CYSA+ Certification Test Bank

Welcome to the Bare Metal Cyber Audio Academy, an audio-first learning library built to help you pass certification exams through clear, practical instruction you can use anywhere. Each course is designed for busy learners who want structured coverage of the exam objectives, high-yield recall practice, and scenario-ready decision skills without needing slides, labs, or extra downloads. The handouts that come with each course are meant to reinforce what you hear, giving you quick reference material like question banks, key definitions, and review prompts you can use before a study session or right before exam day. The goal is simple: help you recognize what the exam is asking, select the best answer confidently, and avoid common traps. You can find the full catalog of courses, books, and resources at https://baremetalcyber.com/, where everything is organized to support steady progress from first listen to test-day readiness.

Find more for free at BareMetalCyber.com

Contents

Bank 1

1. You receive a vulnerability scan report showing several findings, including one with the highest severity score. The system with the highest score is not widely exposed, while another lower-scored finding sits on a critical, exposed system. What is the best next step?
   A. Fix the vulnerability with the highest score first because severity always equals risk
   B. Ignore scoring and remediate vulnerabilities in alphabetical order
   C. Prioritize remediation using severity plus context like exposure and asset criticality
   D. Accept all risks until the next scanning cycle completes

2. A SIEM alert fires for repeated authentication attempts, but the activity matches a known maintenance window and a normal admin pattern in past logs. What is the most accurate interpretation of this alert?
   A. It is automatically a confirmed incident because the SIEM alerted
   B. It is likely a false positive and should be validated using context and baselines
   C. It must be lateral movement and requires immediate network segmentation changes
   D. It indicates data exfiltration and requires eradication first

3. An analyst notices a workstation making small outbound connections to the same external destination on a steady schedule. The traffic pattern is consistent over time and stands out from normal behavior. What is this pattern most commonly called in exam context?
   A. Asset discovery
   B. Normalization
   C. Beaconing
   D. Business continuity

4. During an incident, a responder wants to isolate a host immediately. Another responder warns that the team still needs to preserve key artifacts to understand what happened. Which incident response step best matches limiting damage while preserving options for later actions?
   A. Eradication
   B. Containment
   C. Root cause analysis
   D. Risk acceptance

5. You need more accurate vulnerability details from several servers because unauthenticated scanning is producing incomplete results. Which scan approach best fits that goal?
   A. Credentialed scan
   B. Watering hole attack
   C. Threat intelligence
   D. Baseline

6. A team says, “We can’t apply the ideal fix right now, but we can reduce exposure with an alternative safeguard and document the exception.” What concept does this describe?
   A. Time synchronization
   B. Compensating control
   C. Threat hunting
   D. Digital forensics

7. An investigation depends on building a reliable timeline across endpoint logs, network logs, and identity logs, but the timestamps do not line up between systems. What foundational control is most directly missing?
   A. Playbook
   B. Vulnerability management
   C. Time synchronization
   D. Sandboxing

8. You plan to proactively search across endpoints and logs for signs of attacker activity that might not trigger existing alerts, using a hypothesis and pivoting from weak signals. What is the best term for this activity?
   A. Log correlation
   B. Detection engineering
   C. Threat hunting
   D. Normalization

9. A manager asks for a decision on a known security risk that the organization understands but is not planning to mitigate right now, and the decision must be formal. What is the best label for that action?
   A. Risk acceptance
   B. Tuning
   C. Incident classification
   D. Allowlisting

10. A responder collects evidence that may later be reviewed outside the immediate team. The responder needs to document how the evidence was collected, handled, transferred, and stored to preserve integrity. What is the key concept being applied?
    A. Baseline
    B. Chain of custody
    C. Mean time to detect
    D. Advanced persistent threat

---

1. Correct Answer: C. Prioritize remediation using severity plus context like exposure and asset criticality
   Explanation: Vulnerability prioritization uses severity plus real-world context to rank what to fix first. The exam commonly tests choosing the “fix first” item when the highest score is not the highest risk.
2. Correct Answer: B. It is likely a false positive and should be validated using context and baselines
   Explanation: A false positive is an alert that looks malicious even though the underlying event is benign. The exam expects validation using context like baselines and known change activity before escalation.
3. Correct Answer: C. Beaconing
   Explanation: Beaconing is periodic, patterned communication from a host to an external destination. On the exam, it is treated as a network indicator that drives focused analysis and response choices.
4. Correct Answer: B. Containment
   Explanation: Containment limits spread and damage while preserving options for eradication and recovery. The exam often tests choosing actions that reduce impact without destroying evidence or causing unnecessary disruption.
5. Correct Answer: A. Credentialed scan
   Explanation: A credentialed scan authenticates to the target system to obtain deeper, more accurate vulnerability information. It is tested because it changes result quality and affects how findings are validated.
6. Correct Answer: B. Compensating control
   Explanation: A compensating control is an alternative safeguard used when the ideal fix is not possible. The exam often tests selecting a realistic compensating measure and documenting the exception appropriately.

7. Correct Answer: C. Time synchronization
   Explanation: Time synchronization ensures systems record events using consistent time sources and settings. Investigations rely on reliable timelines, and mismatched clocks can undermine correlation.

8. Correct Answer: C. Threat hunting
   Explanation: Threat hunting is proactive searching for signs of malicious activity that may not trigger alerts. The exam uses it to test how to pivot from a weak signal into broader searches across telemetry.

9. Correct Answer: A. Risk acceptance
   Explanation: Risk acceptance is a formal decision to tolerate a known risk when mitigation is not justified or feasible. The exam frames this as a governance decision that must be documented and approved.

10. Correct Answer: B. Chain of custody
    Explanation: Chain of custody documents how evidence is collected, handled, transferred, and stored to preserve integrity. The exam tests this when choosing evidence handling steps that avoid contamination.

Bank 2

1. A security team wants to improve detection of suspicious behavior but is overwhelmed by noisy alerts that repeatedly turn out benign. Which activity most directly focuses on adjusting rules, thresholds, and logic to improve signal quality?
   A. Tuning
   B. Eradication
   C. Data retention
   D. Asset discovery

2. An analyst needs to understand what happened during an incident and selects evidence sources that can be examined without destroying key artifacts. Which discipline most directly describes collecting and analyzing digital evidence in a repeatable way?
   A. Business continuity
   B. Digital forensics
   C. Risk acceptance
   D. Allowlisting

3. A responder sees a suspicious file attached to an email and wants to observe what it does without risking production systems. Which approach best fits running suspicious code in an isolated environment to observe behavior safely?
   A. Normalization
   B. Log correlation
   C. Sandboxing
   D. Chain of custody

4. A web server begins making unexpected outbound connections and you find a new script file sitting in a web directory that can accept commands through HTTP requests. What is the best label for this artifact?
   A. Web shell
   B. Watering hole attack
   C. Baseline
   D. CVSS

5. A SOC lead wants faster understanding of incidents by combining endpoint, network, and identity events into a single coherent timeline. Which technique best describes combining events across multiple sources to build cause-and-effect?
   A. Threat intelligence
   B. Log correlation

C. Network segmentation
D. Dwell time

6. A team is deciding between two analysis approaches for a suspicious executable. One approach inspects the file without running it, and the other executes it in a controlled environment to observe actions. What pair of approaches is being contrasted?
   A. Containment vs. eradication
   B. Strategic vs. tactical intelligence
   C. Static vs. dynamic malware analysis
   D. Baseline vs. normalization

7. A critical goal is to limit what systems can talk to each other so that compromise of one area does not easily spread to others. Which control best matches separating systems into zones to control traffic flow and reduce lateral movement?
   A. Time synchronization
   B. Network segmentation
   C. Data exfiltration
   D. Incident classification

8. After an incident is detected, leadership asks how quickly the organization typically contains and remediates incidents once they are identified. Which metric best matches that description?
   A. Mean time to respond (MTTR)
   B. Mean time to detect (MTTD)
   C. Dwell time
   D. Passing score

9. A security team wants a platform that collects, normalizes, correlates, and alerts on security events from many sources. Which tool category best fits that description?
   A. EDR
   B. CASB
   C. SIEM
   D. SOAR

10. A known attacker group aims to maintain access for a long period and achieve strategic goals while remaining stealthy. Which term best fits that attacker profile in exam context?
    A. False positive
    B. Advanced persistent threat (APT)

C. Credentialed scan
D. Incident classification

---

1. Correct Answer: A. Tuning
   Explanation: Tuning adjusts detection logic, thresholds, and enrichment to improve signal quality and reduce noise. The exam frequently tests choosing what to tune after repeated false positives or missed detections.

2. Correct Answer: B. Digital forensics
   Explanation: Digital forensics is collecting and analyzing digital evidence in a repeatable way to understand what happened. The exam emphasizes selecting appropriate evidence sources and avoiding actions that alter or destroy artifacts.

3. Correct Answer: C. Sandboxing
   Explanation: Sandboxing runs suspicious code in an isolated environment to observe behavior safely. It is tested as a safe analysis choice for files or attachments without risking production systems.

4. Correct Answer: A. Web shell
   Explanation: A web shell is a malicious script that enables remote command execution through web requests. The exam commonly links it to unexpected web artifacts and suspicious outbound activity from a server.

5. Correct Answer: B. Log correlation
   Explanation: Log correlation combines events across multiple sources to build a coherent timeline. The exam tests selecting sources and connecting cause-and-effect rather than treating alerts in isolation.

6. Correct Answer: C. Static vs. dynamic malware analysis
   Explanation: Static analysis examines a file without executing it, while dynamic analysis observes behavior by executing in a controlled environment. The exam tests which approach fits quick triage versus behavior confirmation and IOC extraction.

7. Correct Answer: B. Network segmentation
   Explanation: Network segmentation separates systems into zones to control traffic flow and limit lateral movement. The exam often uses it as a design control that reduces spread during or after compromise.

8. Correct Answer: A. Mean time to respond (MTTR)
   Explanation: MTTR measures the average time to contain and remediate once an

incident is detected. The exam uses it to evaluate response efficiency and the impact of process or tooling improvements.

9. Correct Answer: C. SIEM
   Explanation: A SIEM collects, normalizes, correlates, and alerts on security-relevant events from many sources. CySA+ tests choosing SIEM data sources and correlation approaches to validate incidents.

10. Correct Answer: B. Advanced persistent threat (APT)
    Explanation: An APT is a well-resourced attacker that maintains access over time to achieve strategic objectives. The exam uses it to frame stealthy, staged campaigns where monitoring and response choices must fit long-running activity.

Bank 3

1. An analyst is asked to reduce the likelihood that users can run unapproved tools, even if attackers introduce new binaries that are not yet on any blocklist. Which control best matches allowing only approved applications by default?
   A. Allowlisting
   B. Data retention
   C. Incident classification
   D. Dwell time

2. An investigation identifies unusually large archive files being created on a server, followed by sustained outbound transfers to an unfamiliar external destination. What activity is this most directly consistent with?
   A. Normalization
   B. Data exfiltration
   C. Risk acceptance
   D. Baseline

3. A SOC wants to reduce the time between the start of an incident and when the team identifies it as malicious activity. Which metric best matches that goal?
   A. Mean time to detect (MTTD)
   B. Mean time to respond (MTTR)
   C. Chain of custody
   D. Business continuity

4. A responder is asked to “remove the attacker’s presence and the cause of compromise” after the environment has been stabilized and key evidence has been preserved. Which incident response step is being described?
   A. Triage
   B. Incident classification
   C. Eradication
   D. Containment

5. A company needs to keep critical services operating during disruptions, even if systems are degraded, and wants plans that support that outcome. Which concept best matches this goal?
   A. Root cause analysis
   B. Business continuity (BC)
   C. Credentialed scan
   D. Threat hunting

6. Multiple systems send logs to a central platform, but field names and formats differ, making searches and correlations unreliable. Which process best addresses converting data into consistent formats and fields?
   A. Normalization
   B. Playbook
   C. Watering hole attack
   D. Privilege escalation

7. An analyst is asked to reduce the time an attacker remains undetected inside the environment. Which concept most directly represents that period?
   A. CVSS
   B. Dwell time
   C. MTTR
   D. Asset discovery

8. A team is deciding which threat intelligence to use. One type supports immediate blocking and hunting through specific artifacts, while the other is meant to guide higher-level prioritization and trends. What contrast is being described?
   A. Static vs. dynamic analysis
   B. Triage vs. containment
   C. Tactical vs. strategic threat intelligence
   D. Baseline vs. anomaly detection

9. An attacker gains a foothold on one host and then moves to other internal systems using remote services and reused credentials. What is this movement inside the environment most commonly called?
   A. Asset discovery
   B. Lateral movement
   C. Sandboxing
   D. File integrity monitoring

10. A team wants a tool that can coordinate and automate response steps across systems, such as enrichment and ticketing, but still allow approvals for high-impact actions. Which tool category best fits?
    A. CASB
    B. SOAR
    C. SIEM
    D. CVSS

---

1. Correct Answer: A. Allowlisting
   Explanation: Allowlisting permits only approved applications or scripts while blocking everything else by default. The exam uses it as a control choice that is more resilient than blocklists against new attacker tools.

2. Correct Answer: B. Data exfiltration
   Explanation: Data exfiltration is the unauthorized removal of data to an attacker-controlled location. The exam commonly links archive creation and unusual outbound transfers to exfiltration indicators and response decisions.

3. Correct Answer: A. Mean time to detect (MTTD)
   Explanation: MTTD measures the average time it takes to identify an incident after it begins. The exam uses it to evaluate monitoring effectiveness and improvements that reduce detection delay.

4. Correct Answer: C. Eradication
   Explanation: Eradication removes the attacker's presence and the underlying cause of compromise, such as malware or persistence. The exam frames it as the step that follows stabilization and drives prevention of repeat entry.

5. Correct Answer: B. Business continuity (BC)
   Explanation: Business continuity focuses on keeping critical services operating during disruptions. The exam ties BC to incident decision-making that balances security actions with operational impact.

6. Correct Answer: A. Normalization
   Explanation: Normalization converts logs and data into consistent formats and fields so they can be searched and correlated reliably. The exam tests it as a root cause when correlation fails due to inconsistent parsing.

7. Correct Answer: B. Dwell time
   Explanation: Dwell time is how long an attacker remains undetected in the environment. The exam uses it to reason about monitoring gaps and the likely extent of attacker activity.

8. Correct Answer: C. Tactical vs. strategic threat intelligence
   Explanation: Tactical intelligence is immediately actionable, such as IOCs and patterns used for detection and blocking. Strategic intelligence focuses on trends and risk drivers used for prioritization and higher-level decisions.

9. Correct Answer: B. Lateral movement
   Explanation: Lateral movement is moving from one system to another inside the

environment after initial access. The exam tests recognition through clues like remote service use and unusual authentication patterns.

10. Correct Answer: B. SOAR
    Explanation: SOAR tools automate and coordinate response steps across systems while supporting approvals for risky actions. The exam tests selecting which parts of response can be safely automated versus requiring human gates.

Bank 4

1. A company wants to ensure that even if a user's device is on an internal network, access is still continuously verified using identity and context rather than assumed. Which security approach best matches that mindset?
   A. Zero trust
   B. Baseline
   C. Asset discovery
   D. Chain of custody

2. A team uses endpoint tooling to review process trees, parent-child relationships, and command-line activity to investigate suspicious behavior on a host. Which tool category best fits this capability?
   A. CASB
   B. EDR
   C. CVSS
   D. Risk acceptance

3. A SOC lead wants to sort incoming alerts quickly to decide which items need deeper investigation first. Which step best describes this initial sorting and prioritization?
   A. Triage
   B. Root cause analysis
   C. Eradication
   D. Business continuity

4. A team sees repeated unauthorized changes to key configuration files on a server and wants to detect and record changes to critical files over time. Which control best matches that need?
   A. Sandboxing
   B. File integrity monitoring (FIM)
   C. Mean time to respond
   D. Threat intelligence

5. A leadership review asks, "What is the underlying cause that allowed this incident to occur, and what change prevents it from happening again?" Which activity best matches that goal?
   A. Threat hunting
   B. Root cause analysis (RCA)

C. Credentialed scan
D. Normalization

6. A SOC is asked to create and maintain detection logic that translates observed behaviors into practical rules and correlations, then validate that those detections work using telemetry and baselines. What is the best term for this work?
   A. Detection engineering
   B. Incident classification
   C. Business continuity
   D. Asset discovery

7. A responder notices that an attacker gained higher access than originally granted by exploiting weaknesses and abusing privileges. Which term best fits this action?
   A. Privilege escalation
   B. Log correlation
   C. Sandboxing
   D. Watering hole attack

8. A team wants to combine endpoint, network, and identity logs, but first must ensure parsing and field naming are consistent so correlation logic works. Which prerequisite process best supports that outcome?
   A. Normalization
   B. Risk acceptance
   C. Chain of custody
   D. Baseline

9. A security platform is needed to enforce security policies for cloud service usage, especially to monitor and govern cloud access and data movement. Which tool category best matches this role?
   A. CASB
   B. SIEM
   C. SOAR
   D. FIM

10. A SOC manager asks for the average time an attacker remains undetected in the environment, because long undetected periods usually indicate deeper spread and persistence. Which term best matches this measure?
    A. Mean time to detect
    B. Dwell time

C. Mean time to respond
D. CVSS

---

1. Correct Answer: A. Zero trust
   Explanation: Zero trust assumes no implicit trust based on network location and continuously verifies identity and context. The exam uses it as a design mindset to reduce lateral movement and unnecessary trust.
2. Correct Answer: B. EDR
   Explanation: EDR collects endpoint telemetry and supports investigation and response actions on hosts. The exam commonly ties EDR to host-based evidence like process trees and command-line details.
3. Correct Answer: A. Triage
   Explanation: Triage is the initial sorting and prioritization of alerts to determine what needs deeper investigation first. The exam expects quick validation and severity judgment before taking disruptive actions.
4. Correct Answer: B. File integrity monitoring (FIM)
   Explanation: FIM monitors key files and directories for unauthorized changes, often using hashes and change alerts. The exam links it to detecting tampering, web artifacts, and unexpected configuration changes.
5. Correct Answer: B. Root cause analysis (RCA)
   Explanation: RCA identifies the underlying cause of an incident rather than just symptoms. The exam tests it as a post-incident step that supports remediation that prevents recurrence.
6. Correct Answer: A. Detection engineering
   Explanation: Detection engineering is designing and maintaining detection logic such as rules and correlations. The exam tests translating observed behavior into actionable detections and validating them against telemetry and baselines.
7. Correct Answer: A. Privilege escalation
   Explanation: Privilege escalation is gaining higher access than originally granted through exploitation or abuse. The exam tests recognition through evidence like unexpected privilege changes and suspicious high-privilege activity.
8. Correct Answer: A. Normalization
   Explanation: Normalization converts logs into consistent formats and fields so

searching and correlation work reliably. The exam treats poor parsing and inconsistent fields as common causes of detection and correlation failures.

9. Correct Answer: A. CASB
   Explanation: A CASB helps enforce security policies for cloud service usage by monitoring and governing access and data movement. The exam frames it as a cloud and hybrid control point tied to access and visibility.

10. Correct Answer: B. Dwell time
    Explanation: Dwell time is the length of time an attacker remains undetected in an environment. The exam uses it to reason about monitoring gaps and the likely extent of attacker activity.

Bank 5

1. A SOC analyst sees a user account authenticate at an unusual hour from a location that does not match the organization's normal patterns. The analyst compares the event to known normal behavior before escalating. Which concept most directly supports that comparison step?
   A. Baseline
   B. Sandboxing
   C. Eradication
   D. Asset discovery

2. A security team wants to ensure evidence gathered during an investigation can be trusted and reviewed later without questions about handling. They document how each artifact was collected, transferred, and stored. What is the key practice being applied?
   A. Normalization
   B. Chain of custody
   C. Tuning
   D. Risk acceptance

3. A host begins making periodic, patterned outbound connections to the same external destination, and the pattern is uncommon for that system. What is this pattern most commonly called in exam context?
   A. Asset discovery
   B. Vulnerability management
   C. Beaconing
   D. File integrity monitoring

4. After containment, the team needs to remove the attacker's presence and the underlying cause of compromise so the environment does not immediately get re-infected. Which step best matches that goal?
   A. Triage
   B. Root cause analysis
   C. Incident classification
   D. Eradication

5. A program manager wants a repeatable cycle that identifies systems, assesses vulnerabilities, prioritizes fixes with context, and verifies remediation. Which concept best describes this ongoing program?
   A. Vulnerability management

B. Allowlisting
C. Dwell time
D. Time synchronization

6. The SOC receives frequent alerts that later prove benign, and leadership asks for changes that reduce noise without losing true detections. Which activity most directly addresses adjusting thresholds and rule logic to improve signal quality?
   A. Incident classification
   B. Tuning
   C. Digital forensics
   D. Business continuity

7. An attacker gains access to one workstation and then uses internal paths to move to additional systems using remote services and authentication activity that stands out from normal patterns. What is this movement inside the environment called?
   A. Risk acceptance
   B. Data retention
   C. Lateral movement
   D. Static analysis

8. A team wants to disrupt an attacker early by recognizing where observed behavior fits in a phased attack model and then applying controls and detections appropriate to that phase. Which model best matches that use?
   A. CVSS
   B. Chain of custody
   C. Baseline
   D. Kill chain

9. A security architect wants to reduce the blast radius of compromised accounts and services by ensuring they only have the access they need. Which principle best matches that goal?
   A. Least privilege
   B. Threat hunting
   C. Business continuity
   D. Sandboxing

10. A SOC lead wants to combine endpoint, network, and identity events to build a coherent timeline and identify cause-and-effect. Which technique best describes that approach?
    A. Asset discovery

B. Log correlation
C. Risk acceptance
D. Allowlisting

---

1. Correct Answer: A. Baseline
   Explanation: A baseline is the normal, expected pattern of behavior for systems and users over time. The exam uses baselines to validate whether an event is truly suspicious or consistent with normal operations.
2. Correct Answer: B. Chain of custody
   Explanation: Chain of custody is the documented record of how evidence is collected, handled, transferred, and stored to preserve integrity. The exam tests it as the correct way to protect evidence from contamination or disputes.
3. Correct Answer: C. Beaconing
   Explanation: Beaconing is periodic, patterned communication from a host to an external destination. The exam treats it as a strong network indicator that drives focused investigation and response decisions.
4. Correct Answer: D. Eradication
   Explanation: Eradication removes the attacker's presence and the cause of compromise, such as malware or persistence mechanisms. The exam frames it as the step that prevents immediate reinfection after the environment is stabilized.
5. Correct Answer: A. Vulnerability management
   Explanation: Vulnerability management is the ongoing process of discovering, assessing, prioritizing, remediating, and verifying vulnerabilities. The exam expects the full cycle rather than treating a scan report as the final outcome.
6. Correct Answer: B. Tuning
   Explanation: Tuning is adjusting detection logic, thresholds, and enrichment to reduce noise and improve alert quality. The exam often tests tuning as the right response to repeated false positives or missed detections.
7. Correct Answer: C. Lateral movement
   Explanation: Lateral movement is moving from one system to another inside the environment after initial access. The exam tests recognition through clues like unusual remote access behavior and authentication patterns.
8. Correct Answer: D. Kill chain
   Explanation: A kill chain is a model that describes phases of an attack from early

steps through actions on objectives. The exam uses it to help decide which controls, detections, or response actions best disrupt the attacker at a given phase.

9. Correct Answer: A. Least privilege
   Explanation: Least privilege means granting only the access needed for a role, service, or process. The exam emphasizes it because excessive permissions increase incident impact and make attacker escalation easier.

10. Correct Answer: B. Log correlation
    Explanation: Log correlation combines events across multiple sources to build a coherent timeline and connect cause-and-effect. The exam expects selecting and correlating the right sources rather than relying on a single alert.