CERTLABZ CERTIFICATION BOARD

CAES-001

Certified Adversary Emulation Specialist (CAES)

Exam Objectives CAES-001

About the exam

Item	Detail
Level	Advanced
Number of questions	120. 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 42, 39, 39 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	180 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 two to three years in offensive security, SOC or detection work and 60 to 100 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 75 CEUs per cycle and the $55 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$199 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 Adversary Emulation Foundations and Threat Intelligence (16%)	19

D2 Planning, Scoping and Rules of Engagement (16%)

	19
D3 Reconnaissance, Initial Access and Execution (17%)	21
D4 Command and Control, and Infrastructure (17%)	21
D5 Post-Exploitation, Persistence and Lateral Movement (17%)	20
D6 Detection, Purple Teaming and Reporting (17%)	20
Total (100%)	**120**

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 Adversary Emulation Foundations and Threat Intelligence — 16% — 19 questions

D1.1 Emulation versus penetration testing and red teaming
D1.2 MITRE ATT&CK tactics, techniques and procedures
D1.3 Threat-informed actor selection from CTI
D1.4 The Pyramid of Pain and why TTPs matter
D1.5 Building an adversary emulation plan
D1.6 ATT&CK Navigator for scope and coverage

D2 Planning, Scoping and Rules of Engagement — 16% — 19 questions

D2.1 Written authorization and legal boundaries
D2.2 Rules of engagement, scope and stop conditions
D2.3 White team, deconfliction and safety
D2.4 Assumed-breach versus full-chain scenarios
D2.5 Objectives, flags and success criteria
D2.6 Handling discovery of a real intrusion

D3 Reconnaissance, Initial Access and Execution — 17% — 21 questions

D3.1 Passive and active reconnaissance
D3.2 Phishing, pretexts and user execution
D3.3 Exploiting public-facing applications
D3.4 Valid accounts and password spraying
D3.5 Living off the land and macro abuse
D3.6 Safe, faithful execution within the RoE

D4 Command and Control, and Infrastructure — 17% — 21 questions

D4.1 C2 channels over HTTPS, DNS and cloud services
D4.2 Beacon intervals, jitter and traffic shaping
D4.3 Redirectors, team servers and OPSEC
D4.4 Malleable profiles and domain fronting
D4.5 Resilience and channel failover
D4.6 Controlled, attributable infrastructure

D5 Post-Exploitation, Persistence and Lateral Movement — 17% — 20 questions

D5.1 Privilege escalation and token abuse
D5.2 Credential access, pass-the-hash and Kerberoasting
D5.3 Discovery, lateral movement and remote execution
D5.4 Persistence mechanisms
D5.5 Collection and safe exfiltration with markers
D5.6 Defense evasion and faithful sequencing

D6 Detection, Purple Teaming and Reporting — 17% — 20 questions

D6.1 Purple teaming and the improvement loop
D6.2 Detection gaps, telemetry and true positives
D6.3 Atomic tests and full-chain validation
D6.4 ATT&CK-mapped coverage reporting
D6.5 Deconfliction records and re-testing
D6.6 Prioritized, actionable recommendations

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	75
Annual CE fee	$55
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
Red team, adversary emulation or detection work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or open-source contributions	Up to 15 per cycle
College courses in security or computing	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 CAES-001.
https://certlabz.com/certifications/certified-adversary-emulation-specialist.html