiring further user interaction. What type of malware delivery method and propagation is described in this scenario?

A. A phishing attack delivering ransomware B. A phishing attack delivering a worm
C. A brute-force attack delivering a rootkit
D. A watering hole attack delivering a Trojan

Answer: B

Question: 87

A security operations center (SOC) analyst reviews an alert indicating potential malware activity on a user's workstation. Upon investigation, the analyst finds that the activity was caused by a legitimate business application performing its intended function. How would this alert be classified?

A. A true negative alert B. A true positive alert C. A false positive alert D. A false negative alert

Answer: C

Question: 88

An e-commerce company is scaling its operations globally. To ensure the effectiveness of its Security Operations strategy, which approach most accurately reflects the business-centric pillar of effective security operations?

A. Prioritizing protection of data assets based on their classification, business value, and regulatory implications.
B. Focusing solely on regulatory compliance to avoid legal liabilities, without considering other business risks.
C. Developing a SOC strategy that mirrors industry trends, without adapting it to the organization's unique needs and risks.
D. Outsourcing the entire security operations function to a third-party vendor without defining business-specific metrics for performance evaluation.

Answer: A

Question: 89

In the context of the cloud shared responsibility model, which of the following scenarios best illustrates a

misunderstanding of security responsibilities when using Infrastructure as a Service (IaaS)?

A. The customer encrypts sensitive data stored on the cloud.
B. The CSP maintains physical security and prevents unauthorized access to data centers.
C. The CSP implements multi-factor authentication (MFA) for access to its management console.
D. The customer assumes the CSP is responsible for securing access to their virtual machines.

Answer: D

Question: 90

Which of the following technologies is most critical in enabling the detection and response to threats in modern security operations?

A. Data Loss Prevention (DLP) tools
B. Next-Generation Firewalls (NGFWs)
C. Security Information and Event Management (SIEM) systems
D. Endpoint Detection and Response (EDR) tools

Answer: C

Question: 91

A security team deploys a Network-Based Intrusion Detection System (NIDS) to monitor traffic on their corporate network. They notice that the system fails to detect some malicious activities. Which of the following is the most likely reason for this limitation?

A. It operates only on endpoints, not the network
B. It relies solely on user authentication for threat detection
C. The system lacks a robust encryption mechanism
D. Encrypted network traffic prevents analysis

Answer: D

Question: 92

Which two components of the "Four Cs of Cloud Native Security" are primarily responsible for ensuring secure deployment pipelines and runtime environments in cloud-native applications? (Choose two)

A. Containers
B. Clusters
C. Cryptography
D. Cloud
E. Compliance

Answer: A, B

Question: 93

In the cloud shared responsibility model, which of the following responsibilities typically falls under the

customer when using a Platform as a Service (PaaS) model?

A. Ensuring the physical infrastructure complies with regulatory requirements.
B. Securing the application data and user access to the application.
C. Maintaining the underlying operating system and middleware.
D. Managing physical security of the data center and hardware.

Answer: B

Question: 94

An administrator is configuring a new corporate network and needs to ensure secure communication between internal departments using VLANs. What is the primary purpose of implementing VLANs in a network?

A. Increase the physical bandwidth of the network by adding more devices.
B. Allow dynamic assignment of IP addresses to connected devices.
C. Automatically encrypt all traffic transmitted between network segments.
D. Enable logical segmentation of networks to isolate and secure traffic.

Answer: D

Question: 95

An organization has implemented an Intrusion Detection System (IDS) to monitor network traffic for suspicious activity. During a review, the security team notices frequent alerts about a benign internal file-sharing protocol. Which of the following is the most effective action the security team should take to address this issue without compromising network security?

A. Upgrade the IDS to a newer version that supports the protocol natively.
B. Ignore the alerts since the protocol is internal and trusted.
C. Disable the IDS temporarily to stop the alerts.
D. Adjust the IDS rules to whitelist the internal file-sharing protocol.

Answer: D

Question: 96

A network administrator connects a new device to a network. The device is configured to obtain an IP address dynamically. During the DHCP process, which of the following steps ensures the device is assigned a unique IP address?

A. DHCP Acknowledgment
B. DHCP Discovery
C. IP Conflict Detection
D. DHCP Request

Answer: C

Question: 97

Which of the following is the most effective first step for mitigating a ransomware attack within a Security Operations Center (SOC)?

A. Disconnecting infected systems from the network to prevent further spread of the ransomware. B. Installing an anti-malware solution on infected systems while keeping them connected to the network.
C. Restoring the compromised system from a backup without analyzing the attack's entry point.
D. Paying the ransom to regain access to encrypted data as quickly as possible.

Answer: A

Question: 98

During the reconnaissance phase of the cyberattack lifecycle, what is the primary goal of the attacker?

A. Disrupting the target's operations through a denial-of-service attack
B. Collecting information about the target's infrastructure and vulnerabilities
C. Gaining unauthorized access to the target's systems
D. Deploying malware to compromise critical systems

Answer: B

Question: 99

A Security Operations Center (SOC) analyst is investigating a potential breach after receiving an alert from a next-generation firewall. Which of the following steps should the analyst prioritize first during the investigation?

A. Erase the data on the affected system to prevent further damage.
B. Notify all users and stakeholders about the potential breach.
C. Identify and verify the alert by correlating it with other logs and events.
D. Isolate the affected system and perform a detailed forensic analysis to identify the root cause.

Answer: C

Question: 100

Complete the following sentence.

A. During the installation stage of a cyberattack, an attacker is most likely to...
B. Install keylogging software to capture user credentials on a compromised system.
C. Gain unauthorized access to a system by exploiting a zero-day vulnerability.
D. Modify DNS records to redirect users to a malicious website.
E. Execute a spear-phishing campaign to compromise an employee’s email account.

Answer: B

Question: 101

Which of the following scenarios best illustrates a Platform as a Service (PaaS) offering in cloud computing?

A. An organization stores large volumes of unstructured data in a cloud provider's storage service and analyzes it using their own analytics tools.
B. A team rents raw computing power and storage from a cloud provider to train machine learning models.
C. A company uses a cloud provider's virtual machines to install and configure its own web server, database, and application software.
D. A development team utilizes a cloud-based environment that provides pre-configured tools for building, testing, and deploying applications.

Answer: D

Question: 102

An organization is considering using an Infrastructure as a Service (IaaS) model for its cloud deployments. The security team is tasked with understanding what responsibilities fall on the organization when utilizing IaaS to ensure compliance and operational security. Which of the following is an organizational responsibility when using an IaaS cloud service model?

A. Managing and updating the underlying hypervisor software.
B. Provisioning and maintaining virtual machines.
C. Maintaining the cooling and power supply for server hardware.
D. Ensuring physical security of data center facilities.

Answer: B

Question: 103

A company has a network with multiple branches connected through routers. The network administrator needs to decide between using static routing or dynamic routing protocols to manage route advertisement and updates efficiently. Based on the network's requirements, answer the following question: Which of the following statements accurately describe the differences between static routing and dynamic routing protocols? (Choose two)

A. Static routing requires a significant amount of CPU and memory resources compared to dynamic routing.
B. Dynamic routing protocols like OSPF and BGP require periodic manual updates to maintain routing tables.
C. Dynamic routing automatically adjusts to network topology changes without manual intervention.
D. Static routing is better suited for small, stable networks with minimal changes.
E. Dynamic routing does not require any configuration of routing tables by the network administrator.

Answer: C, D

Question: 104

As part of a cybersecurity training simulation, you are analyzing traffic logs for suspicious activities targeting a web application. Your task is to identify SQL injection techniques commonly used by attackers. Which two of the following are examples of SQL injection techniques? (Choose two)

A. Error-based SQL injection
B. DNS tunneling
C. Command injection
D. Union-based SQL injection
E. Cross-site scripting (XSS)

Answer: A, D

Question: 105

Which two stages of the cyberattack lifecycle focus on attackers expanding control and gathering sensitive information within the target network? (Choose two)

A. Action on Objectives
B. Lateral Movement
C. Command and Control
D. Installation
E. Reconnaissance

Answer: A, B

Question: 106

Which characteristic best demonstrates a critical aspect of the "people" pillar in effective security operations?

A. Procurement of cutting-edge cybersecurity tools and platforms
B. Expertise in interpreting and analyzing security alerts generated by automated tools
C. Outsourcing all security operations to third-party vendors
D. Focus on reducing mean time to detect (MTTD) through automated systems

Answer: B

Question: 107

Your organization wants to migrate its network infrastructure to a cloud-based service to reduce the cost and complexity of managing hardware. Which of the following best describes the Network as a Service (NaaS) model and its capabilities?

A. NaaS offers managed IT services for identity and access management.
B. NaaS provides a virtualized network infrastructure, including firewalls, routing, and load balancing.
C. NaaS is a software-based platform that automates the deployment of containerized applications.
D. NaaS allows organizations to deploy and manage virtual machines on demand.

Answer: B

Question: 108

Which statement best describes the shared responsibility model in cloud security?

A. The customer and cloud provider are jointly responsible for securing all cloud resources.
B. The cloud provider secures the infrastructure, while the customer secures data, applications, and operating systems.
C. The cloud provider is responsible for securing both the infrastructure and the data.
D. The customer is responsible for securing the physical infrastructure.

Answer: B

Question: 109

Which of the following is an example of a service commonly hosted in a demilitarized zone (DMZ)?

A. A database server storing sensitive customer information.
B. An internal file-sharing server accessible only to employees.
C. A backup server used for storing disaster recovery data.
D. A web server hosting the company's public website.

Answer: D

Question: 110

A Security Operations Center (SOC) is experiencing delays in identifying and responding to threats due to a high volume of false-positive alerts. What is the most effective approach to improve threat detection accuracy?

A. Implement a machine learning-based system to dynamically filter alerts.
B. Disable alerts for low-priority events to reduce overall alert volume.
C. Increase the number of rules and signatures in the detection system.
D. Ignore alerts that do not match previously reported attack patterns.

Answer: A

Question: 111

Which of the following actions is most likely to result from a device being infected with spyware?

A. The device frequently restarts itself due to corrupted system files.
B. The user notices a significant slowdown in device performance due to high CPU usage.
C. Sensitive credentials such as passwords and credit card numbers are leaked without the user's knowledge.
D. The user is bombarded with pop-up advertisements, even when not browsing the web.

Answer: C

Question: 112

Which of the following best describes the role of the "Identify" function in a security operations context?

A. Performing continuous vulnerability scans on network endpoints to mitigate risks.
B. Establishing an understanding of organizational assets, systems, and risks.
C. Detecting malicious activity in real-time through threat intelligence feeds.
D. Monitoring user activity logs for suspicious behavior in cloud environments.

Answer: B

Question: 113

You are a junior cybersecurity analyst investigating a breach in your organization's system. During your analysis, you find an unpatched software application and evidence that a threat actor leveraged it to gain unauthorized access to sensitive data. Which of the following statements correctly differentiate between vulnerabilities and exploits in the context of this scenario? (Choose two)

A. An exploit is a deliberate action taken to fix a system's vulnerability and prevent breaches.
B. A vulnerability is a weakness in the system that can potentially be exploited by a threat actor.
C. A vulnerability always leads to a system compromise, while an exploit only has potential risks.
D. Vulnerabilities are caused solely by unpatched software, while exploits result only from malware usage.
E. An exploit takes advantage of a vulnerability to execute unauthorized actions on a system.

Answer: B, E

Question: 114

Which of the following features is most critical to the effectiveness of an antivirus solution in protecting endpoints?

A. Application sandboxing, which restricts all software to predefined operating environments.
B. Open-source architecture, which ensures the antivirus is freely accessible to developers worldwide.
C. Cloud-based management, which eliminates the need for updates to antivirus databases.
D. Signature-based detection, which identifies malware by comparing files to a database of known malware signatures.

Answer: D

Question: 115

A financial organization uses endpoint security software across all employee devices. Which approach ensures the endpoints remain protected against the latest vulnerabilities and exploits?

A. Install updates annually to minimize downtime.
B. Apply updates only when a major breach occurs.
C. Implement automated patch management tools for regular updates.

D. Manually update devices during non-business hours.

Answer: C

Question: 116

Your organization is drafting its first disaster recovery plan (DRP) to ensure operational continuity during unexpected events. Which of the following components should not be included in the disaster recovery plan?

A. A comprehensive risk assessment to identify potential threats
B. Detailed staffing plans for normal business operations
C. Backup and recovery procedures for critical systems
D. Communication protocols for internal and external stakeholders

Answer: B

Question: 117

Which of the following is a primary component of an endpoint security solution?

A. Physical firewall appliance
B. Antivirus and Anti-Malware software
C. Network Intrusion Detection System (NIDS)
D. Email spam filter

Answer: B

Question: 118

A mid-sized organization has a network with multiple branches. The network administrator is evaluating whether to use static or dynamic routing for managing network traffic. Which of the following statements best differentiates between static and dynamic routing protocols?

A. Static routing requires less administrative effort compared to dynamic routing.
B. Dynamic routing protocols can automatically adjust to changes in the network topology.
C. Static routing is better suited for large, complex networks with frequent topology changes.
D. Static routing uses routing protocols like RIP and OSPF, while dynamic routing does not use protocols.

Answer: B

Question: 119

Which of the following is a common method used by attackers to deliver ransomware to target systems?

A. Performing social engineering scams to gain administrative access
B. Exploiting vulnerabilities in outdated software

C. Deploying brute-force attacks on password-protected systems
D. Sending phishing emails with malicious attachments or links

Answer: D

Question: 120

Which of the following statements best describes the primary benefit of using SD-WAN over traditional WAN in a geographically distributed organization?

A. SD-WAN improves application performance by dynamically routing traffic based on real-time network conditions.
B. SD-WAN restricts users to using a single ISP for connectivity, simplifying management.
C. SD-WAN eliminates the need for any hardware at branch offices by using cloud-based solutions exclusively.
D. SD-WAN encrypts all traffic end-to-end, ensuring absolute security from all types of cyber threats.

Answer: A

Question: 121

A healthcare organization is designing its security operations processes to enhance threat detection and response capabilities. Which of the following processes best demonstrates adherence to the pillars of effective security operations?

A. Creating processes that prioritize speed over accuracy when handling security alerts.
B. Deploying a centralized logging system but not defining log retention or review processes.
C. Relying on ad-hoc processes for responding to incidents, focusing solely on the most severe events.
D. Establishing a repeatable incident response process with clear steps for detection, containment, eradication, and recovery.

Answer: D

Question: 122

What is the primary function of an Intrusion Prevention System (IPS) in a cybersecurity setup?

A. Monitoring traffic without taking any preventive action
B. Replacing firewalls to filter unauthorized access
C. Encrypting sensitive data before transmission
D. Detecting and actively blocking malicious network traffic

Answer: D

Question: 123

During the cyberattack lifecycle, which stage involves crafting a malicious payload designed to exploit a target's vulnerabilities and prepare it for deployment?

A. Reconnaissance
B. Exploitation
C. Delivery
D. Weaponization

Answer: D

Question: 124

During an investigation into unusual network activity, a SOC analyst identifies a high volume of outbound traffic from a specific server to an unknown external IP address. What is the most effective next step to proceed with the investigation?

A. Replace the server's network adapter to ensure the hardware isn't compromised.
B. Report the activity to law enforcement as a potential data exfiltration incident.
C. Disable the server's outbound network connection immediately to stop the traffic.
D. Analyze the server's outbound traffic patterns and compare them against historical baselines.

Answer: D

Question: 125

A financial organization has recently deployed a Host-Based Intrusion Detection System (HIDS) on their critical servers. The security administrator notices alerts indicating potential malicious activity. However, upon investigation, they discover that the alerts are false positives. To minimize false positives while maintaining effective threat detection, what is the best course of action for the security administrator?

A. Configure the HIDS to only monitor specific critical files and directories.
B. Switch to a Network-Based Intrusion Detection System (NIDS) instead of HIDS.
C. Disable all HIDS rules that generate false positives.
D. Update the HIDS signatures and tailor rules based on the environment.

Answer: D

Question: 126

Which of the following endpoint security components focuses on monitoring and preventing unauthorized applications from executing?

A. Application Whitelisting
B. Web Application Firewall (WAF)
C. Data Loss Prevention (DLP)
D. Host Intrusion Prevention System (HIPS)

Answer: A

Question: 127

A cybersecurity analyst is investigating an incident where an online retail website experienced a sudden

surge in network traffic, causing service disruption. Upon inspection, the traffic primarily consisted of legitimate-looking HTTP GET requests sent in massive volumes. What type of Distributed Denial of Service (DDoS) attack is most likely being used in this scenario?

A. UDP Flood
B. HTTP Flood
C. SYN Flood
D. Ping of Death

Answer: B

Question: 128

When comparing TLS to other tunneling protocols, such as IPsec, which of the following is an advantage of TLS in securing communication tunnels?

A. TLS operates at the network layer, making it faster than application-layer protocols.
B. TLS does not require a certificate authority, unlike other tunneling protocols.
C. TLS supports multicast traffic, whereas IPsec cannot handle multicast traffic.
D. TLS is designed to secure individual sessions at the application layer, providing granular control.

Answer: D

Question: 129

Which of the following statements best describes the role of TLS (Transport Layer Security) in a secure tunneling protocol?

A. TLS is used exclusively for encrypting email communications between mail servers.
B. TLS ensures end-to-end encryption and authentication for data transmitted over the tunnel.
C. TLS is an outdated protocol that has been replaced entirely by SSL (Secure Sockets Layer).
D. TLS is only used in VPNs and does not apply to other tunneling or communication protocols.

Answer: B

Question: 130

What is a key characteristic of a WAN compared to other types of area networks?

A. It is primarily used for short-range communication between personal devices.
B. It uses private IP addresses and operates exclusively within a single building.
C. It relies exclusively on wireless technology for device connectivity.
D. It connects multiple local networks across large geographical areas using telecommunications infrastructure.

Answer: D

Question: 131

A cybersecurity team at a financial institution is investigating a potential phishing attack. The attack involved a fraudulent email sent to employees with a subject line: "Urgent: Update Your Account Details." The email contained a link to a website resembling the company's intranet login page. What

characteristic of phishing attacks does this scenario best illustrate?

A. Social engineering to manipulate trust B. SQL Injection on the intranet login page C. Exploitation of zero-day vulnerabilities D. Distributed Denial of Service (DDoS)

Answer: A

Question: 132

A SOC manager wants to improve the organization's incident response capabilities. Which of the following strategies would be the most impactful for achieving this goal?

A. Delay reporting incidents until a full investigation is complete to avoid false alarms.
B. Focus solely on automating all SOC processes to save time.
C. Conduct regular incident response drills and tabletop exercises.
D. Hire additional analysts to increase response capacity.

Answer: C

Question: 133

A cybersecurity analyst is troubleshooting a network connectivity issue and observes that a device is unable to access external resources. Which layer of the OSI model should the analyst investigate first to diagnose the issue?

A. Physical Layer
B. Application Layer
C. Data Link Layer
D. Network Layer

Answer: D

Question: 134

A security administrator is tasked with securing access to sensitive data within an organization. They implement a system requiring users to log in with both a password and a temporary code sent to their mobile devices. Which of the following statements accurately describe the implemented authentication method? (Choose two)

A. It uses single-factor authentication because a password is sufficient to access the system.
B. It uses single-factor authentication because both credentials are entered by the user.
C. It uses multi-factor authentication because it requires two separate passwords.

D. It uses multi-factor authentication because it combines something the user knows and something the user has.
E. It uses multi-factor authentication because it leverages two independent factors for authentication.

Answer: D, E

Question: 135

Which of the following is a defining feature of a hybrid cloud deployment model?

A. Resources are shared across multiple organizations with similar needs.
B. Resources are hosted on multiple public cloud providers but not on-premises.
C. Resources are distributed between on-premises infrastructure and public cloud providers.
D. Resources are entirely owned and managed by a single organization.

Answer: C

Question: 136

An organization plans to test its disaster recovery plan (DRP) for the first time. Which of the following testing methods is least effective for validating the DRP's robustness and practicality?

A. A full-scale simulation that temporarily shuts down production systems
B. Tabletop exercises with key stakeholders simulating disaster scenarios
C. Relying on external auditors to verify the organization's readiness
D. Walkthrough tests where team members review their roles and responsibilities

Answer: C

Question: 137

Which two capabilities are essential for effective threat detection and response in a Security Operations Center (SOC)? (Choose two)

A. Security Orchestration, Automation, and Response (SOAR)
B. Penetration Testing
C. Security Information and Event Management (SIEM)
D. Endpoint Encryption
E. Perimeter Firewalls

Answer: A, C

Question: 138

Which of the following are examples of common threat detection systems used in cybersecurity for monitoring network traffic and identifying potential threats? (Choose two)

A. Virtual Private Network (VPN)
B. Firewall

C. Content Delivery Network (CDN)
D. Security Information and Event Management (SIEM)

E. Intrusion Detection System (IDS)

Answer: D, E

Question: 139

Which of the following devices primarily operates at Layer 2 of the OSI model and is responsible for forwarding data based on MAC addresses?

A. Firewall
B. Switch
C. Hub
D. Router

Answer: B

Question: 140

An endpoint security team is evaluating the capabilities of an antivirus solution. Which detection technique is most effective at identifying new, previously unknown malware threats?

A. Signature-based detection, which matches files against a database of known threats.
B. Heuristic analysis, which detects malicious behavior by analyzing suspicious patterns.
C. Whitelist filtering, which allows only pre-approved applications to run on the endpoint.
D. Device control, which restricts the use of external USB devices.

Answer: B

Question: 141

Which of the following best explains why automation tools are considered a critical technology pillar in security operations?

A. They ensure compliance with regulatory frameworks by automating audit processes.
B. They eliminate the need for human analysts by fully automating all security tasks.
C. They improve response times by streamlining repetitive tasks and reducing alert fatigue.
D. They provide static rules for detecting known threats based on predefined signatures.

Answer: C

Question: 142

Which of the following statements about VLANs (Virtual Local Area Networks) and network segmentation is correct?

A. VLANs eliminate the need for firewalls by ensuring complete isolation of traffic between segments.

B. VLANs segment a network by grouping devices logically, regardless of their physical location.

C. VLANs rely on Layer 1 physical segmentation for isolating network traffic.
D. VLANs segment a network by separating traffic based on IP address ranges.

Answer: B

Question: 143

What does the term "Mean Time to Respond (MTTR)" signify in the context of security operations?

A. The average time taken to patch a known vulnerability in the system
B. The average time taken to detect a threat after it enters the network
C. The average time between identifying a threat and reporting it to stakeholders
D. The average time taken by the security team to respond to and mitigate a security incident

Answer: D

Question: 144

Which type of area network is most commonly leveraged in an SD-WAN architecture to connect branch offices to cloud services?

A. Personal Area Network (PAN)
B. Wide Area Network (WAN)
C. Storage Area Network (SAN)
D. Metropolitan Area Network (MAN)

Answer: B

Question: 145

Which is the greatest risk associated with failing to apply regular security updates to endpoint devices in an organization?

A. Reduced compatibility with older hardware systems.
B. Increased operational costs due to frequent updates.
C. Increased vulnerability to zero-day attacks and exploits.
D. Reduced performance of endpoint devices.

Answer: C

Question: 146

A cybersecurity analyst is investigating an alert triggered by the organization's IDS. The IDS flagged a sequence of packets as suspicious due to abnormal behavior resembling a port scan. Which type of IDS detection method is most likely being used in this scenario?

A. Heuristic detection

B. Behavior-based detection
C. Signature-based detection
D. Anomaly-based detection

Answer: D

Question: 147

What is a primary goal of the "Detect" function within a security operations framework?

A. To proactively secure sensitive data through encryption and tokenization.
B. To analyze network traffic in real-time for potential indicators of compromise (IoCs).
C. To map out critical organizational assets and define access policies.
D. To design disaster recovery plans for post-breach scenarios.

Answer: B

Question: 148

You are configuring a network for a small office with limited IT staff and minimal changes to its network topology. Which of the following is the best reason to choose static routing over dynamic routing in this scenario?

A. Static routing supports faster convergence times than dynamic routing.
B. Static routing protocols, like BGP, are more secure than dynamic routing protocols.
C. Static routing consumes less bandwidth because it does not involve route advertisement.
D. Static routing reduces the risk of routing loops in complex network topologies.

Answer: C

Question: 149

Which of the following best describes the primary role of DHCP in a modern network?

A. To route traffic between different subnets in a network.
B. To provide end-to-end encryption for all network traffic.
C. To ensure all devices use static IP addresses for stability.
D. To dynamically assign IP addresses to devices and maintain a pool of available addresses.

Answer: D

Question: 150

Which of the following threat detection systems primarily relies on monitoring network traffic in real time to identify potential security threats?

A. Network-Based Intrusion Detection System (NIDS)
B. Antivirus Software

C. Data Loss Prevention (DLP) System
D. Host-Based Intrusion Detection System (HIDS)

Answer: A

Question: 151

During an active Distributed Denial of Service (DDoS) attack, what is the most appropriate mitigation action a Security Operations team should take?

A. Redirecting all incoming traffic to a backup server until the attack subsides.
B. Implementing rate limiting and leveraging a Content Delivery Network (CDN) to absorb malicious traffic.
C. Scaling up the network infrastructure to handle the increased traffic volume.
D. Blocking the source IP addresses of the attack using a firewall.

Answer: B

Question: 152

A startup evaluates IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS) to determine the best fit for hosting their custom application. They prioritize flexibility and control over the underlying infrastructure while managing application-level operations themselves. Why might an organization choose IaaS over PaaS or SaaS for deploying a custom application?

A. IaaS provides prebuilt application-level services to reduce the need for in-house development expertise.
B. IaaS guarantees higher performance for applications compared to SaaS and PaaS.
C. IaaS eliminates the need to manage storage, compute, or network resources entirely.
D. IaaS allows the organization to configure and control the underlying operating systems and network components.

Answer: D

Question: 153

An organization is deploying a VPN to allow branch offices to securely connect to the corporate network over the internet. Which type of VPN configuration would best suit this requirement?

A. Client-to-Site VPN, as it allows individual devices to connect to the network securely.
B. Full Mesh VPN, as it allows direct communication between any two devices without a central hub.
C. Site-to-Site VPN, as it connects entire networks securely over the internet.
D. Split Tunnel VPN, as it only encrypts traffic meant for the corporate network.

Answer: C

Question: 154

Which of the following scenarios would be the most suitable use case for adopting Network as a Service

(NaaS)?

A. A startup looking to analyze customer data using cloud-based machine learning models.
B. A retail company needing scalable bandwidth and secure VPN connections across multiple branches.
C. An enterprise implementing a comprehensive identity and access management system.
D. A software development team requiring a platform to host their containerized applications.

Answer: B

Question: 155

Which of the following best describes the impact of false negative alerts compared to false positive alerts in a security environment?

A. False negatives and false positives have identical impacts on security operations.
B. False positives can lead to unnoticed breaches.
C. False negatives are more dangerous because they allow malicious activity to go undetected.
D. False negatives are less dangerous because they do not generate alerts.

Answer: C

Question: 156

You are part of a cybersecurity team tasked with assessing the security posture of a newly developed application. During the assessment, you discover an input field in the application that does not properly validate user inputs, potentially allowing SQL injection. Which of the following best describes the situation?

A. This is an example of exploit chaining, where multiple vulnerabilities combine to form a single exploit.
B. A vulnerability exists because the input field fails to validate user input.
C. This is not a security issue since no active attacks have been reported.
D. An exploit exists because attackers can already take advantage of the SQL injection vulnerability.

Answer: B

Question: 157

Which of the following actions is an example of passive reconnaissance in the cyberattack lifecycle?

A. Intercepting network traffic using a packet sniffer
B. Scanning the target's network ports using tools like Nmap
C. Phishing employees of the target organization to collect credentials
D. Searching publicly available information about the target, such as LinkedIn profiles

Answer: D

Question: 158

A cybersecurity analyst identifies malware attempting to exfiltrate sensitive data to an external server. The analyst uses the Palo Alto Networks firewall to create threat prevention policies. Which two actions should be included in the configuration to prevent data exfiltration? (Choose two)

A. Use Application Override to bypass inspection for encrypted traffic.
B. Create a URL Filtering profile to block access to newly registered domains.
C. Enable Anti-Spyware profiles to block connections to known malicious command-and-control (C2) servers.
D. Set the action for all malware signatures to "alert" in the Antivirus profile.
E. Enable a Data Filtering profile to detect and block sensitive data patterns in outbound traffic.

Answer: C, E

Question: 159

A retail company wants to improve its network security by implementing URL filtering to manage employee web access and block access to malicious sites. However, the IT team needs to configure policies that balance security with employee productivity. Which of the following options describe valid use cases or capabilities of URL filtering in this scenario? (Choose two)

A. Enforcing time-based access restrictions to social media websites during working hours.
B. Blocking access to websites that contain specific keywords within their URL or domain name.
C. Allowing access to uncategorized URLs only after manual administrator review.
D. Using URL filtering to prevent data exfiltration by analyzing file content for sensitive information.
E. Identifying and blocking malicious file uploads to an external file-sharing website.

Answer: A, C

Question: 160

Which of the following is not a characteristic of a Platform as a Service (PaaS) offering in cloud computing?

A. Developers retain control over the operating system and hardware
B. It allows developers to focus on writing and deploying code rather than managing underlying infrastructure.
C. Pre-configured development tools and environments are provided by the cloud provider.
D. The cloud provider handles software updates and infrastructure maintenance.

Answer: A

Question: 161

Which of the following best describes the role of interfaces in effective security operations within a Security Operations Center (SOC)?

A. Interfaces are exclusively responsible for managing cloud-based resources monitored by the SOC.
B. Interfaces serve as entry points for external attackers to exploit vulnerabilities in the SOC's infrastructure.
C. Interfaces are physical connections between the SOC and network devices for manual data collection and analysis.
D. Interfaces ensure seamless communication between SOC tools, such as Security Information and Event Management (SIEM) systems, and external threat intelligence feeds.

Answer: D

Question: 162

Which of the following functions is the primary responsibility of a Security Operations Center (SOC)?

A. Ensuring compliance with regulatory requirements by preparing audit reports and documentation.
B. Performing continuous monitoring, detection, and response to security incidents across an organization’s infrastructure.
C. Managing physical security measures such as access control and surveillance systems.
D. Developing secure software applications to prevent vulnerabilities during the design phase.

Answer: B

Question: 163

A cloud administrator is tasked with deploying a secure cloud environment using virtualization. Which statement best describes the role of a hypervisor in cloud virtualization?

A. A hypervisor is a container orchestration tool used for managing application deployment.
B. A hypervisor ensures high availability by replicating virtual machines across multiple cloud regions.
C. A hypervisor is a cloud-native service designed to provide direct data encryption between virtual machines.
D. A hypervisor is software that enables multiple virtual machines to run on a single physical machine by abstracting the underlying hardware.

Answer: D

Question: 164

Which of the following best describes the concept of "hosted" in cloud computing?

A. A virtual environment that exists solely within the local network of the user organization.
B. A physical server located on-site but managed remotely by a cloud provider.
C. A service that is entirely managed and run on a customer’s on-premises data center.
D. A service provided by a third-party cloud provider and accessed over the internet.

Answer: D

Question: 165

Which of the following threat detection systems is best suited for analyzing endpoint activity and responding to advanced threats like fileless malware?

A. Security Information and Event Management (SIEM) System
B. Firewall
C. Endpoint Detection and Response (EDR)
D. Honeypot

Answer: C

Question: 166

When deploying threat detection systems in a corporate network, which of the following capabilities are most commonly associated with identifying and mitigating threats? (Choose two)

A. Behavioral anomaly detection B. Static IP allocation
C. Packet forwarding
D. Network Address Translation (NAT)
E. Signature-based detection

Answer: A, E

Question: 167

Which of the following best describes a virtual machine (VM) in the context of cloud computing?

A. A physical server that runs multiple operating systems simultaneously.
B. A containerized application runtime environment that isolates dependencies at the application level.
C. A software-based representation of a physical computer that runs an operating system and applications.
D. A software development environment specifically designed for building cloud-native applications.

Answer: C

Question: 168

When comparing types of area networks based on their range and use cases, which of the following statements correctly differentiate between them? (Choose two)

A. A Metropolitan Area Network (MAN) spans a city or urban area.
B. A Wide Area Network (WAN) connects multiple LANs across large geographic areas.
C. Wide Area Network (WAN) is restricted to a single building.
D. Campus Area Network (CAN) is designed for personal device connectivity.
E. Local Area Network (LAN) is suitable for global communications.

Answer: A, B

Question: 169

A threat actor gains initial access to a company's network through a phishing email containing malicious attachments. Once inside, the attacker moves laterally to other systems, identifies sensitive data, and exfiltrates it. Which stages of the cyberattack lifecycle are being described in this scenario? (Choose two)

A. Data Exfiltration
B. Exploitation
C. Delivery
D. Lateral Movement
E. Initial Reconnaissance

Answer: A, D

Question: 170

An organization wants to segment its network to improve security by isolating critical systems, ensuring compliance with data protection regulations, and reducing the attack surface. Which of the following methods of network segmentation provides the most granular control over traffic between segments?

A. Air-gapped networks
B. Switch-based port mirroring
C. Firewall-based segmentation
D. VLANs

Answer: C

Question: 171

Which of the following statements best describes the primary functionality of the Secure Shell (SSH) protocol in the context of network security?

A. SSH uses symmetric encryption only, ensuring that both ends of the communication share the same key.
B. SSH is used to encapsulate IP packets for secure VPN connections over the internet.
C. SSH provides secure remote access to systems and the ability to tunnel network traffic over encrypted channels.
D. SSH operates as a stateless protocol, primarily designed to manage file transfers across untrusted networks.

Answer: C

Question: 172

Which device operates at Layer 4 of the OSI model to inspect and control traffic based on TCP or UDP port numbers?

A. Switch

B. Router
C. Hub
D. Load Balancer

Answer: D

Question: 173

In the Command-and-Control (C2) stage of the cyberattack lifecycle, what is the primary purpose of the communication between the attacker and the compromised system?

A. To execute lateral movement within the compromised network
B. To maintain persistent access and control over the compromised system
C. To scan for vulnerabilities in the compromised network
D. To exfiltrate data to the attacker's remote server

Answer: B

Question: 174

A cybersecurity analyst is tasked with securing a containerized application running on a cloud platform. Which of the following actions is the most effective in ensuring the security of the containers?

A. Keeping the base image unchanged, even if vulnerabilities are found, to maintain consistency.
B. Using runtime security tools to monitor container activity and detect anomalies.
C. Running containers as root for ease of configuration and management.
D. Disabling all networking capabilities for the containers to prevent external communication.

Answer: B

Question: 175

A DevOps engineer is tasked with deploying a containerized application in a cloud-native environment. The engineer must configure cluster security to prevent potential attacks while ensuring smooth operations for the application. Which of the following is the most effective security measure for protecting a Kubernetes cluster in a cloud-native environment?

A. Running all containers with root privileges for easier access.

B. Enabling Role-Based Access Control (RBAC) to manage user permissions.
C. Disabling Kubernetes API audit logs to improve performance.
D. Using default namespaces for all workloads.

Answer: B

Question: 176

What is the primary function of a proxy in network security?

A. Routing traffic directly to its destination without modifying or analyzing it.
B. Replacing firewalls to prevent unauthorized access to a network.
C. Encrypting all network traffic to protect sensitive data during transmission.
D. Acting as an intermediary between a client and a server to enhance security and privacy.

Answer: D

Question: 177

An organization's IT team discovers that several employees' computers display a message demanding cryptocurrency payments in exchange for unlocking encrypted files. After analysis, they find no signs of data exfiltration but identify encrypted system files. What is the primary characteristic of the attack described?

A. Keylogging to steal credentials
B. Advanced Persistent Threat (APT)
C. Encryption of data for extortion
D. Lateral movement within the network

Answer: C

Question: 178

A company wants to deploy a HIDS solution to detect and respond to unauthorized changes on endpoints. The security team plans to use the HIDS primarily for file integrity monitoring (FIM). What is the primary role of file integrity monitoring in a HIDS?

A. Identifying unauthorized changes to monitored files or directories.
B. Preventing unauthorized users from accessing the system.
C. Blocking all attempts to modify critical system files in real time.
D. Detecting anomalies in network traffic between the host and external systems.

Answer: A

Question: 179

An organization is experiencing a volumetric DDoS attack targeting its web servers. The attack is saturating the server's bandwidth with massive amounts of traffic from various IP addresses. Which of the following mitigation strategies would be most effective in this scenario?

A. Utilizing a cloud-based DDoS mitigation service
B. Configuring rate-limiting on the server
C. Deploying a Web Application Firewall (WAF)
D. Installing an intrusion detection system (IDS)

Answer: A

Question: 180

An organization using a Palo Alto Networks firewall receives a notification about a new zero-day vulnerability affecting its network infrastructure. What is the most effective step the security team should take to minimize the risk associated with this vulnerability?

A. Perform a complete system reboot to clear any potential threats
B. Create custom threat signatures to detect and block the zero-day vulnerability
C. Wait for official confirmation of active exploitation before taking any action
D. Immediately apply the latest security update released by Palo Alto Networks.

Answer: D

Question: 181

A security operations center (SOC) analyst receives an alert indicating unusual outbound traffic from a corporate device to an unfamiliar IP address. Which of the following should the analyst do first in response to the alert?

A. Notify the incident response team without further analysis.
B. Investigate the alert by correlating it with other logs and contextual data.
C. Immediately block the IP address in the firewall.
D. Disable the corporate device to prevent further activity

Answer: B

Question: 182

In the context of cloud-native security, which of the following best describes a security challenge specific to containers within the "Four Cs of Cloud Native Security"?

A. Containers are inherently secure and do not require runtime monitoring.
B. Containers introduce risks related to misconfigured host kernel access.
C. Containers are isolated from the host and therefore do not require security patches.
D. Containers always inherit security policies from the host operating system.

Answer: B

Question: 183

A company wants to restrict internet access to specific employees while ensuring that critical business services remain accessible. Which firewall policy configuration is most appropriate to achieve this goal?

A. Use a default "Allow All" policy but log all traffic for analysis.
B. Disable NAT for the restricted employees' subnets.
C. Enable a global "Deny All" policy to block all outgoing traffic.
D. Create a policy to allow traffic only to specific business-critical applications.

Answer: D

Question: 184

During a penetration test, you discover that a database server is vulnerable to SQL injection due to improper input validation. The tester uses a script to extract sensitive customer records. Which of the following correctly differentiates between vulnerabilities and exploits in this situation? (Choose two)

A. The SQL injection flaw and the tester's actions are both vulnerabilities since they expose sensitive data.
B. The script used to extract sensitive records is a vulnerability because it exposes the database to unauthorized actions.
C. The SQL injection flaw in the server is a vulnerability because it represents a weakness in the database's input validation.
D. Vulnerabilities like SQL injection can be exploited even if a system is properly patched.
E. The script used to extract sensitive customer records is an exploit because it takes advantage of the vulnerability to achieve unauthorized actions.

Answer: C, E

Question: 185

Which of the following best represents the role of "Cloud" in the Four Cs of Cloud Native Security?

A. Ensuring that cloud service providers implement encryption for all stored data.
B. Automating application deployment through continuous integration and continuous delivery (CI/CD) pipelines.
C. Offering built-in security features to protect sensitive data within application code.
D. Providing the underlying infrastructure, such as compute, storage, and networking, on which applications are built.

Answer: D

Question: 186

Which of the following represents a critical requirement for interfaces to support the pillars of effective security operations?

A. Using interfaces only for automated alerts, leaving manual investigations to analysts.
B. Providing real-time data synchronization across security tools and third-party integrations.
C. Limiting interfaces to a single vendor's ecosystem to reduce compatibility issues.
D. Ensuring interfaces operate on a completely isolated network to prevent unauthorized access.

Answer: B

Question: 187

A security researcher discovers a buffer overflow vulnerability in a software application. They demonstrate how an attacker could use the vulnerability to execute arbitrary code, gaining full control of the target system. What best describes the researcher's actions?

A. The researcher has demonstrated an exploit based on the identified vulnerability.
B. The researcher has fixed the vulnerability by showing how it works.
C. The researcher has identified a vulnerability but not an exploit.
D. The researcher has created a new vulnerability by executing arbitrary code.

Answer: A

Question: 188

Which of the following statements best describes the key difference between endpoint security and network security?

A. Endpoint security focuses on securing individual devices, while network security focuses on securing communication between devices.
B. Endpoint security manages encryption of data in transit, whereas network security handles data at rest.
C. Endpoint security is only implemented on servers, while network security protects all devices in the network.
D. Endpoint security applies only to physical devices, while network security applies only to virtual environments.

Answer: A

Question: 189

You are designing a network for a medium-sized enterprise. The goal is to optimize security and traffic flow within the environment. Which of the following scenarios best describes a north-south traffic flow?

A. Two virtual machines on the same subnet exchange data.
B. A development team deploys a containerized microservice that communicates with other services within the same Kubernetes cluster.
C. A user in the corporate office downloads a file from a public cloud storage provider.
D. A database server communicates with a web application server hosted in the same data center.

Answer: C

Question: 190

Which two activities are critical for an SOC analyst to investigate and mitigate security incidents effectively? (Choose two)

A. Configuring access control lists (ACLs)
B. Installing anti-virus software
C. Performing routine data backups
D. Monitoring network traffic for anomalies
E. Reviewing and correlating security alerts

Answer: D, E

Question: 191

Which tunneling protocol is best suited for encrypting traffic over the internet while supporting site-to-site and remote access VPNs with strong authentication features?

A. PPTP (Point-to-Point Tunneling Protocol)
B. L2TP/IPsec (Layer 2 Tunneling Protocol with Internet Protocol Security)
C. OpenVPN
D. GRE (Generic Routing Encapsulation)

Answer: B

Question: 192

Which of the following best describes the function of IKE (Internet Key Exchange) in a VPN setup?

A. It establishes a secure channel to negotiate and manage encryption keys for VPN communication.
B. It authenticates user credentials for remote VPN access.
C. It assigns private IP addresses to VPN clients.
D. It provides data encryption to secure the communication between VPN endpoints.

Answer: A

Question: 193

Which of the following statements best describes the role of a default gateway in a network?

A. It is the device responsible for assigning IP addresses to devices in a network.
B. It blocks all traffic that is destined for external networks to maintain network security.
C. It ensures that devices on the same network can communicate directly with each other.
D. It forwards traffic between different networks when no specific route is defined for the destination.

Answer: D

Question: 194

In security operations, what is the most accurate definition of a "false positive"

A. A malicious activity that goes undetected by a security system
B. A legitimate activity mistakenly identified as malicious by a security analyst
C. An alert generated by a security tool that does not correspond to an actual threat
D. An attacker who successfully bypasses all layers of defense without triggering any alerts

Answer: C

Question: 195

What is the primary role of a Security Operations Center (SOC) within an organization?

A. To oversee the physical security of an organization's premises.
B. To deploy and manage network infrastructure, such as routers and switches.
C. To monitor, detect, investigate, and respond to cybersecurity threats in real-time.
D. To develop and implement software applications for business operations.

Answer: C

Question: 196

An e-commerce company is evaluating its processes for vulnerability management. Which process most effectively reflects the pillars of effective security operations?

A. Scheduling vulnerability scans annually and remediating vulnerabilities only if they are deemed critical.
B. Outsourcing vulnerability management without integrating it into the organization’s overall security operations strategy.
C. Assigning remediation tasks without defining accountability or tracking progress.
D. Conducting regular vulnerability assessments, prioritizing remediation efforts based on asset criticality and threat intelligence.

Answer: D

Question: 197

An enterprise network has recently been compromised by a phishing attack, resulting in the installation of malware on several endpoints. To enhance their threat prevention measures, what should be the primary focus when implementing a new threat prevention strategy?

A. Blocking access to social media sites on the corporate network B. Implementing zero-trust architecture with endpoint protection C. Conducting regular employee training on phishing awareness D. Deploying a centralized log management system

Answer: B

Question: 198

A Security Operations Center (SOC) team is tasked with improving their visibility across the organization’s network. Which of the following measures is the most effective to enhance visibility for threat detection and response?

A. Deploying endpoint detection and response (EDR) tools to all devices.
B. Implementing a unified Security Information and Event Management (SIEM) system with log aggregation and analysis.
C. Increasing the frequency of network scans to detect potential vulnerabilities.
D. Relying solely on application logs for monitoring.

Answer: B

Question: 199

Which stage of the cyberattack lifecycle focuses on transmitting a malicious payload to a target through mechanisms like phishing emails, USB drives, or malicious websites?

A. Reconnaissance
B. Lateral Movement
C. Weaponization
D. Delivery

Answer: D

Question: 200

Which of the following is the most effective way to enhance security when configuring VLANs?

A. Use a single VLAN for all devices to simplify management and prevent misconfigurations.
B. Configure inter-VLAN routing on the same switch without using access control lists (ACLs). C. Allow unrestricted trunking to ensure all VLANs can communicate with one another without additional configurations.
D. Disable unused switch ports and assign them to a dedicated, unused VLAN.

Answer: D

Question: 201

A mid-sized organization uses an antivirus solution to protect its endpoints from malware. The IT administrator notices that some malware infections are not being detected despite the antivirus software running up-to-date virus definitions. What is the most likely reason for these infections, and how should the administrator address the issue?

A. The antivirus software is outdated and needs a software update.
B. The antivirus is incompatible with the organization's operating system.
C. The antivirus has been configured to run only manual scans.
D. The antivirus relies only on signature-based detection, missing advanced threats.

Answer: D

Question: 202

Which of the following best illustrates how endpoint security and network security complement each other in a cybersecurity strategy?

A. Endpoint security prevents phishing emails, while network security protects against hardware failures.
B. Endpoint security protects devices from internal threats, while network security detects external threats targeting the network.
C. Endpoint security monitors traffic flows across the network, while network security scans individual

devices for vulnerabilities.
D. Endpoint security prevents malware from executing on devices, while network security blocks malicious traffic from entering the network.

Answer: D

Question: 203

What is the primary function of the syslog protocol in security operations?

A. To act as a dedicated intrusion detection system (IDS).
B. To actively block malicious IP addresses on the network.
C. To collect, store, and transport log messages from various devices in a standardized format.
D. To scan files and detect malware on endpoint devices.

Answer: C

Question: 204

An organization wants to securely forward database traffic (on port 3306) from a local machine to a remote server for administration purposes. Which SSH feature allows this functionality, and why?

A. SSH dynamic port forwarding, which forwards traffic dynamically based on application-layer protocols.
B. SSH remote port forwarding, which forwards traffic from the client to the remote server.
C. SSH agent forwarding, which allows the use of private keys stored on the client.
D. SSH local port forwarding, which forwards traffic from a local port to a remote server over the SSH tunnel.

Answer: D

Question: 205

Which statement about the "Cloud" layer in the Four Cs of Cloud Native Security is most accurate?

A. The "Cloud" layer ensures application-level security through runtime vulnerability scanning.
B. The "Cloud" layer eliminates the need for security configurations at the application and container levels.
C. The "Cloud" layer supports the other layers by providing secure, scalable infrastructure services and network controls.
D. The "Cloud" layer focuses exclusively on securing Kubernetes clusters and orchestration platforms.

Answer: C

Question: 206

What is the primary purpose of an Incident Response (IR) plan in security operations?

A. To ensure that all security incidents are logged and stored for auditing purposes
B. To define a structured process for identifying, mitigating, and recovering from security incidents
C. To document compliance requirements for security certifications
D. To automatically block all malicious traffic detected by security tools

Answer: B

Question: 207

Which of the following are accurate examples of types of area networks, based on their scope and functionality? (Choose two)

A. National Area Network (NAN) B. Local Area Network (LAN) C. Personal Area Network (PAN) D. Global Area Network (GAN) E. Public Area Network (PuAN)

Answer: B, C

Question: 208

What is the primary benefit of using a hosted cloud solution over maintaining an on-premises infrastructure?

A. Reduction in capital expenditures and increased operational flexibility.
B. Full customization of hardware and software configurations.
C. Elimination of all security risks associated with data breaches.
D. Complete control over all aspects of the physical and virtual infrastructure.

Answer: A

Question: 209

An organization is configuring an IPsec VPN to connect two branch offices. During the setup, they must choose a tunneling protocol for negotiating encryption keys. Which phase of IKE and protocol combination is best suited for this task?

A. IKE Phase 2 using aggressive mode to negotiate encryption keys.
B. IKE Phase 2 using quick mode to negotiate encryption parameters for the data tunnel.
C. IKE Phase 1 using quick mode to manage key exchanges.
D. IKE Phase 1 using main mode to establish a secure channel.

Answer: B

Question: 210

A security administrator is responsible for managing the firewalls in a distributed enterprise network. The administrator notices that some firewalls have outdated antivirus and application signature databases. Which of the following practices would best ensure the consistent deployment of security updates across the organization?

A. Rely on the operating system’s built-in security features instead of firewall updates.

B. Configure all firewalls to sync updates during business hours for better visibility.
C. Perform manual updates on each firewall during scheduled maintenance.
D. Enable the automatic update feature for all firewalls.

Answer: D

Question: 211

How does automation improve the efficiency of security operations in a SOC?

A. By eliminating the need for human intervention in resolving complex security incidents.
B. By developing policies and procedures for regulatory compliance frameworks.
C. By reducing alert fatigue through automated prioritization and enrichment of security events.
D. By deploying endpoint security software across an organization's devices.

Answer: C

Question: 212

Which of the following scenarios best demonstrates the use of a virtual machine (VM) in a cloud environment?

A. Hosting multiple operating systems on a developer's laptop simultaneously for software testing.
B. Deploying a microservices-based application using Docker containers to ensure resource efficiency.
C. Utilizing a lightweight serverless computing model to run functions only when triggered by an event.
D. Running a database application on a virtualized instance of an operating system in a public cloud.

Answer: D

Question: 213

A financial organization requires a secure tunneling protocol for remote employee connections. The protocol must integrate easily with Active Directory and provide native support on modern operating systems without requiring third-party software. Which protocol should they choose?

A. SSTP (Secure Socket Tunneling Protocol)
B. IKEv2/IPsec (Internet Key Exchange Version 2 with IPsec)
C. GRE (Generic Routing Encapsulation)
D. PPTP (Point-to-Point Tunneling Protocol)

Answer: A

Question: 214

Which of the following best describes the role of a container orchestration tool in cloud environments?

A. It provides load balancing, scaling, and automated deployment of containers.
B. It secures containers by encrypting all data within container volumes.

C. It ensures all containers share the same operating system kernel and libraries.
D. It creates lightweight virtual machines that run isolated applications.

Answer: A

Question: 215

Which of the following is the most effective end-user awareness practice to prevent phishing attacks?

A. Encouraging users to avoid opening any email attachments.
B. Requiring users to change their email passwords weekly.
C. Training users to identify suspicious email links and verify their authenticity before clicking.
D. Instructing users to forward all unknown emails to IT without reading them.

Answer: C

Question: 216

During the reconnaissance stage of the cyberattack lifecycle, which of the following activities is most likely performed by an attacker?

A. Installing malware to establish persistence on a compromised system.
B. Scanning for open ports on a target network.
C. Exfiltrating sensitive data to an external server.
D. Encrypting files to demand a ransom from the target.

Answer: B

Question: 217

An organization is transitioning to a DevSecOps approach to integrate security into its software development lifecycle (SDLC). Which of the following best exemplifies the principles of DevSecOps?

A. Automating security checks as part of the CI/CD pipeline to identify vulnerabilities early in the development process.
B. Assigning responsibility for security only to developers with specialized training, excluding others in the team.
C. Conducting security testing exclusively at the final stage of the SDLC to minimize disruptions to development.
D. Relying on a separate security team to perform manual reviews of code after deployment.

Answer: A

Question: 218

An organization is looking to deploy a threat prevention system to safeguard its network against advanced cyber threats. Which of the following features is most critical for an effective threat prevention system?

A. Signature-based detection
B. Network segmentation enforcement
C. Machine learning-based threat analysis
D. Perimeter firewalls for packet filtering

Answer: C

Question: 219

Which of the following statements best describes the purpose of using zones in network segmentation?

A. Zones are physical network boundaries defined by cabling and switch configurations.
B. Zones are primarily configured on switches to separate VLANs.
C. Zones are used exclusively to restrict access to specific physical devices within a network.
D. Zones group interfaces logically to enforce security policies for traffic between them.

Answer: D

Question: 220

Which of the following practices is most critical for securing containers in alignment with the "Four Cs of Cloud Native Security"

A. Avoiding orchestration tools like Kubernetes to reduce complexity.
B. Using trusted and regularly updated container images.
C. Enabling privileged mode for all containers to increase compatibility with the host.
D. Running containers as root to simplify permissions management.

Answer: B

Question: 221

A network administrator is tasked with improving the organization's cybersecurity posture by implementing a Next-Generation Firewall (NGFW). Which of the following features best distinguishes an NGFW from a traditional firewall?

A. Static IP whitelisting
B. Deep packet inspection (DPI)
C. Packet filtering based on IP and port
D. Stateful inspection of traffic

Answer: B

Question: 222

During an investigation, a cybersecurity analyst discovers that an attacker intercepted and modified data transmitted between two employees. The attacker was able to alter the contents of an email in transit without either party noticing. Which of the following best describes the type of attack observed?

A. Distributed Denial of Service (DDoS)
B. Phishing attack
C. Buffer overflow attack
D. Man-in-the-Middle (MITM) attack

Answer: D

Question: 223

Which of the following scenarios demonstrates the correct use of a proxy in network security?

A. Using a forward proxy to enforce network segmentation within a private LAN.
B. Using a reverse proxy to restrict internal employees' access to external websites.
C. Using a forward proxy to route incoming requests to internal servers in a data center.
D. Deploying a forward proxy to control and monitor employees' outbound internet traffic.

Answer: D

Question: 224

Which of the following best describes a Tier 1 analyst's role within a Security Operations Center (SOC)?

A. Managing the organization's overall cybersecurity strategy and policies.
B. Monitoring alerts, performing initial triage, and escalating issues as needed.
C. Responding to and remediating complex cybersecurity incidents involving advanced persistent threats (APTs).
D. Conducting forensic analysis of malware samples for incident investigation.

Answer: B

Question: 225

An organization implements a new cloud-based collaboration platform. The SOC team notices a lack of visibility into activities on the platform, increasing the risk of data breaches. What should the SOC team prioritize to improve visibility in this context?

A. Rely on employee reports to detect suspicious activity on the platform.
B. Increase the number of access controls to limit platform usage.
C. Use native security features of the collaboration platform, such as logging and monitoring APIs.
D. Monitor only administrative accounts to save on resource usage.

Answer: C

Question: 226

Which of the following is a common technique used in the Command-and-Control (C2) stage to avoid detection?

A. Using standard HTTP or HTTPS traffic to communicate with the compromised system

B. Deploying ransomware to encrypt files on the compromised system
C. Scanning external-facing systems for vulnerabilities
D. Sending large volumes of anomalous traffic to overwhelm detection systems

Answer: A

Question: 227

When focusing on "Code" as part of the four Cs of cloud native security, which practice would most effectively reduce the risk of introducing vulnerabilities?

A. Employing secure coding practices and integrating SAST tools into the CI/CD pipeline.
B. Relying solely on runtime monitoring tools to detect vulnerabilities in the application.
C. Regularly conducting manual code reviews without incorporating automated security scans.
D. Using hardcoded credentials within the application to ensure consistent authentication.

Answer: A

Question: 228

Which two of the following best describe the characteristics of false positive alerts in a security operations context? (Choose two)

A. A scenario where legitimate user actions are flagged as potential threats
B. An alert triggered by a benign activity incorrectly identified as malicious
C. An alert triggered by a suspicious activity with high confidence of being malicious
D. An indicator that no action is needed for the triggered alert
E. An alert triggered by malicious activity but ignored by the system

Answer: A, B

Question: 229

Which two of the following activities align with the pillars of effective security operations? (Choose two)

A. Establishing a Security Information and Event Management (SIEM) platform
B. Creating ad-hoc policies for new types of attacks
C. Relying exclusively on signature-based detection tools
D. Performing regular incident post-mortems to improve processes
E. Training staff for continuous improvement in threat response

Answer: D, E

Question: 230

What is the primary purpose of Network Address Translation (NAT) in a network?

A. To allow internal devices to communicate with external networks by translating private IP addresses to public IP addresses

B. To assign unique IP addresses to all devices in a private network
C. To encrypt data packets to ensure secure transmission over the internet
D. To increase the bandwidth of the network by reducing congestion

Answer: A

Question: 231

Which of the following best defines virtualization in the context of cloud computing?

A. Virtualization is the process of segmenting cloud networks into smaller subnetworks to enhance security and isolation.
B. Virtualization refers to the practice of distributing applications across multiple cloud service providers.
C. Virtualization is the exclusive use of containers instead of traditional VMs to optimize resource usage.

D. Virtualization is the technique of creating multiple virtual instances of computing resources from a single physical resource.

Answer: D

Question: 232

During the cyberattack lifecycle, which stage involves attackers fulfilling their ultimate goal, such as data exfiltration, encryption for ransom, or system disruption?

A. Actions on the Objective
B. Command and Control
C. Exploitation
D. Lateral Movement

Answer: A

Question: 233

In the context of security operations, which of the following best describes the role of an alert in a Security Information and Event Management (SIEM) system?

A. It is a notification triggered by predefined detection rules or anomaly thresholds.
B. It replaces the need for manual threat hunting.
C. It automatically resolves all detected security incidents.
D. It provides conclusive evidence of a breach.

Answer: A

Question: 234

A company is deploying network segmentation to isolate guest devices from internal corporate systems while allowing guests to access the internet. The IT team needs to ensure minimal configuration effort and scalability. Which network segmentation method would be the most appropriate?

A. Creating air-gapped networks for guest devices.
B. Implementing VLANs with appropriate ACLs.
C. Using firewall-based segmentation for all traffic.
D. Configuring port mirroring on guest access ports.

Answer: B

Question: 235

A company deploys a hybrid cloud architecture where part of their infrastructure is on-premises and part resides in a public cloud. Which of the following traffic patterns represents an east-west flow in this hybrid environment?

A. An on-premises Active Directory server synchronizes user credentials with a cloud-based identity provider.
B. A web application in the public cloud communicates with a backend database server hosted on the same cloud provider.
C. A developer pushes application updates from their local machine to a cloud-based Git repository.
D. A customer accesses the company's e-commerce website hosted in the public cloud.

Answer: B

Question: 236

Which of the following best defines a "security event" in the context of Security Operations?

A. A malicious activity that successfully compromises a system or network.
B. A confirmed security incident that requires immediate response from the SOC team.
C. Any observable occurrence in a system or network, regardless of its impact or intent.
D. A series of coordinated attacks detected by intrusion detection systems (IDS).

Answer: C

Question: 237

An attacker sends a carefully crafted malicious email attachment to an employee in a target organization. When the employee opens the attachment, a vulnerability in the application processing the file is triggered, allowing the attacker to execute unauthorized commands on the victim's system. At which stage of the cyberattack lifecycle does this event occur?

A. Actions on Objectives
B. Exploitation

C. Weaponization
D. Reconnaissance

Answer: B

Question: 238

Which scenario requires a properly configured default gateway for successful communication?

A. A device needs to access a server located on a different subnet.
B. A router within the network is exchanging routing updates with its peers.
C. Two devices within the same local subnet need to exchange data.
D. A device is sending a broadcast message to all devices on the local network.

Answer: A

Question: 239

A cybersecurity team is implementing network segmentation to enhance security. What is the primary advantage of network segmentation in preventing unauthorized access?

A. It ensures that devices on one segment cannot communicate with other segments unless explicitly allowed.
B. It disables all traffic between network segments by default.
C. It isolates traffic into virtual LANs (VLANs) to limit broadcast domains.
D. It allows unrestricted traffic within segments to improve performance.

Answer: A

Question: 240

Your organization wants to improve its threat prevention capabilities. They are implementing practices to block malicious traffic, detect intrusions, and reduce attack surface areas. Which two practices are essential components of an effective threat prevention system? (Choose two)

A. Disabling firewalls to improve network performance
B. Implementing a zero-trust architecture
C. Relying solely on antivirus software for endpoint security
D. Conducting regular vulnerability assessments
E. Enabling intrusion prevention systems (IPS)

Answer: B, E