

PRACTICE QUESTIONS

GIAC / SANS

GASAE

GIAC AI Security Automation Engineer

SHARED BY [u/Frosty-Kiwi-8327](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 18, 2026

EXAM GIAC / SANS GASAE, GIAC AI Security Automation Engineer

Shared by [u/Frosty-Kiwi-8327](#) on aiexamcerts

10 practice questions for the GIAC / SANS GASAE exam, GIAC AI Security Automation Engineer, each followed by its answer and a short explanation. More free sets and the full practice exam:

aiexamcerts.com/giac-sans/gasae. Spotted a mistake? Email support@aiexamcerts.com with the exam code GASAE and the question number.

1. Does Amazon GuardDuty use AWS CloudTrail event logs as one of its data sources for threat detection?

- A True
- B False

Answer: A (True)

True. GuardDuty analyzes CloudTrail management events, VPC Flow Logs and DNS query logs, among other sources, to detect suspicious account and network activity. Knowing its inputs helps explain why a finding can appear without any agent on a host.

2. A detection engineer must port a vendor-neutral Sigma rule to the organization's SIEM. What is the typical approach?

- A Upload the YAML file unchanged because SIEMs execute Sigma natively
- B Rewrite the logic in Python and run it against the local file system only
- C Convert it with a Sigma backend into the SIEM query language, then test it on sample logs
- D Replace the detection with a static list of file hashes that the team updates manually once a quarter

Answer: C

Sigma rules are written in a generic format and are converted into a target platform's query language with a backend converter, after which the result must be tested against sample data. Uploading the YAML unchanged is the tempting distractor, since most SIEMs do not execute Sigma directly. A hash list cannot express the behavior the rule describes.

3. What is the primary purpose of an Ansible inventory?

- A To store encrypted secrets used by the Vault integration
- B To define the hosts and groups that playbooks target
- C To hold the compiled bytecode of each task
- D To schedule playbook runs on a recurring timer

Answer: B

An inventory lists the managed hosts and organizes them into groups so that plays can target the right machines. Ansible Vault is the most tempting distractor because it is also a configuration artifact, but it stores encrypted variables rather than host lists. Tasks are not compiled into bytecode, and scheduling is handled by external tools.

4. An agentic AI tool plans simulation steps for an authorized lab test. Which control matters most for keeping its activity within the engagement?
- A The agent is allowed to reach any host so it can plan without limits
 - B Logging is turned off to avoid slowing the agent down during the run
 - C Results are published to a shared channel before the client reviews them
 - D Scope and rules of engagement are defined, and the agent is restricted to in-scope targets

Answer: D

A written scope and rules of engagement, enforced as technical restrictions on the agent's targets, keep automated tooling inside what the client authorized. Unrestricted reach is the obvious wrong design, but the more tempting distractor is a disabled log, which would remove the evidence needed to prove what happened. Publishing results early violates the engagement's reporting terms.

5. Which Azure service gives centralized security posture management and security recommendations across subscriptions?
- A Microsoft Defender for Cloud
 - B Azure Bastion, which provides secure remote access to virtual machines without public IP addresses
 - C Azure Front Door
 - D Azure Cost Management

Answer: A

Microsoft Defender for Cloud assesses resource configurations against security benchmarks and provides recommendations and posture scores across subscriptions. Azure Bastion is the most tempting distractor because it appears in security designs, but it provides secure remote access to virtual machines. Front Door handles global traffic routing and Cost Management tracks spending.

6. Does granting automation accounts domain administrator rights by default follow the principle of least privilege?
- A True
 - B False

Answer: B (False)

False. Least privilege means an automation account receives only the permissions each task needs, scoped to the systems it manages. Domain administrator rights by default would give a compromised or misconfigured script control over the entire directory.

7. In SOAR terminology, a reusable sequence of automated and manual steps that responds to a specific type of alert is called a _____.

Answer: playbook (also accepted: response playbook, SOAR playbook)

A playbook packages the decision logic and actions for one alert type so that responses are consistent and repeatable. Playbooks are distinct from cases, which group the artifacts of a single investigation. Accepted answers cover the common phrasings used by SOAR products.

8. In the NIST SP 800-61 Rev. 2 incident response lifecycle, which phase comes directly after detection and analysis?

- A Preparation, which covers policies, tooling, playbooks and staff training before any incident occurs
- B Post-incident activity
- C Containment, eradication and recovery
- D Threat modeling

Answer: C

The NIST SP 800-61 Rev. 2 lifecycle runs preparation, detection and analysis, containment eradication and recovery, then post-incident activity. Preparation is the most tempting distractor because it is also a lifecycle phase, but it comes before detection. Post-incident activity closes the cycle, and threat modeling is a design activity outside the lifecycle.

9. During host triage, which evidence is the most volatile and should usually be collected first, according to common order-of-volatility guidance?

- A Archived backups stored in an offsite vault
- B The running process list and active network connections
- C Printed copies of the event logs from last quarter
- D The installed software inventory from the asset database

Answer: B

Running processes and live network connections disappear when the host is rebooted or isolated, so they sit near the top of the order of volatility. Installed software inventories are the tempting distractor because they are useful evidence, but they change slowly and persist on disk. Offsite backups and printed logs are stable sources that can be collected later.

10. Which Azure Policy effect blocks a non-compliant resource from being created or updated?

- A Audit
- B AuditIfNotExists
- C DeployIfNotExists
- D Deny

Answer: D

The Deny effect prevents a request that would create or update a non-compliant resource. Audit is the most tempting distractor because it reports non-compliance but still allows the change. AuditIfNotExists checks for related resources, and DeployIfNotExists remediates after the fact rather than blocking.