COMPTIA SECURITY+ SY0-701 · WEEK 1

Course Orientation and Fundamental Security Concepts



Objective 1.2 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Describe how the lessons, labs, quizzes, and the Lakeside Family Clinic project fit together.
2. Define confidentiality, integrity, and availability, and match a control to each.
3. Explain non-repudiation and why it depends on a digital signature or individual accounts.
4. Distinguish authentication, authorization, and accounting for both people and systems.
5. Outline a gap analysis and name the control plane and data plane parts of zero trust.
6. Select physical security and deception controls for a stated problem.

AGENDA

8 min	How this course works
10 min	CIA and non-repudiation
8 min	Authentication, authorization, and accounting
8 min	Authenticating people and systems
10 min	Exercise 1: name the concept
7 min	Gap analysis
10 min	Zero trust
10 min	Physical security
6 min	Deception and disruption
10 min	Exercise 2: the Lakeside walkthrough
3 min	Wrap-up

Every week follows the same rhythm

1. **Read** — Read the lesson page before class
2. **Lecture** — Ninety minutes on one or two exam objectives
3. **Exercises** — Apply each idea to a short scenario in class
4. **Lab** — Hands-on work in your own isolated virtual lab
5. **Project** — Each lab adds a piece to the clinic's security plan
6. **Quiz** — Ten exam-style questions to check yourself

Four goals every control serves



Confidentiality

Only authorized people can read the data.

Encrypted patient records



Integrity

Data is accurate and has not been changed without approval.

File hashes, change logs



Availability

Systems and data are there when authorized users need them.

Backups, redundant power



Non-repudiation

A person cannot credibly deny an action they took.

Digitally signed e-prescription

Authentication, authorization, and accounting

Step	Question it answers	Clinic example
Identification	Who do you claim to be?	A nurse types her username, jlopez
Authentication	Can you prove it?	Password plus a code from a phone app
Authorization	What are you allowed to do?	She can open charts but not payroll
Accounting	What did you do, and when?	The EHR logs every chart she opens

People and systems both prove who they are

Authenticating people

- Something you know: a password or PIN
- Something you have: a smart card or phone app
- Something you are: a fingerprint or face
- MFA combines two or more different factors

Authenticating systems

- A device certificate proves a laptop's identity
- 802.1X checks a device before the port opens
- Services use their own accounts and keys
- Mutual TLS: both ends present certificates

Which goal or function does each control serve



8

MINUTES · PAIRS

For each item, name the CIA goal, non-repudiation, or the AAA function it mainly supports. Be ready to defend it.

1. Nightly backups copied to a second site
2. A hash value posted next to a software download
3. A badge and a PIN are required at the pharmacy door
4. Front desk staff cannot open billing reports
5. Every chart view is logged with the user and the time
6. A doctor signs e-prescriptions with a private key
7. Laptop drives are encrypted with BitLocker
8. A second internet line from a different provider
9. The VPN checks the laptop's device certificate

Gap analysis compares today with the target

1

Pick a target

Choose a framework such as the NIST CSF or CIS Controls

2

Assess today

Document the controls actually in place now

3

Find the gaps

List each requirement not met, or met only in part

4

Prioritize

Rank the gaps by risk, cost, and effort

5

Plan

Write a remediation plan with owners and dates

Zero trust splits decisions from enforcement

Control plane: decides

- Adaptive identity: context changes the checks
- Threat scope reduction: least access needed
- Policy-driven access control
- Policy Engine decides; Administrator applies it

Data plane: enforces

- Subject or system: the user or device asking
- Policy Enforcement Point allows or blocks
- Implicit trust zone: kept as small as possible
- Traffic reaches the resource only after a yes

Layers that keep people and vehicles out

Bollards

Posts that stop vehicles but let people walk past.

Clinic entrance

Access vestibule

Two doors, one open at a time. Stops tailgating.

Data center entry

Fencing

Marks the boundary and slows anyone on foot.

Generator yard

Video surveillance

Cameras record events and deter attempts.

Lobby and back door

Guards and badges

Guards use judgment; badges show who may enter.

Front desk check-in

Lighting and sensors

Light deters; sensors detect motion or presence.

IR, pressure, microwave

Deception tools turn attackers into alerts

Tool	What it is	Clinic example
Honeypot	A decoy system that looks real and valuable	A fake file server named BILLING-01
Honeynet	A network of honeypots that mimics a segment	A decoy subnet of servers and workstations
Honeyfile	A bait file that alerts when opened	passwords.xlsx on a share, with an alert
Honeytoken	Fake data or credentials that alert when used	A fake admin account no one should use

Fix the gaps at Lakeside Family Clinic



10

MINUTES · SMALL GROUPS

For each finding, name the weakness, one control that fixes it, and the goal or function that control supports.

1. Staff share one admin login on the front desk PC
2. The server closet opens with a key kept on a hook beside it
3. No log shows who opened which patient chart
4. A laptop on the guest Wi-Fi can reach the file server
5. The back door to the parking lot is propped open at lunch
6. Nobody would notice someone browsing the file shares at night
7. The parking lot is dark after evening clinic hours

REVIEW

Five questions: write your answers first

1. A user hashes a downloaded installer and compares it to the vendor's posted hash. Which CIA goal does this check?
2. A logged-in nurse is blocked from opening payroll records. Which AAA function blocked her?
3. A login asks for a password and a code from an authenticator app. Is this MFA, and why?
4. In zero trust, which component makes the access decision, and which enforces it?
5. A fake administrator account exists only to raise an alert if someone uses it. What is it called?

TAKEAWAYS

Four things to take with you

01

CIA plus non-repudiation

Every control protects secrecy, accuracy, uptime, or proof of who acted.

02

AAA needs one account each

Shared logins break authentication, accounting, and non-repudiation.

03

Zero trust checks every request

The control plane decides; the Policy Enforcement Point enforces.

04

Layer physical and deception

Fences, doors, cameras, and decoys catch what technical controls miss.

NEXT Lab 1: Build the course lab