COMPTIA SECURITY+ SY0-701 · WEEK 11

Hardening, Assets, and Vulnerability Management



Objectives 4.1, 4.2 and 4.3 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Describe how a secure baseline is established, deployed, and maintained.
2. Choose hardening steps for workstations, servers, network gear, cloud, mobile, ICS, embedded, and IoT.
3. Recommend wireless and mobile settings, including WPA3, RADIUS, MDM, and a deployment model.
4. Explain application security techniques such as input validation, secure cookies, and code signing.
5. Trace an asset from procurement to certified disposal and name the security task at each stage.
6. Compare vulnerability identification methods, from scanning to bug bounties and threat feeds.
7. Prioritize vulnerabilities with CVSS and context, then pick a response and validate the fix.

AGENDA

8 min	Secure baselines
10 min	Hardening targets
8 min	Wireless installation and security settings
7 min	Mobile solutions and deployment models
8 min	Application security and sandboxing
10 min	Exercise 1: harden the clinic
9 min	Hardware, software, and data asset management
9 min	Identifying vulnerabilities
10 min	Analysis, response, validation, and reporting
9 min	Exercise 2: prioritize the findings
2 min	Wrap-up

A baseline is the known good starting point

1

Establish

Start from a CIS Benchmark or vendor guide, then adapt it

2

Test

Pilot on a few machines so the baseline breaks nothing

3

Deploy

Push it with GPO, MDM, images, or configuration scripts

4

Maintain

Rescan for drift, update with new versions and threats

Every device class hardens a little differently

Target	Key hardening moves
Workstations and servers	Remove unused software, patch, EDR, host firewall
Switches and routers	SSH not Telnet, change defaults, update firmware
Mobile devices	MDM, screen lock, encryption, app store controls
Cloud infrastructure	Least privilege IAM, no public buckets, logging on
ICS and SCADA	Segment from IT, restrict remote access, monitor
Embedded, RTOS, IoT	Change defaults, update firmware, isolate network

Plan the radio, then lock down the connection

Site survey

Walk the site to measure signal, noise, and neighbors

Before and after install

Heat map

Color map of signal strength over the floor plan

Finds dead zones and leaks

WPA3

SAE replaces the WPA2 pre-shared key exchange

WPA3-Personal and Enterprise

AAA and RADIUS

802.1X sends each user's login to a RADIUS server

Per-user accounts and logs

EAP methods

EAP-TLS, PEAP, and EAP-TTLS carry the credentials

EAP-TLS: certificates both sides

Who owns the phone decides how much you control

Model	Who owns it	Security tradeoff
BYOD	The employee	Cheap, least control; use containerization
COPE	The company, personal use allowed	Full control, with privacy rules for staff
CYOD	The company, user picks from a list	Control with a small, supported model list
MDM (all models)	Managed by IT	Enforces lock, encryption, wipe, app rules
Connection methods	Cellular, Wi-Fi, Bluetooth	Disable unused radios, VPN on open Wi-Fi

Build security into the application

Input validation

Check every input server side against an allow list

Secure cookies

Set Secure, HttpOnly, and SameSite on session cookies

Static code analysis

Scan source code for flaws before it runs

Code signing

Signature proves the author and that code is unchanged

Sandboxing

Run code in isolation, away from the host system

Monitoring

Log app errors and abuse, and alert on odd patterns

Exercise 1: harden Lakeside Family Clinic



8

MINUTES · PAIRS

For each problem, name the device class, the first hardening step, and the baseline setting that keeps it fixed.

1. Front desk PCs all log in with one shared local admin account
2. Staff Wi-Fi uses WPA2-Personal; the password is on a sticky note
3. Doctors read email on personal phones with no lock screen
4. The core switch is managed over Telnet with the default password
5. The vaccine fridge sensor is an IoT device on the main network
6. The patient portal login form passes input straight to SQL
7. The file server runs FTP and a print spooler it does not need
8. Old laptops sit in a closet, waiting to be thrown away

Track every asset from purchase to disposal

1

Acquire

Buy from vetted vendors; security reviews the purchase

2

Assign

Record an owner and a data classification

3

Monitor

Keep the inventory current with discovery scans

4

Dispose

Sanitize or destroy, get a certificate, honor retention

Many ways to find a weakness before attackers

Method	What it finds
Vulnerability scan	Known flaws and missing patches across hosts
Static and dynamic analysis	Code flaws at rest (SAST) and running (DAST)
Package monitoring	Vulnerable third-party libraries in your apps
Threat feeds	OSINT, vendor, ISAC, and dark web intelligence
Penetration testing	Exploitable paths a skilled tester can chain
Disclosure and bug bounty	Flaws reported by outside researchers

Confirm, prioritize, fix, and prove it is fixed

1

Confirm

Rule out false positives; watch for false negatives

2

Prioritize

CVSS plus exposure, environment, and impact

3

Respond

Patch, segment, compensate, insure, or except

4

Validate

Rescan, audit, and verify the fix holds

5

Report

Show owners the trend, open items, and exceptions

Exercise 2: rank the clinic's findings



7

MINUTES · SMALL GROUPS

Rank the six findings from first to last fix. For each, pick a response and say how you will validate it.

1. A: VPN appliance, CVSS 9.8, internet facing, listed in CISA KEV
2. B: Lab test server, CVSS 9.1, no network path to patient data
3. C: EHR web server, CVSS 6.5, public exploit, holds patient records
4. D: Printer, CVSS 7.5, but the vendor backported the fix last month
5. E: Intranet server still allows TLS 1.0, CVSS 5.3
6. F: Old X-ray PC, CVSS 8.8, vendor will not support a patch

REVIEW

Five questions: write your answers first

1. What are the three stages in the life of a secure baseline?
2. Why should a site survey come before installing wireless access points?
3. How do COPE and CYOD differ?
4. What is the difference between sanitization and destruction?
5. A scan flags a critical CVE, but the server has the vendor's backported fix. What is this, and what next?

TAKEAWAYS

Four things to take with you

01

Baselines beat one-off fixes

Write the standard once, deploy it everywhere, and scan for drift.

02

Fit hardening to the device

A switch, a phone, and a PLC each need their own hardening steps.

03

Know every asset you own

You cannot patch, track, or wipe a device that is not in the inventory.

04

Score, then add context

CVSS starts the ranking; exposure and impact finish it. Then rescan.

NEXT Lab 11: Harden a lab host against a CIS Benchmark and rescan