CERTLABZ CERTIFICATION BOARD

Certified Security Operations Analyst (CSOA)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working security operations analyst would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1 — Domain 1: SOC and SIEM Foundations — DATA

Sarah Miller maps each SOC tier to its main task, with one task missing.

Tier	Main task
Tier 1	Triage and alert review
Tier 2	(to choose)
Tier 3	Threat hunting
SOC lead	Run the shift

Table 1.1 SOC tiers and tasks.

What is the Tier 2 task?

A. Sign the budget
B. Deep investigation
C. Approve all hires
D. Set board strategy

Correct answer: B
Tier 2 analysts take escalations from Tier 1 and carry out deep investigation of confirmed or complex alerts. Budgets and hiring sit with management, and setting strategy is not the analyst role.

Question 2 — Domain 2: Log Sources and Data — DATA

James Carter matches each log source to what it records, with one entry missing.

Source	Records
Firewall	Allowed and denied flows
DNS	(to choose)
EDR	Process and file events
Proxy	Web requests

Table 2.1 Sources and their records.

What does the DNS log record?

A. Disk read errors
B. Name lookups
C. Payroll changes
D. Screen brightness

Correct answer: B
DNS logs record the name lookups that hosts perform, which helps analysts spot beaconing and suspicious domains. Firewalls record flows, EDR records endpoint activity, and proxies record web requests.

Question 3 — Domain 3: Detection and Correlation — DATA

Emma Wilson reviews correlated alerts and their severity for one shift.

Alert	Count	Severity
Failed logins	40	Low
Malware on host	1	High
Port scan	6	Medium
Policy notice	3	Low

Table 3.1 Alerts by severity.

Which alert should be handled first?

A. Failed logins
B. Policy notice

C Malware on host

D Port scan

Correct answer: C
The malware on host alert carries high severity and points to an active compromise, so it takes priority over the lower items. Failed logins, a port scan, and a policy notice are lower severity and can wait behind the high alert.

Question 4 — Domain 4: Threat Detection and Hunting — CONFIG

Olivia Davis reviews a detection rule written to catch a common technique.

```
title: Many failed logons
source: windows security
event_id: 4625
threshold: 10 in 5m
group_by: source_ip
```

Listing 4.1 The detection rule.

Which technique does this rule catch?

A Data backup

B Brute force

C Patch install

D Log rotation

Correct answer: B
The rule counts many failed logon events from one source in a short window, which is the signature of a brute force attempt. A backup, a patch install, and log rotation do not produce bursts of failed logons.

Question 5 — Domain 5: Incident Triage and Response — DATA

David Brown maps each response step to its phase, with one phase missing.

Step	Phase
Isolate the host	Containment
Remove the malware	(to choose)
Restore from backup	Recovery
Write the report	Lessons learned

Table 5.1 Steps and phases.

What phase is removing the malware?

A Eradication

B Discovery
C Planning
D Billing

Correct answer: A
Removing the malware from the affected systems is the eradication phase, which follows containment and precedes recovery. Discovery and planning come earlier, and billing is not an incident response phase.

Question 6

Domain 6: Metrics, Automation and Compliance

CONFIG

Ava Thompson lists the shift metrics the SOC reports each week.

```
MTTD  mean time to detect
MTTR  mean time to respond
alerts_per_analyst
false_positive_rate
dwell_time
```

Listing 6.1 Weekly SOC metrics.

Which metric shows how fast threats are found?

A MTTR
B MTTD
C Dwell time
D False positives

Correct answer: B
MTTD, the mean time to detect, measures how quickly the SOC finds a threat after it starts. MTTR measures response speed, dwell time measures how long an attacker stays undetected, and the false positive rate measures alert quality.

Question 7

Domain 1: SOC and SIEM Foundations

A new SOC forwards logs into the SIEM but never tunes the correlation rules, so analysts drown in low value alerts and miss real threats. What best fixes this?

A Tune the rules
B Add more sources
C Turn off the SIEM
D Ignore all alerts

Correct answer: A
A SIEM only helps when its correlation rules are tuned to cut noise and surface real threats. Adding more raw sources worsens the flood, and turning it off or ignoring alerts leaves the SOC blind.

Question 8 Domain 2: Log Sources and Data

An analyst finds that endpoint clocks differ by minutes, so events from two hosts cannot be lined up during an investigation. What practice best prevents this?

A. Delete old logs
B. Sync time by NTP
C. Lower log volume
D. Store logs locally

Correct answer: B
Synchronising every source to a common time using NTP lets analysts correlate events across hosts on one timeline. Deleting logs, storing them only locally, or lowering volume does not fix mismatched clocks.

Question 9 Domain 4: Threat Detection and Hunting

Rather than wait for alerts, an analyst forms a hypothesis that an attacker is using a living off the land binary and searches the data to confirm or reject it. What is this activity?

A. Patch review
B. Threat hunting
C. Asset tagging
D. Backup testing

Correct answer: B
Forming a hypothesis and searching the data to prove or disprove it is threat hunting, a proactive search for hidden activity. Patch review, asset tagging, and backup testing are maintenance tasks, not proactive detection.

Question 10 Domain 6: Metrics, Automation and Compliance

A SOC handles the same phishing alert by hand dozens of times a day, and analysts spend hours on the repeat steps instead of real investigation. What best reduces this load?

A. Hire more staff
B. Delete the alerts
C. A SOAR playbook
D. Longer shifts

Correct answer: C
A SOAR playbook automates the repeatable steps of a common alert so analysts spend their time on real investigation. Adding staff or longer shifts scales the manual work, and deleting the alerts hides real threats.

CSOA-001. https://certlabz.com/certifications/certified-security-operations-analyst.html