

PRACTICE QUESTIONS

Elastic Certified SIEM Analyst

SHARED BY [u/Curious-Cluster-9724](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Elastic Certified SIEM Analyst

Shared by [u/Curious-Cluster-9724](#) 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 data view does the Security app use by default to read alert and event data?

- A logs-*
- B metrics-*
- C security-solution-default
- D apm-*

Answer: C

The security-solution-default data view covers the security indices the app expects. logs-* is the tempting distractor because logs are central to detection, but it does not include the security alerts index.

2. Mapping errors can cause detection rules to miss events, so field normalization is an important part of ingestion.

- A True
- B False

Answer: A (True)

Rules match on normalized field names, so an event with the wrong field produces no alert. Treating normalization as cosmetic is the tempting but wrong view.

3. Which Elastic Security capability tracks risk scores for users and hosts over time?

- A Index lifecycle management
- B Anomaly detection in Observability
- C Synthetic browser monitoring
- D Entity analytics with risk scores

Answer: D

Entity analytics computes user and host risk scores from alerts and behavior. Anomaly detection is the tempting distractor because it also finds unusual behavior, but it is a separate machine learning capability.

4. A rule that matches a sequence of events in order uses the EQL keyword _____ to start the chain.

Answer: sequence

EQL uses sequence to introduce an ordered set of event queries. join is the tempting distractor because it combines data in SQL, but EQL does not use it for ordered chains.

5. Which two ECS fields identify the process and its parent for a process event? (Choose two.)

- A process.name
- B host.name
- C process.parent.name
- D user.name
- E source.ip

Answer: A, C

process.name names the running process and process.parent.name names the process that started it. host.name and user.name identify where and who, and source.ip describes network origin, so they are tempting but wrong for this question.

6. Which rule type uses machine learning jobs to flag unusual behavior rather than matching a fixed condition?

- A Custom query rule
- B Machine learning rule
- C Threshold rule
- D Indicator match rule

Answer: B

Machine learning rules alert on anomalies from trained jobs. A threshold rule is the tempting distractor because it also flags counts, but it checks a fixed limit.

7. Which action on a Kibana alert moves it into a case for team investigation?

- A Create an exception
- B Add to a timeline only
- C Add to a case
- D Change the rule interval

Answer: C

Adding an alert to a case groups it with related evidence for the team. Creating an exception is the tempting distractor because it also handles alerts, but it suppresses future matches rather than tracking the investigation.

8. Alert suppression can reduce duplicate alerts, but it can also hide repeats that need separate review if the grouping fields are chosen poorly.

- A True
- B False

Answer: A (True)

Suppression collapses repeats by chosen fields, so a broad grouping can merge distinct incidents. The assumption that suppression never affects investigations is the tempting error.

9. Which setting in a timeline controls the time window shown for the investigation?

- A Date and time picker
- B Rule severity filter for alerts
- C Action connector for notifications
- D Exception operator for matching values

Answer: A

The date and time picker sets the window that a timeline searches. Rule severity is the tempting distractor because it describes an alert, but it does not limit the search window.

10. Which Elastic Defend response action isolates an endpoint from the network while keeping the management channel open?

- A Kill process
- B Host isolation
- C Suspend process
- D Get file

Answer: B

Host isolation cuts network access except to the Elastic management channel. Kill process is the tempting distractor because it is also a containment step, but it stops one process, not the host's network.