AP Cybersecurity Study Sheet

Threat → Vulnerability → Attack → Impact → Detection → Mitigation

Study goal: Identify each concept in a scenario and explain how a security control reduces risk.

The six essential concepts

Concept	Meaning and question to ask	Example
Threat	A potential source of harm. Who or what could cause harm?	A cybercriminal group
Vulnerability	A weakness that can be exploited. What makes the system susceptible?	A weak administrator password
Attack	An attempt to exploit a weakness or compromise a system. What action is taken?	Guessing a password and logging in
Impact	The resulting harm or consequence. What was lost, changed, or interrupted?	Customer records are deleted
Detection	Recognizing or investigating suspicious activity. How do defenders notice it?	An alert about failed logins
Mitigation	Reducing the likelihood or severity of harm. What reduces risk?	Enable multifactor authentication

Remember the relationship

A threat may exploit a vulnerability through an attack, causing an impact. Defenders use detection to recognize activity and mitigation to reduce risk.

The arrows are a study model, not a required timeline. Vulnerabilities may exist before a threat appears. Detection can occur before damage, and mitigation can be used before, during, or after an incident.

Connect impact to the CIA triad

Confidentiality: information is exposed to unauthorized people.
Integrity: information is changed or deleted without authorization.
Availability: authorized users cannot access a service or information.

Apply the concepts: common scenarios

1. Weak password and remote access

Threat: An attacker seeks access to an administrator account.

Vulnerability: The remote-desktop service is protected by a weak password.

Attack: The attacker guesses the password and logs in.

Impact: Files are stolen (confidentiality) or deleted (integrity and possibly availability).

Detection: Logs show repeated failed logins or logins from distant locations within minutes.

Mitigation: Use strong, unique passwords and MFA; disable unnecessary remote access; reset compromised credentials.

2. Ransomware and an unpatched server

Threat: A criminal group capable of deploying ransomware.

Vulnerability: A known software flaw remains unpatched.

Attack: An attacker exploits the flaw and installs ransomware.

Impact: Encrypted files become inaccessible, harming availability.

Detection: Antivirus or endpoint software reports suspicious processes or ransomware activity.

Mitigation: Patch software; isolate infected devices; use protected, tested backups to support recovery.

3. SQL injection and exposed records

Threat: An attacker wants to access a website’s database.

Vulnerability: The application builds SQL commands by combining untrusted input with query text.

Attack: The attacker submits input that changes the intended database command.

Impact: Customer records are exposed, harming confidentiality.

Detection: A web application firewall or application logs flag suspicious input.

Mitigation: Use parameterized queries and appropriate database permissions; validate input as an additional control.

Key idea: Parameterized queries keep user input separate from SQL instructions. Input validation alone is not a substitute.

More scenarios and security tools

4. Phishing and a malicious attachment

Threat: A malicious sender impersonates a trusted person.

Vulnerability: Employees do not recognize suspicious attachments; execution controls are insufficient.

Attack: An employee opens an attachment that installs a remote access Trojan (RAT).

Impact: The attacker steals confidential documents.

Detection: Endpoint software flags suspicious programs or connections to an external server.

Mitigation: Train users to verify unexpected requests; filter risky attachments; restrict execution and isolate compromised devices.

5. Distributed denial of service (DDoS)

Threat: A group controls many compromised computers.

Vulnerability: The service has limited capacity and inadequate traffic controls.

Attack: Many devices flood the web server with requests.

Impact: Customers cannot reach the store, harming availability.

Detection: Monitoring detects unusual traffic volume and service degradation.

Mitigation: Use rate limiting, DDoS filtering, and a CDN or provider with DDoS protection.

Know these tools and terms

Social engineering: Manipulating people into revealing information or taking unsafe actions. Phishing uses deceptive messages.

SIEM: Security information and event management: collects and correlates logs to help identify suspicious patterns.

Endpoint detection: Monitors computers for suspicious processes, files, and network activity.

WAF: Web application firewall: inspects web requests and can alert on or block suspicious traffic.

MFA: Multifactor authentication: requires different types of evidence, such as a password and a security key. Two passwords are not two factors.

Rate limiting / CDN: Rate limiting restricts request volume. A content delivery network distributes content delivery; DDoS protection depends on its capabilities and configuration.

How to analyze a question

Focus on the specific detail being asked about

A single scenario can include all six concepts. Identify the highlighted person, weakness, action, consequence, observation, or control.

Threat vs. vulnerability: The criminal is the threat; the weak password is the vulnerability.

Attack vs. impact: Flooding a server is the attack; customers being unable to use it is the impact.

Detection vs. mitigation: A tool reporting malware is detection; blocking or isolating it is mitigation. One tool may do both.

Attempt vs. success: An attack does not have to succeed. Controls may prevent the intended impact.

Alert vs. proof: An unusual login or traffic spike needs investigation. Travel, VPNs, or legitimate demand can also create unusual patterns.

Open port vs. weakness: An open port may support a needed service. Weak authentication or unnecessary exposure creates risk.

Quick self-check

Classify each item as threat, vulnerability, attack, impact, detection, or mitigation. Explain your choice before checking the answers.

1. A criminal group plans to steal student records.
2. An administrator uses a reused, easily guessed password.
3. Someone uses stolen credentials to sign in.
4. Student records are copied to an unauthorized person.
5. A security tool alerts on the unusual sign-in.
6. The school revokes active sessions and enables MFA.

Self-check answers

1. Threat - potential source of harm.
2. Vulnerability - exploitable weakness.
3. Attack - unauthorized access attempt.
4. Impact - confidentiality is lost.
5. Detection - suspicious activity is recognized.
6. Mitigation - access is contained and future risk is reduced.

Before the assessment, you should be able to...

Define all six terms; separate an attacker from a weakness; distinguish an action from its consequence; recognize detection tools; and choose a mitigation that addresses the specific weakness or harm.

Based on the supplied 40-question AP Cybersecurity review. This sheet expands the explanations and clarifies that detection and mitigation are not limited to the end of an incident.