CompTIA CySA+ CS0-003

100 Questions & Answers

Welcome to your complete CySA+ CS0-003 practice questions collection.
This set is designed not just to test — but also to ***teach, reinforce, and deepen your readiness for the real exam****.*

Learning Objectives and Expectations

You'll get:

- **Real-world style questions** modeled after actual CompTIA CySA+ CS0-003 scenarios.
- Structured in sets of **10 questions followed by 10 answers** for fast verification.
- Clear, concise explanations to help you **understand** the why behind each correct answer.

CySA+ CS0-003 Domains

Each domain is weighted differently on the exam. **Security Operations** is the largest, focusing on analysis, detection, and monitoring.

- Domain 1: **Security Operations (33%)**
- Domain 2: **Vulnerability Management (30%)**
- Domain 3: **Incident Response and Management (20%)**
- Domain 4: **Reporting and Communication (17%)**

Quick Reminder: How the Exam Works

- **Number of Questions**: Up to 85
- **Question Types**: Multiple Choice + Performance-Based Questions (PBQs)
- **Time Limit**: 165 minutes
- **Passing Score**: 750 / 900 (about 83%)
- **Exam Delivery**: Pearson VUE (in-person or online)
- **Recommended Experience**: Security+, Network

Questions by Domain

Domain	Title	Questions Assigned	Question Numbers
Domain 1	**Security Operations (33%)**	33 Questions	Q1, Q3, Q6–7, Q10, Q13, Q16, Q20–21, Q23, Q25, Q30–31, Q34, Q37–38, Q41, Q43, Q52, Q60, Q63–64, Q66, Q70, Q73, Q76–77, Q81–82, Q84, Q87–88, Q90
Domain 2	**Vulnerability Management (30%)**	30 Questions	Q2, Q4–5, Q11–12, Q18–19, Q22, Q24, Q28–29, Q36, Q39, Q44–45, Q49, Q54, Q58, Q61, Q68–69, Q74–75, Q79–80, Q86, Q96–97
Domain 3	**Incident Response and Management (20%)**	20 Questions	Q8–9, Q14–15, Q26–27, Q32, Q35, Q40, Q42, Q46–48, Q50–51, Q53, Q55, Q59, Q83, Q89, Q100
Domain 4	**Reporting and Communication (17%)**	17 Questions	Q17, Q33, Q56–57, Q62, Q65, Q67, Q71–72, Q78, Q85, Q91–95, Q98–99

Remember — You Don’t Need to Be Perfect to Pass

The passing score for CySA+ is about **83%.** That means you can miss **up to 14 questions** and still pass.

Don’t stress over a few tricky questions. What matters most is your ability to:

- Think like an analyst
- Prioritize and triage incidents
- Analyze and respond under pressure
- Assess findings in context

Questions 1–10

Q1.
What is the FIRST action an analyst should take when a critical alert is triggered in the SIEM?
A) Notify executive leadership
B) Delete the alert to avoid duplicates
C) Investigate and validate the alert
D) Reboot the affected system

Q2.
Which of the following BEST describes a use case for a threat intelligence platform (TIP)?
A) Encrypting outbound web traffic
B) Automating remediation of alerts
C) Aggregating indicators of compromise from external sources
D) Creating firewall rules for internal VLANs

Q3.
An attacker used stolen credentials to access a cloud console and launch cryptomining instances. Which ATT&CK tactic does this MOST align with?
A) Execution
B) Credential Access
C) Initial Access
D) Impact

Q4.
What type of scanning provides the most comprehensive results by logging into the host system during scanning?
A) External
B) Passive
C) Credentialed
D) Non-credentialed

Q5.
Which of the following is a PRIMARY function of a SOAR platform?
A) Encrypting SIEM logs

B) Generating monthly compliance reports
C) Automating and orchestrating security response workflows
D) Detecting zero-day threats in network packets

Q6.
What type of vulnerability allows an attacker to include and execute unauthorized local files on a web server?
A) XSS
B) LFI
C) CSRF
D) SQLi

Q7.
An analyst is reviewing logs and notices a workstation making DNS requests every 30 seconds to random subdomains. What type of activity is this MOST likely?
A) Normal DNS load balancing
B) DNS exfiltration using data tunneling
C) Load testing from an internal script
D) Endpoint antivirus signature update

Q8.
Which of the following actions would MOST likely occur during the containment phase of incident response?
A) Generating a public incident report
B) Blocking malicious IP addresses
C) Performing forensic imaging of affected endpoints
D) Analyzing root cause of the incident

Q9.
What log source would BEST help detect brute-force attempts against an SSH server?
A) Web server logs
B) Packet captures from DNS
C) /var/log/auth.log
D) Antivirus quarantine logs

Q10.
Which of the following attack types relies on abusing legitimate system tools like

PowerShell or WMI?
A) Watering hole
B) Living off the Land
C) SQL Injection
D) Cross-Site Scripting

Answers 1–10

A1.
Answer: C) Investigate and validate the alert
Explanation: The analyst must first confirm whether the alert is real before escalating or acting on it.

A2.
Answer: C) Aggregating indicators of compromise from external sources
Explanation: A Threat Intelligence Platform (TIP) collects, enriches, and correlates IOCs from multiple sources to enhance threat awareness.

A3.
Answer: D) Impact
Explanation: Cryptomining consumes resources and causes business disruption, which aligns with the Impact tactic in MITRE ATT&CK.

A4.
Answer: C) Credentialed
Explanation: Credentialed scans log into the host to provide accurate, in-depth vulnerability detection.

A5.
Answer: C) Automating and orchestrating security response workflows
Explanation: SOAR tools are designed to automate and streamline incident response and remediation tasks.

A6.
Answer: B) LFI
Explanation: Local File Inclusion (LFI) allows attackers to trick a web app into executing or revealing files on the server.

A7.
Answer: B) DNS exfiltration using data tunneling
Explanation: Frequent DNS queries with randomized subdomains are common in covert data exfiltration via DNS tunneling.

A8.
Answer: B) Blocking malicious IP addresses
Explanation: Containment is about stopping the threat from spreading — blocking C2 IPs is a key tactic.

A9.
Answer: C) /var/log/auth.log
Explanation: On Linux systems, this log contains authentication attempts and is key for identifying brute-force login behavior.

A10.
Answer: B) Living off the Land
Explanation: Living off the Land (LotL) techniques abuse legitimate tools like PowerShell to evade detection.

Questions 11–20

Q11.
A vulnerability scanner reports that a public-facing server has OpenSSL 1.0.1e installed. What should an analyst do NEXT to validate the finding?
A) Submit a risk acceptance form
B) Launch a denial-of-service test
C) Check the actual version running on the host
D) Ignore the finding as a false positive

Q12.
Which of the following BEST describes an IOC?
A) Security policy defining user access
B) Behavior profile used for insider threat detection
C) Evidence of a security breach or compromise
D) Traffic log showing bandwidth consumption

Q13.
During a threat hunt, an analyst uses MITRE ATT&CK to map observed behavior. What is the PRIMARY reason to use this framework?
A) To validate patch management effectiveness
B) To build password policies
C) To track and categorize adversary tactics
D) To document log retention policies

Q14.
Which of the following would MOST likely be used to analyze an unknown binary in a safe environment?
A) IDS
B) SIEM
C) Sandbox
D) Load balancer

Q15.
What type of control is an organization using when it forces password changes every 90 days via a policy?
A) Physical

B) Technical
C) Administrative
D) Corrective

Q16.
Which of the following is the MOST effective way to reduce alert fatigue in a SOC?
A) Hire more Tier 1 analysts
B) Add more detection rules
C) Tune SIEM use cases and reduce false positives
D) Limit alerting to critical systems only

Q17.
An analyst identifies a file named `invoice.scr` sent via email. What's the MOST likely reason this is suspicious?
A) It's a Microsoft Office document
B) SCR files are typically legitimate invoices
C) The file type is an executable disguised as a document
D) SCR files are used by Adobe

Q18.
Which component of the Diamond Model identifies the malware or exploit used in an attack?
A) Victim
B) Infrastructure
C) Capability
D) Adversary

Q19.
An organization cannot patch a critical server due to application dependencies. What should be done NEXT?
A) Take the server offline
B) Disable logging temporarily
C) Apply a compensating control
D) Remove all admin accounts

Q20.
An attacker exploits a misconfigured S3 bucket to access public files. What type of

vulnerability is this?
A) Injection
B) Cryptographic failure
C) Insecure configuration
D) Broken authentication

Answers 11–20

A11.
Answer: C) Check the actual version running on the host
Explanation: Always validate scan findings by confirming software versions manually before escalating or patching.

A12.
Answer: C) Evidence of a security breach or compromise
Explanation: IOCs are signs that a system or environment has been attacked or breached.

A13.
Answer: C) To track and categorize adversary tactics
Explanation: MITRE ATT&CK is used to map attacker behavior to known tactics and techniques.

A14.
Answer: C) Sandbox
Explanation: A sandbox allows analysts to execute suspicious files in isolation to observe behavior safely.

A15.
Answer: C) Administrative
Explanation: Policies like password expiration are administrative controls—they guide user behavior.

A16.
Answer: C) Tune SIEM use cases and reduce false positives

Explanation: Alert fatigue is best addressed by tuning the SIEM to reduce noise and increase alert relevance.

A17.
Answer: C) The file type is an executable disguised as a document
Explanation: .scr is an executable file type (screensaver), often used to bypass filters by masquerading as documents.

A18.
Answer: C) Capability
Explanation: In the Diamond Model, Capability refers to the tools, malware, or techniques used by the attacker.

A19.
Answer: C) Apply a compensating control
Explanation: If a patch can't be applied, use network segmentation, stricter firewall rules, or enhanced monitoring to reduce risk.

A20.
Answer: C) Insecure configuration
Explanation: A misconfigured storage bucket exposing data is an example of poor configuration, not a code flaw.

Questions 21–30

Q21.
An attacker performs a scan and finds port 3389 open on a server. What service is MOST likely being targeted?
A) FTP
B) SSH
C) RDP
D) SMTP

Q22.
What type of scan would BEST simulate an external attacker probing an organization's perimeter?
A) Internal, credentialed
B) External, non-credentialed
C) Internal, agent-based
D) External, credentialed

Q23.
Which of the following tools would MOST likely be used to search historical log data for failed login patterns?
A) Nmap
B) Splunk
C) Wireshark
D) OpenVAS

Q24.
An analyst sees a surge in outbound traffic from a workstation late at night. What's the BEST next step?
A) Reboot the machine
B) Escalate to HR
C) Investigate logs for possible data exfiltration
D) Email the user to ask what they were doing

Q25.
Which of the following frameworks is designed to describe attacker behavior across various phases like Initial Access and Lateral Movement?

A) NIST
B) STRIDE
C) MITRE ATT&CK
D) Cyber Kill Chain

Q26.
An analyst is investigating a phishing email. What element in the email header should be examined to verify the sender?
A) Subject line
B) DKIM signature
C) Font size
D) Image alt text

Q27.
Which of the following log sources would BEST identify a brute-force attack against a web application login form?
A) Firewall logs
B) Apache access logs
C) Antivirus logs
D) DHCP logs

Q28.
What is the PRIMARY benefit of applying a zero trust model in network design?
A) It removes the need for firewalls
B) It limits insider threat by enforcing strict access validation
C) It allows shared admin credentials across departments
D) It blocks all encrypted traffic by default

Q29.
An attacker uses a macro inside a Word document to download and run malware. What technique does this represent?
A) Defense Evasion
B) Lateral Movement
C) Initial Access
D) Persistence

Q30.
What type of response is being used if an IDS alert triggers an automatic firewall rule to block an IP address?
A) Passive
B) Forensic
C) Manual
D) Automated

Answers 21–30

A21.
Answer: C) RDP
Explanation: Port 3389 is the default port for Remote Desktop Protocol (RDP), commonly used in attacks for remote access.

A22.
Answer: B) External, non-credentialed
Explanation: This type of scan mimics how an outsider with no credentials would see the network.

A23.
Answer: B) Splunk
Explanation: Splunk is a SIEM tool designed to analyze and search large volumes of logs.

A24.
Answer: C) Investigate logs for possible data exfiltration
Explanation: A sudden spike in outbound traffic, especially at off-hours, may indicate data being stolen.

A25.
Answer: C) MITRE ATT&CK
Explanation: MITRE ATT&CK provides detailed mapping of adversary tactics and techniques throughout the attack lifecycle.

A26.
Answer: B) DKIM signature
Explanation: DomainKeys Identified Mail (DKIM) is used to verify the authenticity of an email's sender domain.

A27.
Answer: B) Apache access logs
Explanation: Web server logs (like Apache) show repeated login attempts that could indicate brute-force attacks.

A28.
Answer: B) It limits insider threat by enforcing strict access validation
Explanation: Zero Trust assumes no implicit trust — every access must be verified, reducing risks even from internal users.

A29.
Answer: C) Initial Access
Explanation: Using a malicious document to gain entry is part of the initial access phase in an attack chain.

A30.
Answer: D) Automated
Explanation: When detection tools trigger pre-defined actions (like blocking IPs), it's an automated response.

Questions 31–40

Q31.
Which of the following BEST describes the function of a SIEM?
A) Provides DNS resolution
B) Blocks unauthorized USB devices
C) Collects and correlates log data for analysis
D) Performs full-disk encryption

Q32.
What term refers to a threat that is specifically crafted to avoid detection by antivirus and other automated tools?
A) Logic bomb
B) Zero-day
C) Polymorphic malware
D) Spyware

Q33.
A vulnerability is discovered in a legacy system that cannot be patched. What’s the BEST approach?
A) Accept the risk and take no further action
B) Reboot the system regularly
C) Apply compensating controls and isolate the system
D) Disable all monitoring to reduce alert fatigue

Q34.
Which of the following log types would BEST help trace lateral movement in a Windows domain environment?
A) DNS logs
B) Active Directory authentication logs
C) Antivirus quarantine logs
D) DHCP lease logs

Q35.
What is the PRIMARY goal of the recovery phase in incident response?
A) Identify the root cause of the incident
B) Publicly disclose the incident

C) Return systems to normal operation securely
D) Shut down all affected assets permanently

Q36.
What’s the BEST method to reduce the attack surface of a Windows server?
A) Install a faster SSD
B) Disable unnecessary services and ports
C) Increase CPU cores
D) Enable screen savers with password

Q37.
Which framework outlines seven stages from Reconnaissance to Actions on Objectives?
A) Diamond Model
B) STRIDE
C) MITRE ATT&CK
D) Cyber Kill Chain

Q38.
Which of the following is an example of an indicator of attack (IOA) rather than an indicator of compromise (IOC)?
A) Known malware hash found on disk
B) Registry key altered by ransomware
C) Unusual use of PowerShell during normal business hours
D) Outbound traffic to a known malicious IP

Q39.
What is the PRIMARY purpose of using a honeypot in an enterprise environment?
A) Encrypt sensitive data
B) Divert attackers and study their behavior
C) Act as a backup domain controller
D) Replace IDS/IPS devices

Q40.
Which metric is MOST useful when evaluating how quickly an organization detects threats?
A) CVSS score

B) SLA rating
C) MTTD
D) RTO

Answers 31–40

A31.
Answer: C) Collects and correlates log data for analysis
Explanation: SIEM platforms aggregate logs from multiple systems and analyze them for signs of malicious activity.

A32.
Answer: C) Polymorphic malware
Explanation: Polymorphic malware constantly changes its code to evade detection mechanisms.

A33.
Answer: C) Apply compensating controls and isolate the system
Explanation: If patching is not possible, use compensating controls like network isolation or enhanced monitoring.

A34.
Answer: B) Active Directory authentication logs
Explanation: AD logs show login events and can reveal lateral movement through account activity across systems.

A35.
Answer: C) Return systems to normal operation securely
Explanation: Recovery aims to restore services and systems in a safe, validated manner post-incident.

A36.
Answer: B) Disable unnecessary services and ports

Explanation: Reducing the number of exposed services and ports minimizes the attack surface of any system.

A37.
Answer: D) Cyber Kill Chain
Explanation: The Cyber Kill Chain includes Recon, Weaponization, Delivery, Exploitation, Installation, C2, and Actions.

A38.
Answer: C) Unusual use of PowerShell during normal business hours
Explanation: IOAs indicate behavior patterns (like live attacks), whereas IOCs are artifacts of past compromise.

A39.
Answer: B) Divert attackers and study their behavior
Explanation: Honeypots are decoy systems designed to lure attackers and gather intelligence on their techniques.

A40.
Answer: C) MTTD
Explanation: Mean Time to Detect (MTTD) measures how quickly threats are identified after they begin.

Questions 41–50

Q41.
Which of the following BEST describes a “false positive” in a SIEM alert?
A) An alert that accurately detects malicious activity
B) A real attack that goes undetected
C) A benign activity incorrectly flagged as malicious
D) A user who reports a phishing email

Q42.
What type of control is an automated system that isolates infected endpoints once malware is detected?
A) Physical
B) Detective
C) Preventive
D) Corrective

Q43.
Which of the following is MOST useful for tracking unauthorized changes to critical system files?
A) NetFlow
B) Host-based IDS
C) DNS sinkhole
D) Router ACL

Q44.
Which technique is commonly used by attackers to evade signature-based detection?
A) Reverse shell
B) Port knocking
C) Packet fragmentation
D) Code obfuscation

Q45.
An organization is reviewing user activity during an insider threat investigation. Which data source is MOST useful?
A) SIEM alerts
B) Firewall logs

C) User behavior analytics (UBA)
D) DNS request logs

Q46.
What type of threat involves users intentionally or unintentionally causing harm from within the organization?
A) Insider threat
B) Nation-state
C) External threat actor
D) Script kiddie

Q47.
What is the BEST response if a phishing simulation shows that 30% of users clicked a fake link?
A) Disable user accounts
B) Remove email access
C) Provide targeted awareness training
D) Fire employees who clicked

Q48.
What type of log would BEST show details about application-layer activity on a web server?
A) Firewall logs
B) Syslog
C) Web server access logs
D) Antivirus event logs

Q49.
During a red team exercise, simulated attackers successfully exfiltrate data. What should the blue team do FIRST?
A) Wipe the servers
B) Update SIEM software
C) Validate and document the findings
D) Escalate to federal law enforcement

Q50.
What's the PRIMARY benefit of integrating threat intelligence into SIEM workflows?

A) Encrypt all SIEM traffic
B) Allow real-time response to network outages
C) Enrich alerts with external context for faster triage
D) Automatically patch vulnerable software

Answers 41–50

A41.
Answer: C) A benign activity incorrectly flagged as malicious
Explanation: A false positive is when a detection system triggers an alert for something that's actually harmless.

A42.
Answer: D) Corrective
Explanation: Isolating an endpoint to stop malware spread is a corrective control — it addresses damage already done.

A43.
Answer: B) Host-based IDS
Explanation: HIDS monitors system-level changes such as file modifications, which can reveal unauthorized tampering.

A44.
Answer: D) Code obfuscation
Explanation: Obfuscation disguises malware code to bypass signature-based antivirus and detection tools.

A45.
Answer: C) User behavior analytics (UBA)
Explanation: UBA detects anomalies in user behavior patterns that may indicate insider threats.

A46.
Answer: A) Insider threat

Explanation: An insider threat comes from within the organization, whether intentional or accidental.

A47.
Answer: C) Provide targeted awareness training
Explanation: Follow-up training helps reduce future phishing risk and is a positive, constructive response.

A48.
Answer: C) Web server access logs
Explanation: Web access logs contain HTTP requests, status codes, and client IPs — useful for application-level review.

A49.
Answer: C) Validate and document the findings
Explanation: During a red team exercise, the first step is to validate what occurred and document it for analysis.

A50.
Answer: C) Enrich alerts with external context for faster triage
Explanation: Threat intelligence integration helps analysts prioritize alerts by linking them to known threats.

Questions 51–60

Q51.
Which of the following would BEST help identify a persistent threat on an endpoint after reboot?
A) Packet sniffer
B) Volatile memory dump
C) Scheduled task and registry inspection
D) DNS query analysis

Q52.
A SOC analyst receives an alert for multiple failed logins followed by a successful login from the same IP. What is the MOST likely explanation?
A) Reconnaissance
B) Brute-force attack
C) Drive-by download
D) Misconfigured firewall

Q53.
What is the FIRST step in conducting a root cause analysis after a security incident?
A) Isolate affected systems
B) Interview stakeholders
C) Review logs and available evidence
D) Update firewall rules

Q54.
Which of the following BEST defines a compensating control?
A) Control used to prevent social engineering
B) Backup control when primary is too expensive or infeasible
C) Control that verifies password strength
D) Legal requirement for HIPAA compliance

Q55.
What tactic in the MITRE ATT&CK framework involves attackers creating new user accounts to maintain access?
A) Privilege Escalation
B) Defense Evasion

C) Persistence
D) Credential Access

Q56.
Which protocol is commonly used for time synchronization and is important for correlating logs across systems?
A) DHCP
B) FTP
C) SNMP
D) NTP

Q57.
What is the PRIMARY purpose of a post-incident review (lessons learned)?
A) Punish the team that missed the alert
B) Notify law enforcement
C) Improve processes and reduce future risk
D) Restore data from backups

Q58.
Which of the following is a behavioral-based detection method?
A) Checking MD5 hash against VirusTotal
B) Using a YARA rule for signature matching
C) Detecting use of PowerShell at 2AM on a sales user laptop
D) Scanning a ZIP file with antivirus

Q59.
An attacker scans a web application and sends payloads like ../../../etc/passwd in input fields. What type of attack is this?
A) Cross-Site Scripting
B) Directory Traversal
C) Command Injection
D) CSRF

Q60.
Which control type MOST directly supports the "Detection" function of the NIST Cybersecurity Framework?
A) SIEM

B) Firewall
C) Backup system
D) MFA

Answers 51–60

A51.
Answer: C) Scheduled task and registry inspection
Explanation: Persistent malware often uses scheduled tasks or registry keys to re-execute after reboot.

A52.
Answer: B) Brute-force attack
Explanation: Multiple failed login attempts followed by a success typically indicates a brute-force attack.

A53.
Answer: C) Review logs and available evidence
Explanation: Understanding what happened starts with analyzing the available data before taking other actions.

A54.
Answer: B) Backup control when primary is too expensive or infeasible
Explanation: A compensating control provides an alternative safeguard when the ideal control isn't possible.

A55.
Answer: C) Persistence
Explanation: Creating new accounts is a method used by attackers to maintain long-term access—classified under persistence.

A56.
Answer: D) NTP

Explanation: Network Time Protocol (NTP) ensures consistent timestamps across logs and systems.

A57.
Answer: C) Improve processes and reduce future risk
Explanation: The main goal of post-incident reviews is to identify what went wrong and how to prevent recurrence.

A58.
Answer: C) Detecting use of PowerShell at 2AM on a sales user laptop
Explanation: This is a behavior anomaly detection—indicating suspicious use based on context.

A59.
Answer: B) Directory Traversal
Explanation: Using ../../../ attempts to access files outside of the allowed directory.

A60.
Answer: A) SIEM
Explanation: A SIEM is central to detection—it collects, correlates, and alerts on suspicious activity.

Questions 61–70

Q61.
Which of the following would MOST likely detect suspicious file access patterns on a user’s workstation?
A) Network firewall
B) Host-based intrusion detection system (HIDS)
C) Router ACL
D) DNS log analysis

Q62.
Which regulatory framework is focused on protecting healthcare data in the United States?
A) GDPR
B) SOX
C) HIPAA
D) NIST CSF

Q63.
An attacker gains access to an employee’s email and sends phishing messages internally. Which MITRE ATT&CK tactic is being used?
A) Credential Access
B) Initial Access
C) Lateral Movement
D) Execution

Q64.
What would be the BEST next step after identifying the presence of malware on a business-critical server?
A) Immediately shut down the server
B) Wipe and rebuild the server
C) Perform containment and preserve forensic evidence
D) Notify all customers

Q65.
Which of the following BEST explains the use of the CVSS score in vulnerability management?

A) Prioritizes which threats are trending in social media
B) Scores business risk for insurance purposes
C) Rates severity of vulnerabilities to support prioritization
D) Assigns legal responsibility for a data breach

Q66.
Which tool is BEST used to analyze suspicious outbound connections from endpoints?
A) Firewall ruleset
B) Wireshark
C) Nessus
D) OpenVAS

Q67.
What is the PRIMARY benefit of using YARA rules in a malware investigation?
A) Prevent brute-force attacks
B) Block command-line tools
C) Match malware patterns for detection
D) Perform port scanning

Q68.
Which incident response phase involves removing malware and fixing vulnerabilities?
A) Containment
B) Eradication
C) Detection
D) Recovery

Q69.
Which of the following BEST describes "mean time to recover" (MTTR)?
A) Time between incident start and first alert
B) Time to fully restore operations after an incident
C) Time to detect a phishing email
D) Time between patching cycles

Q70.
What is the PRIMARY purpose of a change management policy in cybersecurity operations?
A) Ensure all updates are installed automatically

B) Allow all developers to make production changes freely
C) Prevent unapproved or untracked modifications
D) Disable redundant system features

Answers 61–70

A61.
Answer: B) Host-based intrusion detection system (HIDS)
Explanation: HIDS monitors file and process activity on individual hosts, helping detect local anomalies.

A62.
Answer: C) HIPAA
Explanation: HIPAA governs the privacy and security of protected health information (PHI) in the U.S.

A63.
Answer: C) Lateral Movement
Explanation: Using a compromised internal account to spread phishing is lateral movement within the network.

A64.
Answer: C) Perform containment and preserve forensic evidence
Explanation: The priority is to stop spread and collect evidence before rebooting or wiping systems.

A65.
Answer: C) Rates severity of vulnerabilities to support prioritization
Explanation: CVSS provides a numerical rating of how dangerous a vulnerability is, guiding patching efforts.

A66.
Answer: B) Wireshark

Explanation: Wireshark captures and analyzes network packets, ideal for spotting suspicious outbound traffic.

A67.
Answer: C) Match malware patterns for detection
Explanation: YARA rules help analysts detect known malware by matching specific patterns in files or memory.

A68.
Answer: B) Eradication
Explanation: This phase involves removing threats and fixing exploited vulnerabilities to prevent recurrence.

A69.
Answer: B) Time to fully restore operations after an incident
Explanation: MTTR measures the time needed to recover operations to a normal, functional state.

A70.
Answer: C) Prevent unapproved or untracked modifications
Explanation: Change management ensures that system changes are reviewed, tested, and approved before deployment.

Questions 71–80

Q71.
Which of the following techniques would MOST effectively help identify vulnerable open ports on internal systems?
A) Log review
B) Nmap scan
C) NetFlow analysis
D) DNS lookup

Q72.
Which security concept ensures that a user cannot deny performing an action, such as sending an email?
A) Confidentiality
B) Non-repudiation
C) Least privilege
D) Integrity

Q73.
An organization uses a security tool to simulate malware attacks in a sandbox to observe behavior. What is this process called?
A) Reverse engineering
B) Behavioral analysis
C) Fuzz testing
D) Static analysis

Q74.
Which logging feature BEST supports proper forensic investigations?
A) Syslog formatting
B) Remote logging
C) High-frequency log rotation
D) Obfuscating sensitive log data

Q75.
What is the PRIMARY purpose of a vulnerability scan schedule?
A) Detect data exfiltration attempts
B) Ensure regular identification of weaknesses

C) Block malicious traffic before it enters
D) Monitor baseline network behavior

Q76.
Which of the following is MOST helpful in detecting credential stuffing attacks?
A) Increased CPU load
B) Excessive 200 OK HTTP responses
C) Spike in failed login attempts across multiple accounts
D) Elevated DNS traffic

Q77.
An attacker uses a script that submits thousands of login attempts using different usernames and passwords. What type of attack is this?
A) Password spraying
B) Brute-force
C) Cross-site request forgery
D) Credential harvesting

Q78.
Which control type BEST describes a legal document that outlines expectations of third-party vendors handling sensitive data?
A) Preventive
B) Administrative
C) Technical
D) Detective

Q79.
What log file is MOST useful to analyze user login failures on a Linux system?
A) /var/log/messages
B) /var/log/dmesg
C) /var/log/auth.log
D) /var/log/cron

Q80.
Which of the following would MOST likely appear in a DAST scan report?
A) Missing firewall rule
B) Open port 445

C) SQL injection vulnerability
D) Incorrect file permissions

Answers 71–80

A71.
Answer: B) Nmap scan
Explanation: Nmap actively scans networks and systems for open ports and services.

A72.
Answer: B) Non-repudiation
Explanation: Non-repudiation ensures that actions can be tied to individuals, often using digital signatures.

A73.
Answer: B) Behavioral analysis
Explanation: Observing a file's runtime behavior in a sandbox is behavioral analysis.

A74.
Answer: B) Remote logging
Explanation: Logging to a remote system prevents tampering and preserves evidence for forensic use.

A75.
Answer: B) Ensure regular identification of weaknesses
Explanation: Scheduled scans help continuously detect vulnerabilities as systems and software change.

A76.
Answer: C) Spike in failed login attempts across multiple accounts
Explanation: Credential stuffing involves rapid login attempts across many accounts using leaked credentials.

A77.
Answer: B) Brute-force
Explanation: Brute-force attacks try numerous username-password combinations until access is gained.

A78.
Answer: B) Administrative
Explanation: Contracts and policies are administrative controls that define security expectations and obligations.

A79.
Answer: C) /var/log/auth.log
Explanation: This log tracks authentication attempts and failures on most Linux systems.

A80.
Answer: C) SQL injection vulnerability
Explanation: DAST tools test running applications and often identify input-based vulnerabilities like SQLi.

Questions 81–90

Q81.
What is the PRIMARY objective of the containment phase in the incident response lifecycle?
A) Prevent further spread or damage
B) Eliminate all malicious files
C) Restore normal operations immediately
D) Notify all affected users

Q82.
An alert indicates multiple failed login attempts followed by a successful login and unusual outbound traffic. Which tactic in MITRE ATT&CK is most aligned?
A) Discovery
B) Execution
C) Exfiltration
D) Privilege Escalation

Q83.
Which of the following would BEST detect unauthorized software being installed on endpoints?
A) Web proxy
B) NetFlow
C) Host-based IDS
D) Firewall

Q84.
Which document formally outlines procedures, roles, and responsibilities during security events?
A) Service Level Agreement (SLA)
B) Incident Response Plan (IRP)
C) Data Loss Prevention Policy
D) Acceptable Use Policy (AUP)

Q85.
Which of the following is a characteristic of a zero-day vulnerability?
A) It's publicly disclosed but not yet exploited

B) It’s already patched by vendors
C) It’s unknown to the vendor and has no available fix
D) It requires physical access to exploit

Q86.
A security team uses automation to enrich alerts with threat intelligence before analyst review. What is this an example of?
A) SIEM alert tuning
B) PBQ execution
C) SOAR orchestration
D) Penetration testing

Q87.
What is a key benefit of centralizing logs in a SIEM?
A) It reduces the need for encryption
B) It eliminates insider threats
C) It enables correlation and pattern detection
D) It replaces antivirus software

Q88.
An attacker scans for devices using default SNMP community strings. What are they MOST likely trying to exploit?
A) Privilege escalation
B) Insecure API endpoints
C) Misconfigured management interfaces
D) SSL certificate weaknesses

Q89.
What should analysts review FIRST when triaging a new alert in the SIEM?
A) The company’s security awareness policy
B) Threat intelligence reports from third parties
C) Contextual data: asset, user, and source information
D) The firewall vendor’s patch history

Q90.
Which of the following is an example of a detective control?
A) Firewall blocking access

B) Antivirus deleting malware
C) IDS logging and alerting on port scan activity
D) VPN requiring MFA

Answers 81–90

A81.
Answer: A) Prevent further spread or damage
Explanation: Containment aims to isolate the threat before it can move laterally or escalate.

A82.
Answer: C) Exfiltration
Explanation: Unusual outbound traffic after compromise suggests data is being exfiltrated.

A83.
Answer: C) Host-based IDS
Explanation: HIDS can detect unauthorized software installations or changes to system files.

A84.
Answer: B) Incident Response Plan (IRP)
Explanation: The IRP defines roles, escalation paths, and procedures during security incidents.

A85.
Answer: C) It's unknown to the vendor and has no available fix
Explanation: A zero-day is a previously unknown vulnerability with no patch at the time of discovery or exploitation.

A86.
Answer: C) SOAR orchestration

Explanation: SOAR automates and orchestrates response actions, such as enriching alerts with intel before review.

A87.
Answer: C) It enables correlation and pattern detection
Explanation: SIEMs centralize logs to identify connections across multiple data sources for threat detection.

A88.
Answer: C) Misconfigured management interfaces
Explanation: SNMP with default community strings is often used in management interfaces, which attackers target for reconnaissance or control.

A89.
Answer: C) Contextual data: asset, user, and source information
Explanation: Understanding what system or user is involved helps analysts assess the alert's risk and validity quickly.

A90.
Answer: C) IDS logging and alerting on port scan activity
Explanation: Detective controls monitor for malicious behavior and alert security teams without blocking.

Questions 91–100

Q91.
Which term describes the likelihood that a vulnerability will be exploited, combined with the impact of that exploitation?
A) Exposure
B) Compliance
C) Risk
D) Residual threat

Q92.
An analyst uses historical data to detect activity that deviates from normal behavior. What method is being used?
A) Signature-based detection
B) Anomaly-based detection
C) Whitelisting
D) Rule-based correlation

Q93.
What does the "T" in the TTPs acronym stand for in cybersecurity threat analysis?
A) Trigger
B) Tactic
C) Timeframe
D) Transport

Q94.
What is the MOST effective way to ensure log integrity during a forensic investigation?
A) Obfuscate PII from logs
B) Rotate logs every 24 hours
C) Use centralized logging with hashing
D) Enable SNMP traps

Q95.
Which security principle focuses on ensuring that systems and data are accessible when needed?
A) Integrity
B) Resilience

C) Availability
D) Redundancy

Q96.
Which tool would BEST help a security analyst identify vulnerabilities in systems that are already deployed in production?
A) Nmap
B) Nikto
C) Nessus
D) Wireshark

Q97.
During a routine scan, a system is flagged for having port 445 open. What service is likely exposed?
A) SSH
B) SMB
C) FTP
D) Telnet

Q98.
What log source would BEST help investigate unauthorized database access?
A) Web access logs
B) Application logs
C) Database audit logs
D) DNS logs

Q99.
What is the PRIMARY use of the STIX format in threat intelligence?
A) Define firewall rules
B) Visualize phishing campaigns
C) Structure threat data for automated sharing
D) Collect vulnerability metrics

Q100.
An attacker is using a compromised internal host to pivot into other systems. Which MITRE ATT&CK tactic is being used?
A) Execution

B) Lateral Movement
C) Exfiltration
D) Persistence

Answers 91–100

A91.
Answer: C) Risk
Explanation: Risk combines the likelihood of exploitation with the potential impact on the organization.

A92.
Answer: B) Anomaly-based detection
Explanation: Anomaly detection compares current behavior against established baselines to identify outliers.

A93.
Answer: B) Tactic
Explanation: TTPs = Tactics, Techniques, and Procedures, which describe how threat actors operate.

A94.
Answer: C) Use centralized logging with hashing
Explanation: Centralizing logs and applying hashes ensures they haven't been tampered with.

A95.
Answer: C) Availability
Explanation: Availability ensures that resources are accessible when needed by authorized users.

A96.
Answer: C) Nessus

Explanation: Nessus is a vulnerability scanner that helps identify known vulnerabilities in live systems.

A97.
Answer: B) SMB
Explanation: Port 445 is used for SMB (Server Message Block), often exploited in lateral movement attacks.

A98.
Answer: C) Database audit logs
Explanation: These logs capture access and query activity within the database.

A99.
Answer: C) Structure threat data for automated sharing
Explanation: STIX (Structured Threat Information Expression) allows standard sharing of threat intelligence.

A100.
Answer: B) Lateral Movement
Explanation: Lateral movement involves using a compromised host to access additional systems internally.