AP Cybersecurity

Common Mistakes · 常见错误

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. 自由作答题要给出具体场景中的具体操作：哪条规则、哪个地址、哪项权限。

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.

措施要具体到规则 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.

按题目要求修改现有规则 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.

要说明改动的影响 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.

要引用正确的日志条目 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.

命令语法要准确 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.

最小权限, 不是全部移除 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.

权限位按三组读 SG2026

■ Answer inside the scenario. A control that would be right for another network earns nothing here.

结合题目场景作答 SG2026

1 · Introduction to Security 安全导论

✗ 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 三性要分清 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.

要写出攻击的具体类型 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.

威胁、脆弱性、风险不同 CED 1.3

2 · Securing Spaces 保护物理空间

✗ 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.

物理安全也是考点 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.

多因素要用不同类别 CED 2.4

3 · Securing Networks 保护网络

✗ 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.

防火墙按规则过滤流量 CED 3.3

✗ 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.

路由器、交换机、防火墙功能不同 CED 3.2

✗ 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.

VPN 只加密隧道 CED 3.6

4 · Securing Devices 保护设备

✗ Recommending patching without saying what it fixes.

✓ **Name the vulnerability class the update closes.**

The impact statement is a separate scored component.

补丁要说明修复了什么 CED 4.2

✗ 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.

锁定之外还要监控告警 CED 4.5

5 · Securing Applications and Data 保护应用与数据

✗ 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.

要区分静态与传输加密 CED 5.4

✗ 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.

密码要哈希加盐 CED 5.5

✗ 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.

备份要能恢复并验证 CED 5.6

■ Where a question gives a log, a config or a permissions listing, the answer is in it. Cite the exact line.

答案在给定的日志或配置中 SG2026

✗ 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.

不要重复已有的措施 SG2026

✗ 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.

要写对用户的影响 SG2026

3 · Securing Networks 保护网络

✗ 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.

IP 是主机, 端口是服务 CED 3.4

✗ 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.

防火墙不能防内部威胁 CED 3.7

4 · Securing Devices 保护设备

✗ Treating antivirus as sufficient endpoint protection.

✓ **Add patching, configuration hardening, and logging.**

The unit assesses layered device security, not a single product.

终端防护要多层 CED 4.3

✗ 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.

默认口令必须修改 CED 4.4

5 · Securing Applications and Data 保护应用与数据

✗ 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.

服务端也要校验输入 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.

应急响应有固定阶段 CED 5.7