CYSA+ Exam Glossary

Find more at BareMetalCyber.com

1. **Advanced persistent threat (APT)**
   An APT is a well-resourced, long-running attacker (often an organized group) that aims to maintain access and achieve strategic goals over time. On the exam, it commonly shows up when you must distinguish attacker types and pick monitoring, hunting, or response actions that fit a stealthy, staged campaign.

2. **Anomaly detection**
   Anomaly detection is finding activity that deviates from a known baseline, such as unusual outbound connections, spikes in resource use, or odd authentication patterns. On the exam, it often drives the first decision: triage whether behavior is benign change, misconfiguration, or a likely indicator of compromise worth escalating.

3. **Asset discovery**
   Asset discovery is the process of identifying systems, services, and endpoints that exist in the environment so they can be assessed and monitored. It matters because vulnerability scanning and prioritization are only as good as your inventory; many questions test whether you choose discovery before scanning or remediation planning.

4. **Beaconing**
   Beaconing is periodic, patterned communication from a host to an external destination, often associated with command-and-control activity. On the exam, it shows up as a network indicator where you must choose the right analysis approach (logs, packet capture, reputation checks) and the most appropriate next response step.

5. **Business continuity (BC)**
   Business continuity is the planning and capability to keep critical services operating during disruption, even if systems are degraded. Exam questions frequently connect BC to incident management decisions, such as containment choices that reduce attacker impact without causing unacceptable downtime.

6. **Cloud access security broker (CASB)**
   A CASB is a control point that helps enforce security policies for cloud service usage, commonly by monitoring, governing, and sometimes controlling access and data movement. On the exam, it appears as an architecture or IAM-related control you select to reduce risk in cloud and hybrid environments.

7. **Common Vulnerability Scoring System (CVSS)**
   CVSS is a standardized way to score vulnerability severity, typically producing a numerical score and severity rating. On the exam, the key is not memorizing numbers but using CVSS with context—exploitability, asset value, exposure—to prioritize what to fix first.

8. **Compensating control**
   A compensating control is an alternative safeguard used when the ideal fix (like patching) is not possible, aiming to reduce risk to an acceptable level. Exam scenarios often test whether you choose a realistic compensating measure and document the exception rather than forcing an impractical remediation.

9. **Containment**
   Containment is the incident response step focused on limiting spread and damage while preserving options for eradication and recovery. On the exam, it's a frequent decision point: pick actions that stop impact quickly without destroying evidence or breaking critical business operations unnecessarily.

10. **Credentialed scan**
    A credentialed scan is a vulnerability scan that authenticates to the target system to get deeper, more accurate configuration and patch-state data. It's tested because it changes result quality and risk: you may need to choose credentialed vs. non-credentialed scanning based on scope, permissions, and the kind of findings you're trying to validate.

11. **Data exfiltration**
    Data exfiltration is the unauthorized removal of data from an environment to an attacker-controlled location. On the exam, it often appears as a "what happened?" or "what do you do next?" scenario where you must identify likely indicators (unusual outbound traffic, archive tools, new egress paths) and choose containment that preserves evidence.

12. **Detection engineering**
    Detection engineering is the practice of designing, tuning, and maintaining detection logic (rules, correlation, thresholds, and alerts) to catch malicious activity with manageable false positives. It matters on CySA+ because questions frequently test whether you can translate an observed behavior into a practical detection idea and then validate it against logs and baselines.

13. **Digital forensics**
    Digital forensics is collecting and analyzing digital evidence in a repeatable way to

understand what happened, how, and by whom. On the exam, the focus is usually on choosing the right evidence source (disk, memory, logs) and avoiding actions that would alter or destroy key artifacts.

14. **Dwell time**
    Dwell time is the length of time an attacker remains undetected in an environment. It shows up as a way to reason about monitoring effectiveness and response urgency, because longer dwell time usually means more lateral movement, persistence, and potential data exposure.

15. **Endpoint detection and response (EDR)**
    EDR is a set of tools and processes that collect endpoint telemetry and help detect, investigate, and respond to suspicious activity on hosts. On the exam, it commonly appears in questions where you choose the best data source for a host-based event (process tree, command line, parent-child relationships) and the next response action.

16. **False positive**
    A false positive is an alert that indicates malicious activity when the underlying event is actually benign. CySA+ tests this constantly: you're expected to validate alerts using context (baselines, change windows, known admin tools) and pick the next investigative step instead of immediately escalating or blocking.

17. **File integrity monitoring (FIM)**
    FIM is monitoring key files and directories for unauthorized changes, often using hashes and change notifications. On the exam, it tends to appear in scenarios involving web shells, altered binaries, or unexpected configuration changes, where you must decide how to confirm tampering and what evidence to collect.

18. **Incident classification**
    Incident classification is categorizing an event by type and severity so responders can apply the right playbook and escalation path. It matters because many questions revolve around prioritization—deciding whether something is malware, insider misuse, data loss, or a misconfiguration and then choosing an appropriate response.

19. **Indicator of compromise (IOC)**
    An IOC is an observable artifact linked to possible malicious activity, such as a suspicious hash, domain, registry key, or IP address. On CySA+, you'll often be asked to choose which IOC is most meaningful, how to pivot from it (search logs, hunt endpoints), and how to avoid over-trusting a single weak indicator.

20. **Kill chain**
    A kill chain is a model describing phases of an attack from reconnaissance through actions on objectives. The exam uses it as a reasoning tool: you may need to identify which phase you're observing and then choose the control, detection, or response that best disrupts the attacker at that point.

21. **Lateral movement**
    Lateral movement is when an attacker moves from one system to another inside the environment after initial access. On the exam, it often shows up through clues like remote service use, new admin shares, unusual authentication patterns, or unexpected remote tooling, and you must pick investigation and containment steps that limit spread.

22. **Least privilege**
    Least privilege means giving users, services, and processes only the access they need, and no more. It matters in CySA+ questions because excessive permissions amplify incidents, so many scenarios test whether you recognize privilege overreach and choose controls that reduce blast radius.

23. **Log correlation**
    Log correlation is combining events across multiple sources (endpoint, network, identity, application, cloud) to build a coherent timeline. On the exam, it's a common decision point: you're expected to pick the right sources to correlate and identify cause-and-effect rather than treating alerts in isolation.

24. **Malware analysis (static vs. dynamic)**
    Static analysis examines a file without executing it (hashing, strings, headers), while dynamic analysis executes or emulates behavior in a controlled environment to observe actions. CySA+ tests which approach fits the question—quick triage often starts static, while confirming behavior or IOCs often needs dynamic observation.

25. **Mean time to detect (MTTD)**
    MTTD is the average time it takes to identify an incident after it begins. On the exam, it's used to evaluate monitoring effectiveness and prioritization, and it can influence which improvements you recommend (better telemetry, tuned detections, clearer escalation paths).

26. **Mean time to respond (MTTR)**
    MTTR is the average time it takes to contain and remediate an incident once it's detected. CySA+ scenarios use MTTR to test whether you understand response

efficiency and can choose process and tooling improvements that reduce response delays without sacrificing evidence handling.

27. **Network segmentation**
    Network segmentation is separating systems into zones to control traffic flow and limit what can talk to what. It's heavily tested because it reduces lateral movement; exam questions often ask where to place controls or how to adjust segmentation after an incident to prevent repeat paths.

28. **Normalization**
    Normalization is converting logs and data into consistent formats and fields so they can be searched, compared, and correlated reliably. On the exam, it matters when you're selecting SIEM processes or troubleshooting why detections fail—bad parsing and inconsistent fields can break correlation and dashboards.

29. **Playbook (incident response)**
    A playbook is a documented, repeatable set of response actions for a specific incident type, including triggers, approvals, and handoffs. CySA+ tests whether you pick the right playbook-driven step (triage, isolate, preserve evidence, notify) rather than improvising or skipping key gates.

30. **Privilege escalation**
    Privilege escalation is gaining higher access than originally granted, either by exploiting vulnerabilities, misconfigurations, or credential abuse. On the exam, it often appears as suspicious admin group changes, token abuse, or new service creation, and you must decide how to confirm it and contain it without losing visibility.

31. **Risk acceptance**
    Risk acceptance is a formal decision to tolerate a known risk when the cost or feasibility of mitigation is not justified. On the exam, it shows up when you must pick the correct governance action—documenting and approving the risk—rather than pretending the issue is "fixed" with weak controls.

32. **Root cause analysis (RCA)**
    RCA is the structured process of determining the underlying cause of an incident or control failure, not just the symptoms. CySA+ tests this as a post-incident decision point: you're expected to identify what evidence supports the true cause and which remediation prevents recurrence.

33. **Sandboxing**
    Sandboxing is running suspicious code in an isolated environment to observe

behavior safely. On the exam, it's commonly used to decide how to analyze a file or attachment without detonating it on production systems, and to extract behaviors and IOCs for hunting.

34. **Security information and event management (SIEM)**
    A SIEM is a platform that collects, normalizes, correlates, and alerts on security-relevant events from many sources. CySA+ questions often test whether you can choose the right SIEM data sources and correlation approach to confirm an incident and reduce false positives.

35. **SOAR (security orchestration, automation, and response)**
    SOAR tools automate and coordinate response steps across systems, such as enrichment, ticketing, quarantining endpoints, or blocking indicators. On the exam, it shows up when you must decide which actions are safe to automate and which require human approval to avoid breaking business operations.

36. **Threat hunting**
    Threat hunting is proactive searching for signs of malicious activity that may not trigger alerts, using hypotheses and telemetry. It matters because CySA+ scenarios often ask how to pivot from a weak signal—like a suspicious domain—into a broader search across endpoints and logs.

37. **Threat intelligence (tactical vs. strategic)**
    Tactical intelligence is immediately actionable (IOCs, TTP patterns), while strategic intelligence focuses on higher-level trends and risk drivers. The exam tests whether you use the right type: tactical for detections and blocking, strategic for prioritization and program decisions.

38. **Time synchronization**
    Time synchronization ensures systems record events using consistent time sources and settings. It's tested because investigations depend on reliable timelines; misaligned clocks can make correlation misleading and can hide the true order of attacker actions.

39. **Triage**
    Triage is the initial sorting and prioritization of alerts and events to determine what needs deeper investigation first. On CySA+, triage decisions are everywhere: you must validate signals quickly, identify severity, and choose the next best evidence source before taking disruptive actions.

40. **Tuning (detections/alerts)**
    Tuning is adjusting detection logic, thresholds, and enrichment to improve signal

quality and reduce noise. It matters on the exam because many scenarios require selecting what to tune (source, rule logic, exclusions, thresholds) after repeated false positives or missed detections.

41. **Vulnerability management**
    Vulnerability management is the ongoing process of discovering, assessing, prioritizing, remediating, and verifying vulnerabilities across assets. On CySA+, it's tested as a workflow decision: choose the right order (inventory, scan, validate, prioritize with context, fix, confirm) instead of treating scan results as the finish line.

42. **Vulnerability prioritization**
    Vulnerability prioritization is ranking findings based on real risk, not just severity scores, by adding context like exploit availability, exposure, asset criticality, and compensating controls. The exam often tests whether you can pick the "fix first" item when multiple vulnerabilities exist and the highest CVSS is not the highest business risk.

43. **Watering hole attack**
    A watering hole attack targets a website or service that a victim population regularly visits, infecting or redirecting them when they browse it. On the exam, it shows up as an initial-access scenario where you must recognize the pattern and choose controls like web filtering, endpoint protections, and user-risk investigation.

44. **Web shell**
    A web shell is a malicious script uploaded to a web server that allows an attacker to run commands remotely through HTTP requests. CySA+ commonly tests this by presenting odd web logs, new files in web directories, or unexpected outbound connections from a server, and you must choose the best evidence and containment steps.

45. **Whitelisting (allowlisting)**
    Allowlisting is permitting only approved applications, scripts, or network destinations while blocking everything else by default. The exam uses it as a control choice to reduce execution and persistence risk, and it's often contrasted with blocklists, which are easier but less reliable against new attacker tools.

46. **Zero trust**
    Zero trust is a security approach that continuously verifies identity, device, and context and assumes no implicit trust based on network location. On CySA+, it's tested as a design and control mindset: select access controls and segmentation decisions that reduce lateral movement and limit unnecessary trust.

47. **Baseline**
    A baseline is the normal, expected pattern of behavior for systems, users, and networks over time. It matters because many analysis questions depend on comparing a suspected event to “normal” to determine whether it’s truly suspicious or a routine change.

48. **Chain of custody**
    Chain of custody is the documented record of how evidence is collected, handled, transferred, and stored to preserve integrity. The exam tests this when you must choose how to preserve evidence for internal investigations or potential legal needs without contaminating it.

49. **Data retention**
    Data retention is defining how long logs and other records are kept and ensuring they remain accessible and protected. On CySA+, it affects investigation capability: too little retention blocks timeline reconstruction, while poor retention controls can create risk and compliance gaps.

50. **Eradication**
    Eradication is removing the attacker’s presence and the cause of compromise, such as malware, persistence mechanisms, or abused accounts. On the exam, it’s a decision point after containment: choose actions that fully remove the threat while preserving enough evidence to confirm what happened and prevent repeat entry.