

Quantum Security Course Plan

Cybertection Training Center. Course design, schedule, and assessment

Cybertection LLC

Draft v0.1, October 2026

Course Overview

Working title: Quantum Security for Red Teams **Provider:** Cybertection Training Center
Format: instructor-led, with hands-on labs. Length and format are placeholders until confirmed. **Textbook:** Quantum Cybersecurity Red Team Guide (separate document, draft v0.2) **Lab environment:** Quantum Labs hub (browser and Kali labs) and CyberQuan OS (CQ-Q labs)

Who it's for: Training Center students preparing for red team, SOC, and security analyst roles. They should know basic networking and the command line. No quantum physics background is needed.

Learning outcomes. By the end of the course, a student can:

1. Explain qubits, superposition, entanglement, and measurement in plain language.
2. Compare a classical and a quantum classifier fairly, using several seeds and clear metrics.
3. Explain how Grover's search, BB84, and Shor's algorithm affect real key sizes and protocols.
4. Run authorized recon, capture, and scanning, and save reproducible evidence.
5. Audit a system's TLS and crypto settings and rank its quantum risk.
6. Write a findings report that a technical reader and a manager can both act on.

Career link (to confirm). The work roles and KSAs will be mapped to the NICE Framework (NIST SP 800-181). Likely roles include Penetration Tester, Vulnerability Assessment Analyst, Cyber Defense Analyst, and Security Architect. Confirm all codes against the official NICE spreadsheet before publishing.

Schedule (draft: 8 weeks)

Each week has a lecture or reading block, one or more labs, and a checkpoint. The schedule follows the textbook's five parts.

Week	Topic	Textbook	Labs	Checkpoint
1	Orientation, authorized use, quantum basics	Ch. 1 and rules	B0; set up CyberQuan VM; K1	Evidence folder set up and checked
2	Quantum classifiers for detection	Ch. 2	B1, B2; CQ-Q2	Compare on three seeds
3	Search, randomness, key exchange	Ch. 3	B5, B6, B7; CQ-Q3, CQ-Q4, CQ-Q5	BB84 error rate with and without Eve
4	Shor's algorithm and RSA sizing	Ch. 4	B8; CQ-Q6	Midterm quiz (Weeks 1 to 4)
5	Recon and capture	Ch. 5 to 7	K2, K3, K4; CQ-Q1 capture	Labeled dataset, checked by instructor
6	Quantum-assisted detection	Ch. 8 to 10	K5, K6, K7, K8; CQ-Q1 finish	Confusion matrix and fair comparison
7	Crypto risk and migration	Ch. 11 to 13	K9, K10, K11, B9; CQ-Q7, CQ-Q8, CQ-Q9	Migration note for one system
8	Reporting and capstone	Ch. 14 and 15	K12, K13; CQ-Q10	Final capstone report

Flexibility. If the course runs shorter, merge Weeks 2 and 3, and keep the midterm and the capstone. If it runs longer, add a week for K-lab practice before Week 5.

Assessment

Formative (not graded)

- The check questions at the end of each chapter.
- Weekly labs, with feedback in the hub or from the instructor.
- Evidence folder review at each checkpoint.

Summative (graded)

Assessment	Week	Weight (draft)	What it checks
Lab checkpoints (weeks 1 to 7)	1 to 7	20%	Completed labs and saved evidence
Midterm quiz	4	20%	Foundations, classifiers, quantum key and search

Assessment	Week	Weight (draft)	What it checks
Final capstone report	8	60%	concepts Full engagement, scored on the rubric below

Capstone rubric (draft weights):

Area	Weight	A strong answer shows
Authorization	10%	Written scope; every action inside it
Evidence	20%	Commands and outputs saved and reproducible
Analysis	25%	Models compared fairly, with metrics and seeds
Quantum risk	20%	Findings ranked by how long the data must stay secret
Report	25%	Clear to a technical reader and a manager; each finding has severity and risk

Pass mark: to be set (suggested 70%). A student must pass the capstone and complete the authorization requirement to pass the course.

Academic integrity. Students must write their own report and cite any outside help. Answer keys are for instructors only.

Instructor Notes

Before each class

- Check the lab API health endpoint and the IonQ simulator quota.
- Confirm the CyberQuan VM image starts and the cq command runs.
- Confirm the Cloud Labs target is up for the Kali weeks.
- Keep an offline backup: the local simulator needs no network.

Safety rules to enforce

- Attacks only on assigned Cybertection lab targets.
- No real customer or employee data.
- No API keys in student hands or shared screens.
- Hardware runs (B3) are instructor-only. Show results from a prepared run instead of running live.

When a lab fails

1. Switch the student to the local simulator. It needs no key and no network.
2. If the lab API is down, use the offline labs and mark the checkpoint late, not failed.
3. Record the failure with the exact command and error text, with keys removed.

Pacing

- Lectures: no more than 45 minutes. The rest is lab time.
 - Each lab has a time budget. Students who finish early go to the stretch question in the guide.
-

Completion

A student completes the course when they:

1. Finish all labs in Weeks 1 to 8, or have approved alternatives.
2. Pass the midterm and the capstone.
3. Meet the authorization requirement in every lab.

Certificate or record: to be decided. Options: a Training Center certificate issued by the instructor, or a record in the student platform. A platform record needs student sign-in (Firebase Auth), which is not built yet.

Build Status

Item	Status
Textbook (Red Team Guide)	Draft v0.2
Quantum Labs hub (B and K labs)	Pages built; Cloud Run and hub deploy not done
CyberQuan OS (CQ-Q labs)	Plan and draft build files; ISO and OVA not built
CyberQuan product page	Draft; downloads “Coming soon”
Graded quizzes and answer keys	Not started
Instructor guide (full)	Not started; notes above are a starting point
Student sign-in and records	Not started
NICE mapping	Pending NICCS page confirmation

Open Decisions

1. Course length: 8 weeks, or another length?

2. Format: fully in-person, hybrid, or self-paced with live check-ins?
3. Pass mark and grade weights.
4. Certificate or completion record, and who issues it.
5. Which NICE work roles to advertise.
6. Whether the K labs (Kali, Cloud Labs target) are required for every student or only for the capstone track.