CERTLABZ CERTIFICATION BOARD

CTHS-001

Certified Threat Hunting Specialist (CTHS)

Exam Objectives CTHS-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 years in a SOC, incident response or detection role and 50 to 80 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 Hunting Foundations and Methodology (15%)	18
D2 Adversary Tradecraft and ATT&CK (18%)	22
D3 Telemetry and Data Sources (17%)	20

D4 Analysis Techniques (20%)

	24
D5 Hunting in Endpoint, Network, Cloud and Identity (18%)	22
D6 Detection Engineering, Reporting and Program (12%)	14
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 Hunting Foundations and Methodology — 15% — 18 questions

D1.1 Hypothesis-driven, baseline and model-assisted hunts
D1.2 PEAK and other hunt frameworks; the Hunting Maturity Model
D1.3 MITRE ATT&CK as the shared vocabulary; the Pyramid of Pain
D1.4 Threat-informed prioritization and crown-jewel analysis
D1.5 Hunt planning, scoping and outputs
D1.6 Dwell time, assume breach and the business case for hunting

D2 Adversary Tradecraft and ATT&CK — 18% — 22 questions

D2.1 Tactics, techniques, sub-techniques and procedures
D2.2 Initial access, execution and living off the land
D2.3 Persistence: tasks, services, run keys, WMI, cron
D2.4 Credential access and lateral movement: LSASS, Kerberoasting, pass the hash, RDP, SMB
D2.5 Command and control, beaconing and DNS tunnelling
D2.6 Defense evasion, discovery, exfiltration and pre-impact ransomware signals

D3 Telemetry and Data Sources — 17% — 20 questions

D3.1 Windows event IDs and audit policy: 4688, 4624, 4698, 4769, 7045, 1102
D3.2 Sysmon and EDR telemetry, PowerShell script block logging
D3.3 Network sources: Zeek, NetFlow, DNS, proxy
D3.4 Identity provider and cloud control-plane logs
D3.5 Linux and container telemetry: auditd, eBPF, runtime events
D3.6 Data quality: coverage, fields, retention, time synchronization, forwarding

D4 Analysis Techniques — 20% — 24 questions

D4.1 Stacking and long-tail review
D4.2 Baselines and first-seen analytics
D4.3 Beaconing, interval variance and entropy analysis
D4.4 Timeline reconstruction and cross-source joins
D4.5 Query languages and iterative refinement; known-good management
D4.6 Sigma, YARA and network signatures; model-assisted hunting

D5 Hunting in Endpoint, Network, Cloud and Identity — 18% — 22 questions

D5.1 Endpoint hunts: process lineage, persistence enumeration, LSASS access, remote tools
D5.2 Network hunts: reconnaissance fan-out, C2 over HTTP and DNS, staging and exfiltration
D5.3 Identity hunts: MFA fatigue, impossible travel, token replay, illicit consent
D5.4 Cloud hunts: IAM changes, disabled logging, metadata service access
D5.5 Active Directory hunts: Kerberoasting, golden tickets, GPO abuse
D5.6 Linux and container hunts

D6 Detection Engineering, Reporting and Program — 12% — 14 questions

D6.1 Converting hunts into detections; detection as code
D6.2 Coverage maps and gap prioritization
D6.3 Tuning, testing and re-validating detections
D6.4 Purple teaming and adversary emulation
D6.5 Hunt reports, libraries and metrics
D6.6 Escalation to incident response and program governance

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
Threat hunting, detection or SOC 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, networking 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 CTHS-001.
https://certlabz.com/certifications/certified-threat-hunting-specialist.html