

AP Cybersecurity | Unit 4

4.1 Hardening and Baselines

Solutions

Reference scenario

Create a baseline for shared lab computers used by students.

Current: local administrator for all users

Unused service: enabled

Screen lock: off

Approved applications: documented

4.1.1

Why is a baseline more useful than a one-time instruction to secure each laptop?

It defines repeatable approved settings, supports consistent provisioning, and provides a reference for finding drift or unauthorized changes.

4.1.2

A proposed control prevents a required assistive tool from running. What should happen before broad deployment?

Investigate the conflict in a representative test, involve the responsible owners, and find an approved configuration that preserves access while reducing risk. Document any justified exception and verification.

AP Cybersecurity | Unit 4

4.2 Patch and Vulnerability Management

Solutions

Reference scenario

Prioritize approved updates using exposure and consequences.

A: internet-facing service, high-risk known flaw

B: isolated test device, low-impact flaw

C: staff laptop, routine update

4.2.1

Why should a patch downloaded from an unverified forum not be trusted merely because it claims to fix an urgent flaw?

The source or file may be malicious or incorrect. Obtain updates through trusted vendor or organizational channels and validate the deployment.

4.2.2

List three pieces of evidence that show a patch process is complete.

Record the installed version or update status, verification that the targeted weakness is addressed as expected, and a successful required-workflow test. Track failed or deferred devices separately.

AP Cybersecurity | Unit 4

4.3 Malware, Endpoint Detection, and Response

Solutions

Reference scenario

An endpoint alert quarantines a suspicious attachment. Plan the next investigation.

Alert: attachment quarantined

User report: attachment opened earlier

Outbound connection: recorded after opening

4.3.1

Why is deleting the alert and declaring the device clean a weak response?

It discards useful evidence and ignores activity that may have occurred before quarantine. Investigate execution, persistence indicators, account use, and related devices as appropriate.

4.3.2

Name one containment action and one recovery check for an affected endpoint.

Containment may include approved network isolation to limit further communication. Recovery should verify the corrected baseline, required application behavior, and absence of the investigated indicators under the incident plan.

AP Cybersecurity | Unit 4

4.4 Device Accounts, Logs, and Least Privilege

Solutions

Reference scenario

Build a timeline from device and account evidence.

10:00 individual user login
10:03 new administrator account
10:04 endpoint alert
10:06 device isolated

4.4.1

Why do individual maintenance accounts improve investigation over one shared administrator login?

They make activity easier to attribute to an authorized identity, support role-specific access, and simplify revocation. Logs still require review because accounts can be compromised.

4.4.2

A user needs to install one approved update. Explain a safer approach than granting permanent administrator access.

Use a managed deployment or approved time-limited maintenance privilege. Verify completion, remove the temporary elevation, and record the change.