

AP Cybersecurity	Common Mistakes
<i>Every free-response point here is a specific action in a specific scenario – which rule, which address, which permission. Everything below is a rule the readers apply.</i>	
How the readers score a scenario response	
✗ Recommending a control in general terms – ‘improve the firewall’.	
✓ Say exactly what changes: which rule, which port, which direction.	
The guidelines withhold the point from responses that are vague or unrelated to the policy.	SG2026
✗ Adding a new rule where the question asked you to modify an existing one.	
✓ Modify the rule the scenario names.	
The guidelines list suggesting a new rule instead of modifying one among the responses that earn no point.	SG2026
✗ Naming a change without saying what it will do.	
✓ State the impact: which traffic will now be blocked, and what the user will see.	
The guidelines require an accurate impact of the change for the point.	SG2026
✗ Quoting an IP address or a log line from the wrong row.	
✓ Read the log carefully and cite the exact value the question is about.	
The guidelines reject any address other than the one in the evidence, and entries unrelated to the events asked about.	SG2026
✗ Writing a command with approximate syntax.	
✓ Get the syntax right – the flags, the order, the path.	
The guidelines state that incorrect command syntax earns no point.	SG2026
✗ Removing all permissions to be safe.	
✓ Apply least privilege: remove only what is not needed, and keep the access the role requires.	
The guidelines reject responses that suggest removing all permissions for a file on the system.	SG2026

✗ Misreading the permission bits.	
✓ Read them in threes – owner, group, others – and say which class you are changing.	
Named directly as a reason a response earns no point.	SG2026
■ Answer inside the scenario. A control that would be right for another network earns nothing here.	SG2026
1 · Introduction to Security	
✗ Using confidentiality, integrity and availability interchangeably.	
✓ Confidentiality is who can read it; integrity is whether it is unaltered; availability is whether it can be reached.	
The scenario always maps to one of the three, and naming the wrong one makes the control wrong.	
CIA	CED 1.2
✗ Calling any attack a virus.	
✓ Name the class: worm, trojan, ransomware, phishing, denial of service.	
The response depends on the class, so the label decides the rest of the answer.	CED 1.4
✗ Confusing a threat, a vulnerability and a risk.	
✓ A vulnerability is the weakness; a threat is what could exploit it; risk is the likelihood and impact together.	
The three are separate assessed concepts and questions ask for one specifically.	
、	CED 1.3
2 · Securing Spaces	
✗ Treating physical security as outside cybersecurity.	
✓ Include it: locked racks, badge access, cable management, visitor logs.	
Securing spaces is a unit of the course and appears in scenario questions.	CED 2.1
✗ Naming multi-factor authentication as two passwords.	
✓ The factors must differ: something you know, something you have, something you are.	
Two of the same factor is not multi-factor, which is the point being tested.	CED 2.4

3 · Securing Networks

- ✗ Saying a firewall ‘blocks hackers’.
- ✓ **It filters traffic against rules – by address, port and protocol.**

The mechanism is what lets you say which rule to change.
- ✗ Confusing a router, a switch and a firewall.
- ✓ **A switch forwards within a network, a router between networks, a firewall filters.**

Recommending a change on the wrong device cannot be credited.
- ✗ Saying a VPN makes a user anonymous.
- ✓ **It encrypts the tunnel between the user and the endpoint; it does not hide activity from the endpoint.**

Overstating a control leads to a recommendation the scenario does not support.

4 · Securing Devices

- ✗ Recommending patching without saying what it fixes.
- ✓ **Name the vulnerability class the update closes.**

The impact statement is a separate scored component.
- ✗ Treating an account lockout as a complete answer to failed logins.
- ✓ **Add monitoring and alerting – a lockout without a log entry hides the attack.**

The scenario questions ask what you would detect as well as what you would prevent.

5 · Securing Applications and Data

- ✗ Saying data is ‘encrypted’ with no more detail.
- ✓ **Say where: at rest, in transit, or both – and with symmetric or asymmetric keys.**

The scenario decides which applies, and the distinction is assessed.
- ✗ Storing passwords encrypted.
- ✓ **Hash them, with a salt. Encryption is reversible; hashing is not.**

The distinction is a standard discriminator and the wrong choice is a real vulnerability.

- ✗ Recommending a backup with no recovery test.
- ✓ **Say how the restore would be verified, and where the backup is kept.**

An untested backup is not a control, and the guidelines look for the practical detail.
- Where a question gives a log, a config or a permissions listing, the answer is in it. Cite the exact line.
- ✗ Recommending a control that the scenario says is already in place.
- ✓ **Read what exists, and add or change something that does not.**

A recommendation the scenario already satisfies cannot be an improvement.
- ✗ Answering a ‘describe the impact on users’ question with the technical change.
- ✓ **Say what the user will experience: which service stops working, what they must now do.**

The impact statement is scored separately from the change itself.

3 · Securing Networks

- ✗ Confusing a port number with an IP address.
- ✓ **The address names the host; the port names the service on it.**

A firewall rule needs both, and swapping them makes the rule meaningless.
- ✗ Saying a network is safe because it is behind a firewall.
- ✓ **Defence in depth: a firewall filters traffic and does nothing about a compromised device inside.**

Scenario questions usually turn on the control that the named one does not provide.

4 · Securing Devices

- ✗ Treating antivirus as sufficient endpoint protection.
- ✓ **Add patching, configuration hardening, and logging.**

The unit assesses layered device security, not a single product.
- ✗ Leaving default credentials in place because the device is internal.
- ✓ **Change them, and record that you did.**

Default credentials are a named vulnerability whatever the device’s location.

5 · Securing Applications and Data

✗ Validating user input in the browser only.

✓ **Validate on the SERVER too – client-side checks can be bypassed.**

This is the mechanism behind the injection vulnerabilities the unit covers.

CED 5.2

✗ Describing an incident response as ‘fix it and move on’.

✓ **Follow the phases: identify, contain, eradicate, recover, and review.**

The phases are assessed content and the review is what prevents a repeat.

CED 5.7