

PRACTICE QUESTIONS

Elastic Certified SIEM Analyst

SHARED BY [u/pluckyseal2000](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Elastic Certified SIEM Analyst

Shared by [u/pluckyseal2000](#) on aiexamcerts

10 practice questions for the Elastic Certified SIEM Analyst exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/elastic/elastic-certified-siem-analyst. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. Which Elastic Agent integration turns a host into a protected endpoint with prevention and response capabilities?

- A Synthetics browser monitoring
- B Elastic Defend
- C Kubernetes integration for cluster metrics
- D System integration for host metrics

Answer: B

Elastic Defend is the integration that installs endpoint protection and enables response actions. System is the tempting distractor because it collects host metrics, but it does not prevent or respond to threats.

2. Elastic Security uses the _____ to view alerts, rules and cases in one place.

Answer: Security app (also accepted: Elastic Security app, Security)

The Security app in Kibana is the working area for detection and response. Users sometimes expect the Observability app to show this, which is the tempting but incorrect answer.

3. Which ECS field holds the result of an event, such as success or failure?

- A event.action
- B event.outcome
- C event.result
- D event.status

Answer: B

event.outcome records success, failure or unknown. event.action names the specific action, which makes it the tempting distractor, but it does not describe the result.

4. ECS field names should be used exactly as defined, because detection rules and dashboards match on those names.

- A True
- B False

Answer: A (True)

Rules, dashboards and integrations rely on the standard field names, so a custom name breaks matching. The tempting idea that any name works as long as it is descriptive is wrong.

5. Which two actions can an analyst take to triage an alert in Elastic Security? (Choose two.)

- A Delete the source index from the alert
- B Disable every rule in the Security app
- C Assign the alert and change its status
- D Reinstall the Elastic Defend policy
- E Investigate the alert in a timeline

Answer: C, E

Analysts assign alerts, update status and investigate in timelines as part of triage. Deleting source indices, disabling all rules or reinstalling policies are destructive or unrelated steps, so they are the tempting wrong answers.

6. Which query language is used in Elastic Security for event correlation sequences?

- A ES|QL only
- B Lucene only
- C SQL with joins
- D EQL

Answer: D

EQL, the Event Query Language, supports sequence and sequence by statements. ES|QL is the tempting distractor because it is a newer piped language, but EQL is the one built for ordered event sequences.

7. Which EQL keyword groups a sequence by a shared field such as host.id?

- A sequence by
- B group by, the SQL grouping keyword
- C join by
- D stats by

Answer: A

sequence by constrains each step in the sequence to share the same value of the field. group by is the tempting distractor from SQL, but EQL does not use that keyword.

8. A closed alert can be reopened by changing its status back to _____.

Answer: open

Alert status can move between open and closed as the investigation changes. A new alert is the tempting distractor, but reopening keeps the original alert history.

9. Which timeline feature shows a process tree for a host event?

- A Ingest pipeline simulator
- B Rule exception builder
- C Analyzer view for process ancestry
- D Fleet agent diagnostics

Answer: C

The analyzer view shows related processes and their ancestry around an event. The exception builder is the tempting distractor because it works from the same event, but it creates exclusions rather than showing process trees.

10. Which Osquery-based capability queries live endpoint state during an investigation?

- A Synthetic browser journey
- B Index lifecycle rollover
- C Ingest pipeline simulate
- D Live query with Osquery

Answer: D

Osquery live queries ask an endpoint for current state, such as running processes. The synthetic journey is the tempting distractor because it runs a remote check, but it does not inspect endpoint state.