CERTLABZ CERTIFICATION BOARD

CSOA-001

Certified Security Operations Analyst (CSOA)

Exam Objectives CSOA-001

About the exam

Item	Detail
Level	Intermediate
Number of questions	80. A performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions.
Delivery model	Computer adaptive in 3 stages of 28, 26, 26 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	120 minutes
Scoring	You need a score of 700 out of 900 to pass. Results are reported on a scale of 100 to 900, and 700 corresponds to answering 72% of the exam correctly. Harder questions carry more weight, so a score means the same thing on any route. Multiple-response items and PBQs are scored all or nothing.
Delivery	Online, fully proctored (webcam, microphone and screen).
Prerequisites	No formal prerequisite. Candidates do best with some hands-on IT or security experience and 30 to 50 hours of study.
Retakes	No waiting period after a failed first attempt. Candidates pay the exam price each time they attempt the exam. See the CertLabz Certification Retake Policy at certlabz.com/certification-retake-policy.html
Validity	3 years. Renew with 50 CEUs per cycle and the $35 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$149 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 SOC and SIEM Foundations (16%)	13

D2 Log Sources and Data (16%)

	13
D3 Detection and Correlation (17%)	14
D4 Threat Detection and Hunting (17%)	14
D5 Incident Triage and Response (17%)	13
D6 Metrics, Automation and Compliance (17%)	13
Total (100%)	**80**

Objectives by domain

Each objective may appear as knowledge, a scenario to judge, a circuit to trace or assemble, or a number to compute. Each form can carry up to 5 to 12 performance-based questions: drag-and-drop matching, sequencing and table completion, drawn fresh each attempt. The exam does not test any vendor's SDK syntax.

D1 SOC and SIEM Foundations — 16% — 13 questions

D1.1 What a SOC does
D1.2 SIEM basics
D1.3 Roles and tiers
D1.4 The monitoring workflow
D1.5 Data flow
D1.6 Key terms

D2 Log Sources and Data — 16% — 13 questions

D2.1 Log types
D2.2 Endpoints and network
D2.3 Cloud and identity logs
D2.4 Parsing and normalization
D2.5 Retention
D2.6 Data quality

D3 Detection and Correlation — 17% — 14 questions

D3.1 Detection rules
D3.2 Correlation
D3.3 Use cases
D3.4 Tuning and false positives
D3.5 Enrichment
D3.6 MITRE ATT&CK mapping

D4 Threat Detection and Hunting — 17% — 14 questions

D4.1 Hypothesis-driven hunting
D4.2 Indicators
D4.3 Behavioral analytics
D4.4 Threat intelligence
D4.5 Anomalies
D4.6 Documentation

D5 Incident Triage and Response — 17% — 13 questions

D5.1 Alert triage
D5.2 Prioritization
D5.3 Investigation
D5.4 Containment
D5.5 Escalation
D5.6 Handoff and recovery

D6 Metrics, Automation and Compliance — 17% — 13 questions

D6.1 SOC metrics
D6.2 SOAR and automation
D6.3 Playbooks
D6.4 Reporting
D6.5 Compliance
D6.6 Continuous improvement

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	50
Annual CE fee	$35
Alternative to CEUs	Pass the current version of the exam before the expiry date

Qualifying activities

Activity	CEUs
CertLabz labs, PBQs, courses and SkillTracker assessments	1 CEU per hour, up to 25 per cycle
Other industry certifications earned or renewed	10 to 25 each, depending on level
Conferences, webinars and training	1 CEU per hour, up to 20 per cycle
Security operations or cybersecurity work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or community contributions	Up to 15 per cycle
College courses in computing or security	10 per completed course

CertLabz Certification Retake Policy

- **No waiting period after a failed first attempt:** If you fail your first attempt at any CertLabz certification examination, CertLabz does not require any waiting period between the first and second attempt.
- **Once you pass, you cannot resit the same exam code:** A candidate who has passed an exam and achieved a certification cannot take that exam again under the same exam code without prior consent from CertLabz. You will need to wait until a new series of the exam is published before attempting to recertify by examination.
- **Beta examinations, one attempt only:** A CertLabz beta examination may be taken one time by each candidate.
- **Violations invalidate the attempt:** A test found to be in violation of this policy will be invalidated, and the candidate may be subject to a suspension period. Repeat violators will be permanently banned from the CertLabz Certification Program.
- **Every attempt is paid for:** Candidates must pay the exam price each time they attempt the exam. CertLabz does not offer free retests or discounts on retakes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Objectives document CSOA-001.
https://certlabz.com/certifications/certified-security-operations-analyst.html