

PRACTICE QUESTIONS

GIAC / SANS

GASAE

GIAC AI Security Automation Engineer

SHARED BY [u/boldtiger1989](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 18, 2026

EXAM GIAC / SANS GASAE, GIAC AI Security Automation Engineer

Shared by [u/boldtiger1989](#) 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. Which two data sources most directly support detection of suspicious PowerShell execution on Windows? (Choose two.)

- A PowerShell script block logging (Event ID 4104)
- B Sysmon process creation events (Event ID 1)
- C Printer spooler queue length metrics
- D Monthly disk capacity reports for the file servers
- E DNS cache size statistics from the resolver

Answer: A, B

Script block logging records the code PowerShell actually executes, and Sysmon process creation events capture the command line that launched it. Printer queue metrics and disk reports have no direct link to PowerShell activity, so they are not useful here. DNS cache statistics describe resolver health rather than the commands a user ran.

2. Does agentic AI typically involve a model choosing a sequence of actions and invoking tools to pursue a goal?

- A True
- B False

Answer: A (True)

True. An agent plans steps, calls tools such as search, code execution or ticketing APIs, observes the results and decides what to do next. The defining feature is the loop of decision and action, which is why agent behavior needs tighter controls than a single prompt-and-answer call.

3. Which AWS service aggregates security findings from integrated services such as GuardDuty, Inspector and Macie into one view?
- A AWS Security Hub, which aggregates findings from integrated security services
 - B AWS Artifact, which provides on-demand compliance reports and agreements from AWS auditors and partners
 - C AWS Config, which records the configuration history of resources
 - D AWS Shield, which mitigates distributed denial-of-service attacks

Answer: A

Security Hub collects findings from integrated services and checks them against security standards in one place. AWS Config is the most tempting distractor because it also evaluates security settings, but it records configuration and rule compliance rather than aggregating threat findings. Artifact provides compliance documents and Shield protects against DDoS traffic.

4. What does a breach and attack simulation platform primarily do?
- A It permanently patches vulnerable software on every endpoint it discovers
 - B It automatically blocks all outbound traffic from the protected network
 - C It runs scripted attack techniques in a controlled way to test whether existing controls detect and block them
 - D It stores encrypted backups of mailbox archives for legal hold and eDiscovery requests across every user mailbox in the tenant

Answer: C

Breach and attack simulation platforms run safe, scripted versions of attacker techniques and report whether the existing controls detected or blocked them. Automatic blocking is the tempting distractor, because a platform can help choose controls, but the platform itself is a test tool. Patching and backup storage are separate functions.

5. Sigma is a generic, vendor-neutral _____ format for describing log-based detections, which can be converted into many SIEM query languages.

Answer: rule (also accepted: rule format, detection rule, detection rule format)

Sigma describes a detection in YAML so that one rule can be shared and then converted into the query language of each target platform. Because it is independent of any single product, it is valuable for sharing detection content across organizations. The accepted answers reflect the common ways the format is named.

6. Which DevOps principle is most directly served by storing security automation code in version control and reviewing each change through a pull request?
- A Faster manual configuration of individual hosts
 - B Traceable, reviewable change control
 - C Replacing all audit logging with periodic screenshots
 - D Removing the need for any testing of changes

Answer: B

Version control with reviewed pull requests gives each automation change an author, a reason and a history, so changes can be audited and reverted. Faster manual configuration is the tempting distractor because it sounds like efficiency, but it moves work away from the reviewed, repeatable path. Screenshots are not an audit trail, and review supplements testing rather than replacing it.

7. Which MITRE ATT&CK tactic describes an adversary moving from one host to another inside a network?
- A Exfiltration
 - B Persistence, which keeps an adversary's access alive across restarts and credential changes on one host
 - C Discovery
 - D Lateral Movement

Answer: D

Lateral Movement is the ATT&CK tactic for moving between systems inside an environment, often by reusing credentials or remote services. Discovery is the tempting distractor because attackers enumerate hosts before moving, but discovery is reconnaissance inside the network rather than the move itself. Exfiltration concerns moving data out, and Persistence concerns keeping access.

8. What is a Microsoft Sentinel watchlist typically used for?
- A Storing reference data, such as approved IP ranges or VIP accounts, for use in queries and rules
 - B Creating dashboard visualizations of incident volume over time for the SOC leadership review meeting
 - C Setting the retention period for raw log tables
 - D Acting as a real-time block list for firewall ports

Answer: A

Watchlists hold reference data that queries and analytics rules can join against, such as a list of executive accounts or known-good IP ranges. Dashboards are the job of workbooks, which is the tempting distractor. Retention is configured on the workspace and tables, and watchlists do not enforce firewall behavior.

9. Should a SOAR playbook that quarantines an endpoint usually require an approval step for high-impact actions?
- A True
 - B False

Answer: A (True)

True. Quarantining a production endpoint or disabling an account can interrupt business operations, so a well-designed playbook gates high-impact actions behind a reviewed decision. Fully automatic containment is reasonable for narrow, reversible actions, but not as a default for every high-impact step.

10. Which pattern in failed logon events (Event ID 4625) most suggests password spraying rather than brute force against one account?
- A One account receiving thousands of failed logons within one minute from a single source
 - B Successful logons (Event ID 4624) from known administrator workstations
 - C Many accounts each receiving a small number of failed logons from the same source
 - D Failed logons only on a domain controller during a midnight maintenance window

Answer: C

Password spraying tries one or a few common passwords across many accounts, so it shows many accounts with low failure counts from one source. Heavy failure counts against one account are the tempting distractor, since that is the brute force pattern. Successful logons from admin workstations and failures during maintenance are not spraying indicators.