examundo

CompTIA Security+ 模拟考试（中文题库）

70 题，附答案。指南和译文由软件制作并核对，目前还没有人工审阅。

更新日期：2026 年 11 月 25 日 · examundo.tech/zh/comptia-security-plus/

安全运营

1. 网络管理员想找出发往境外 IP 段的出站带宽异常高峰，但不想在整个企业网络里抓取并存储完整的数据包内容。哪种日志数据源最适合这个目标？

A network administrator wants to identify unusual spikes in outbound bandwidth to a foreign IP range without capturing and storing full packet payloads across the enterprise. Which log data source is MOST appropriate for this goal?

A. 完整数据包捕获（PCAP）
B. Windows 安全事件日志
C. DNS 查询日志
D. NetFlow 数据

---

2. 管理员检查一台新部署的数据库服务器，发现默认启用了 Telnet 和 FTP 服务，还有几个没用的本地用户账户。这违反了哪条加固原则？

An administrator is reviewing a newly provisioned database server and finds Telnet and FTP services enabled by default, along with several unused local user accounts. Which hardening principle is being violated?

A. 最少功能
B. 职责分离
C. 纵深防御
D. 最小权限

---

3. 漏洞扫描报告显示，一台 Linux 服务器运行的 OpenSSL 版本过旧，存在已知 CVE。管理员人工核实后确认，实际安装的是已修补的版本，是扫描器误读了横幅（banner）信息。这种情况属于：

A vulnerability scan flags a Linux server as running an outdated OpenSSL version vulnerable to a known CVE. Upon manual verification, the administrator confirms the patched version is actually installed and the scanner misread the banner information. This scenario describes a:

A. 真阴性
B. 真阳性
C. 假阴性
D. 假阳性

---

4. 取证调查员扣押了一台怀疑存有内部人员窃取数据证据的笔记本电脑，并填写保管链表单，记录每个经手该设备的人。这份记录的主要目的是什么？

A forensic investigator seizes a laptop suspected of containing evidence of insider data theft and completes a chain-of-custody form documenting every individual who handles the device. What is the PRIMARY purpose of this documentation?

A. 确定由哪个部门负责承担更换设备的费用
B. 为保险目的计算被扣押资产的货币价值
C. 建立不间断的记录，证明证据完整且可在法律程序中采纳
D. 在调查结束后安排设备的例行维护

---

5. 一块被扣押的硬盘在两名取证分析师之间移交。每次移交都记录了日期、时间、经手人姓名和接触目的。这份记录维护的是什么?

A seized hard drive is transferred between two forensic analysts. Each transfer is logged with the date, time, individual's name, and purpose of access. What is being maintained by this documentation?

A. 保管链
B. 易失性顺序
C. 法律保全
D. 数据保留策略

---

6. 网络管理员取消了普通用户账户的本地管理员权限，只在某项任务确实需要时才授予提升的权限。这种做法体现了哪条安全原则?

A network administrator removes local administrator rights from standard user accounts, granting elevated access only when required for a specific task. This practice exemplifies which security principle?

A. 纵深防御
B. 零信任
C. 最小权限
D. 职责分离

---

7. 安全分析师根据最近的威胁情报提出一个假设，主动在企业遥测数据中查找一种新型攻击手法的迹象，而这种手法还没有触发任何 SIEM 告警。这项活动最适合归为哪种做法?

A security analyst proactively searches enterprise telemetry for evidence of a novel attack technique that has not yet triggered any SIEM alert, based on a hypothesis derived from recent threat intelligence. This activity is BEST described as which practice?

A. 威胁狩猎
B. 漏洞扫描
C. 自动化日志关联
D. 事件分级（triage）

---

8. 安全团队想检测一种无文件恶意软件攻击：它利用 PowerShell 把恶意代码直接注入内存，不会在磁盘上写入可执行文件。哪种安全工具最适合检测这种行为?

A security team wants to detect a fileless malware attack that uses PowerShell to inject malicious code directly into memory without writing an executable to disk. Which security tool is BEST suited to detect this behavior?

A. 数据防泄漏（DLP）代理
B. 基于签名的杀毒软件
C. 端点检测与响应（EDR）
D. 网络防火墙

---

9. 哪种控制最能保护被盗笔记本电脑硬盘上敏感数据的保密性?

Which control BEST protects the confidentiality of sensitive data stored on a stolen laptop's hard drive?

A. 入侵检测系统
B. 多因素认证
C. 全盘加密
D. 网络分段

---

10. 在服务器加固时，技术人员禁用了 Telnet，删除了默认的 guest 账户，并关闭了所有未使用的网络端口。这项工作最能体现哪个安全概念?

During server hardening, a technician disables Telnet, removes the default guest account, and closes all unused network ports. Which security concept does this activity BEST represent?

A. 建立安全基线
B. 执行最小权限
C. 缩小攻击面
D. 实施网络分段

---

11. 在事件响应中，取证分析师必须从一台已被入侵、但仍在开机的服务器上收集证据。按照易失性顺序，应该首先收集哪类数据?

During incident response, a forensic analyst must collect evidence from a compromised server that is still powered on. According to the order of volatility, which type of data should be collected FIRST?

A. RAM 内容和当前运行的进程
B. 存放在远程备份服务器上的归档日志文件
C. 打印在系统文档中的配置数据
D. 存放在本地硬盘上的文件

---

12. 哪种加固技术通过禁用未使用的端口和服务来缩小服务器的攻击面?

Which hardening technique reduces a server's attack surface by disabling unused ports and services?

A. 启用详细日志记录
B. 禁用不必要的服务
C. 安装杀毒软件
D. 配置蜜罐

---

13. 在取证调查中，分析师把一块被扣押的硬盘送到数字取证实验室制作镜像。哪份文件必须随硬盘一起移交，以保持证据的完整性?

During a forensic investigation, an analyst transfers a seized hard drive to a digital forensics lab for imaging. Which document must accompany the drive to maintain evidentiary integrity?

A. 事件响应剧本
B. 保管链表单
C. 业务连续性计划
D. 数据保留策略

---

14. 安全分析师正在一台仍然开机并联网的工作站上做实时事件响应。按照易失性顺序，分析师应在其他任何证据之前先收集哪项内容?

A security analyst is performing live incident response on a workstation that is still powered on and connected to the network. Following the order of volatility, which artifact should the analyst collect FIRST, before any other evidence?

A. 路由表和 ARP 缓存
B. RAM 内容和当前运行的进程
C. 存放在本地磁盘上的临时文件
D. CPU 寄存器和处理器缓存

威胁、漏洞和缓解措施

15. 网络管理员怀疑攻击者用伪造的 MAC 地址响应 ARP 请求，拦截并篡改内部客户端与默认网关之间的流量。哪种缓解措施最能针对这种攻击?

A network administrator suspects an attacker is intercepting and altering traffic between internal clients and the default gateway by responding to ARP requests with a spoofed MAC address. Which mitigation would BEST address this specific attack?

A. 用 VLAN 做网络分段
B. 实施 WPA3 加密
C. 禁用未使用的交换机端口
D. 动态 ARP 检测（DAI）

---

16. 一名员工打开了一个邮件附件，不久后发现共享盘上的所有文件都被加密了，还有一张要求用加密货币付款才能恢复访问的勒索字条。这次事件是由哪种恶意软件造成的?

An employee opens an email attachment and shortly afterward finds that all files on the shared drive have been encrypted, with a note demanding payment in cryptocurrency to restore access. Which type of malware caused this incident?

A. Rootkit
B. 逻辑炸弹
C. 勒索软件
D. 间谍软件

---

17. 攻击者给 IT 服务台打电话，冒充一位在紧急客户电话中被“锁在系统外”的公司高管，逼技术人员不验证身份就立即重置密码。这是哪种社会工程手法?

An attacker calls the IT help desk posing as a company executive who is 'locked out' during an urgent client call, pressuring the technician to reset a password immediately without verifying identity. Which social engineering technique is being used?

A. 翻垃圾（dumpster diving）
B. 借口（pretexting）
C. 尾随（tailgating）
D. 肩窥（shoulder surfing）

---

18. 攻击者拿到一份从另一家不相关公司以前的数据泄露中流出的大量用户名和密码，并系统地用这些原样的凭证组合去登录多个不同的网上银行平台。这使用的是哪种攻击技术?

An attacker obtains a large list of usernames and passwords leaked from a previous breach at an unrelated company and systematically attempts to log in with those exact credential pairs across several different online banking platforms. Which attack technique is being used?

A. 字典攻击
B. 暴力破解攻击
C. 撞库（credential stuffing）
D. 密码喷洒（password spraying）

---

19. 用户反映，共享网络盘上的文件突然带上了陌生的新扩展名，无法打开。每个受影响的文件夹里都出现了一个文本文件，要求支付加密货币来换取解密密钥。最可能是哪种威胁造成的?

A user reports that files on a shared network drive suddenly have a new, unfamiliar file extension and cannot be opened. A text file demanding cryptocurrency payment for a decryption key has appeared in each affected folder. Which threat is MOST likely responsible?

A. Rootkit
B. 逻辑炸弹
C. 蠕虫
D. 勒索软件

---

20. 攻击者给一名员工打电话，自称是公司服务台的人，要求员工把刚刚发到手机上的一次性验证码念出来。这用的是哪种社会工程途径?

An attacker calls an employee, claiming to be from the corporate help desk, and asks the employee to read back a one-time passcode that was just sent to their phone. Which social engineering vector is being used?

A. 语音钓鱼（vishing）
B. 短信钓鱼（smishing）
C. 肩窥
D. 尾随

---

21. 威胁行为者入侵了一个国防承包商员工经常访问的网站，并嵌入恶意 JavaScript，这段代码只在访问者的 IP 地址落在该承包商已知的范围内时才执行。这描述的是哪种攻击技术?

A threat actor compromises a website frequently visited by employees of a defense contractor and embeds malicious JavaScript that only executes when the visitor's IP address matches the contractor's known range. Which attack technique is being described?

A. 误植域名
B. DNS 投毒
C. 水坑攻击
D. 跨站脚本（XSS）

---

22. 办公室里好几台工作站开始异常发烫，风扇一直全速运转，监控工具显示即使员工没在工作，CPU 使用率也持续接近 100%。哪个失陷指标与这种表现最一致？

Several workstations in an office begin running unusually hot with fans at full speed continuously, and monitoring tools show sustained CPU usage near 100% even when employees are not actively working. Which indicator of compromise is MOST consistent with this behavior?

A. 防火墙规则变更导致内容被拦截
B. 计划任务造成的非周期日志记录
C. 加密挖矿恶意软件造成的资源消耗
D. 被入侵的 SIEM 丢失日志

---

23. 攻击者注册了一个与某银行正规网站几乎一模一样的域名，并入侵了一台公共 DNS 解析器，使输入正确银行网址的用户被悄悄重定向到攻击者的服务器。这描述的是哪种攻击？

An attacker registers a domain nearly identical to a bank's legitimate site and compromises a public DNS resolver so that users who type the correct bank URL are silently redirected to the attacker's server. Which attack does this describe?

A. 网址嫁接（pharming）
B. 借口（pretexting）
C. 语音钓鱼（vishing）
D. 误植域名（typosquatting）

---

24. 安全分析师调查一起入侵事件：攻击者使用定制的零日漏洞利用程序，在未被发现的情况下保持了八个月的持久访问，并窃取了与竞争对手国防合同投标相关的数据。最可能是哪类威胁行为者所为？

A security analyst investigates a breach in which the attacker used custom zero-day exploits, maintained undetected persistent access for eight months, and exfiltrated data tied to a competitor's defense contract bid. Which threat actor type MOST likely conducted this attack?

A. 脚本小子
B. 无意的内部威胁
C. 黑客行动主义者
D. 国家级 APT

---

25. 应付账款部门收到一封看似来自 CEO 账户的邮件，要求紧急向一个新的供应商账户汇款。邮件里没有恶意软件，也没有恶意链接。这属于哪种攻击？

The accounts payable department receives an email that appears to come from the CEO's account instructing them to urgently wire funds to a new vendor account. No malware or malicious link is involved. Which type of attack does this represent?

A. 撞库
B. 水坑攻击
C. 误植域名
D. 商业电子邮件入侵

---

26. 一名最近被解雇的系统管理员，用尚未停用的凭证远程登录，并删除了关键的备份归档。哪种威胁行为者类别最能描述此人？

A systems administrator who was recently terminated uses credentials that had not yet been deactivated to log in remotely and delete critical backup archives. Which threat actor category BEST describes this individual?

A. 黑客行动主义者
B. 国家级行为者
C. 脚本小子
D. 内部威胁

---

27. 安全团队发现，公司客户门户上有数千次成功登录，用的是此前一家不相关的零售网站数据泄露中流出的有效邮箱和密码组合。发生的是哪种攻击？

A security team notices thousands of successful login attempts against the company's customer portal using valid email and password combinations that were previously leaked in a breach of an unrelated retail website. Which attack is occurring?

A. 撞库
B. 彩虹表攻击
C. 密码喷洒
D. 暴力破解攻击

---

28. 攻击者给应付账款部门打电话，自称是外部审计员，在没有出示任何身份证明之前，就要求提供近期的发票记录来“核实合规情况”。这使用的是哪种社会工程手法？

An attacker calls the accounts payable department, claiming to be an external auditor, and requests recent invoice records to 'verify compliance' before offering any proof of identity. Which social engineering technique is being used?

A. 尾随
B. 诱饵（baiting）
C. 借口（pretexting）
D. 等价交换（quid pro quo）

安全计划管理和监督

29. 一家组织的领导层表示，在需要追加安全投入之前，公司愿意接受关键系统每年最多有 5% 的概率发生中断。这句话最能描述该组织的：

An organization's leadership states that the company is willing to accept up to a 5% chance of a critical system outage annually before additional security investment is required. This statement BEST describes the organization's:

A. 风险登记册
B. 风险容忍度（risk tolerance）
C. 风险偏好（risk appetite）
D. 风险例外

30. 一家总部在美国的 SaaS 公司替一家欧洲零售商托管客户关系管理数据，并严格按照零售商关于目的和保留期限的书面指示处理这些数据。依据 GDPR，这家 SaaS 公司担任什么角色？

A US-based SaaS company hosts customer relationship management data on behalf of a European retailer, processing that data strictly according to the retailer's written instructions on purpose and retention. Under GDPR, which role does the SaaS company hold?

A. 数据主体
B. 数据保护官
C. 数据控制者
D. 数据处理者

31. 一位德国客户给网上零售商发邮件，要求从公司系统中永久删除他的全部个人数据。哪部法规赋予这位客户提出该请求的法定权利？

A German customer emails an online retailer requesting that all of their personal data be permanently deleted from the company's systems. Which regulation grants this customer the legal right to make this request?

A. HIPAA
B. GDPR
C. PCI DSS
D. SOX

32. 一家金融服务公司发现，一套老旧的支付处理系统存在残余风险，在预算内无法完全修复。CISO 购买了一份网络保险，以覆盖数据泄露可能造成的损失。这最能代表哪种风险管理策略？

A financial services firm identifies a residual risk from a legacy payment processing system that cannot be fully remediated within budget. The CISO purchases a cyber insurance policy to cover potential losses from a breach. Which risk management strategy does this BEST represent?

A. 风险转移
B. 风险接受
C. 风险规避
D. 风险缓解

33. 一位潜在客户在签合同前，要求云服务提供商提供证据，证明其安全控制在 12 个月的期间内有效运行。提供商应提交哪种审计报告?

A prospective client requests evidence that a cloud service provider's security controls have operated effectively over a 12-month period before signing a contract. Which type of audit report should the provider supply?

A. SOC 2 Type I 报告
B. SOC 2 Type II 报告
C. SOC 1 Type I 报告
D. PCI DSS 合规证明（AOC）

---

34. 一家组织要求云供应商提供证据，证明其安全控制在 12 个月的运行期内有效，而不是只看某一个时间点。哪种报告最能满足这一要求?

An organization requests evidence of a cloud vendor's security control effectiveness over a 12-month operating period rather than at a single point in time. Which type of report BEST satisfies this requirement?

A. SOC 1，侧重与财务报告相关的控制，而不是安全
B. ISO 27001 认证，确认 ISMS 在审核时符合该标准的要求
C. SOC 2 Type I，证明控制设计在某一时间点是适当的
D. SOC 2 Type II，证明控制在较长的审查期内运行有效

---

35. 在与云服务提供商进行合同谈判时，合规官希望确保组织可以随时核查供应商的安全控制，而无需先征得供应商同意来安排审查。应争取在 SLA 中写入哪项合同条款?

During contract negotiations with a cloud service provider, a compliance officer wants to ensure the organization can verify the vendor's security controls at any time without needing the vendor's advance consent to schedule the review. Which contractual clause should be negotiated into the SLA?

A. 赔偿条款
B. 审计权条款
C. 保密协议
D. 不可抗力条款

---

36. 系统管理员想在每周例行维护窗口之外，部署一条紧急的防火墙规则变更，以拦截正在利用某个严重漏洞的攻击。按照标准的变更管理做法，应该首先做什么?

A systems administrator wants to deploy an emergency firewall rule change to block active exploitation of a critical vulnerability outside the normal weekly maintenance window. According to standard change management practices, what should occur FIRST?

A. 通过紧急变更流程提交变更，以加快审批
B. 等到下一次定期召开的变更咨询委员会（CAB）会议
C. 立即实施变更，事后再补记录
D. 在做任何改动之前，先通知终端用户可能出现的停机

---

37. 一家上市公司聘请外部会计师事务所，独立核实其财务报告控制是否符合监管要求。这是哪种类型的审计?

A publicly traded company hires an outside accounting firm to independently verify that its financial reporting controls comply with regulatory requirements. Which type of audit is being performed?

A. 漏洞评估
B. 内部审计
C. 合规自评
D. 外部审计

---

38. 采购团队在签合同之前，需要独立的保证，确认某 SaaS 供应商在安全、可用性和保密性方面的控制在过去 12 个月里有效运行。团队应向供应商索取哪份文件?

A procurement team needs independent assurance that a SaaS vendor's controls over security, availability, and confidentiality operated effectively over the past 12 months before signing a contract. Which document should the team request from the vendor?

A. SOC 2 Type II 报告
B. 自我声明问卷
C. 渗透测试摘要
D. 业务影响分析

---

39. 一家地区性银行的风险评估发现了一个漏洞，被利用的可能性很低，即使发生，造成的财务影响也很小。实施一项控制措施的成本超过了潜在损失。安全团队应向管理层建议哪种风险应对方式？

A risk assessment at a regional bank identifies a vulnerability that has a low likelihood of exploitation and would cause minimal financial impact if realized. The cost of implementing a control exceeds the potential loss. Which risk response should the security team recommend to management?

A. 风险规避
B. 风险缓解
C. 风险接受
D. 风险转移

---

40. 一家公司收到通知，称将有一起涉及数据泄露过失指控的诉讼，法务团队发出了法律保全（legal hold）。关于公司的标准数据保留策略，必须采取什么行动？

A company receives notice of pending litigation involving alleged data breach negligence, and the legal team issues a legal hold. Which action is required regarding the company's standard data retention policy?

A. 把记录移交给对方律师保管
B. 在保全解除之前，暂停对可能相关的记录进行例行销毁
C. 立即删除与案件有关的全部数据，以缩小证据开示（discovery）的范围
D. 加密受保全约束的所有记录，并继续按正常保留计划处理

---

41. 为应对钓鱼相关的风险，公司实施了多因素认证和网络分段，但由于存在中间人（adversary-in-the-middle）会话令牌窃取的可能，账户仍有一定被入侵的风险。这部分剩余的风险叫什么？

After implementing multifactor authentication and network segmentation to address a phishing-related risk, some risk of account compromise still remains due to the possibility of adversary-in-the-middle session token theft. What term describes this remaining risk?

A. 残余风险，即采取控制措施之后仍然存在的风险
B. 控制风险，即控制措施没有按设计运行的风险
C. 固有风险，即在采取任何控制措施之前存在的风险水平
D. 次生风险，即实施控制措施直接带来的新风险

---

42. 一位潜在客户要求供应商提供证据，证明其安全控制在过去六个月里有效运行，而不只是在某个时间点设计得当。供应商应提供哪份报告？

A prospective client requests evidence that a vendor's security controls have operated effectively over the preceding six months, not merely that they were properly designed at a single point in time. Which report should the vendor provide?

A. SOC 1 Type I
B. SOC 2 Type II
C. SOC 2 Type I
D. ISO 27001 证书

安全架构

43. 一家公司想使用专为本组织独家配置、不与任何其他租户共享的云基础设施。这描述的是哪种云部署模式？

A company wants to use cloud infrastructure that is provisioned exclusively for its own organization and is not shared with any other tenant. Which cloud deployment model does this describe?

A. 私有云
B. 社区云
C. 混合云
D. 公有云

---

44. 网络管理员对公司网络进行分段，使财务部门的工作站不能直接与市场部门的设备通信。实施的是哪种技术?

A network administrator segments a corporate network so that finance workstations cannot directly communicate with marketing department devices. Which technology is being implemented?

A. 负载均衡器
B. VLAN
C. NAT
D. VPN

---

45. 用户访问公司内部 Web 应用时，浏览器显示证书错误，提示该证书不受信任。客户端的信任库里最可能缺少 PKI 层级中的哪个组件?

A user's browser displays a certificate error stating the certificate is not trusted when visiting an internal company web application. Which component of the PKI hierarchy is MOST likely missing from the client's trust store?

A. Web 服务器的私钥
B. 客户端的会话票据
C. 根 CA 证书
D. 对称会话密钥

---

46. 系统管理员下载了一个 ISO 文件，想核实它在传输过程中没有损坏或被篡改。哪种方法最能做到这一点?

A systems administrator downloads an ISO file and wants to verify that it was not corrupted or altered during transfer. Which method BEST achieves this?

A. 把下载文件的 SHA-256 哈希值与供应商公布的哈希值比对
B. 把文件的字节大小与供应商网站上列出的大小比对
C. 用 AES-256 加密该文件，并确认可以成功解密
D. 打开 ISO，目视检查其内容

---

47. 网络工程师必须选择一种 TLS 密钥交换机制，保证即使服务器的长期私钥日后被泄露，过去会话的流量仍然保持机密。哪种密钥交换具备这一特性?

A network engineer must select a TLS key exchange mechanism that ensures past session traffic remains confidential even if the server's long-term private key is later compromised. Which key exchange provides this property?

A. 静态 RSA 密钥交换
B. 不带临时参数的预共享密钥（PSK）交换
C. 临时 Diffie-Hellman（DHE）
D. Kerberos 票据交换

---

48. 一家电池供电物联网传感器的制造商，必须对传输中的数据实施加密，但设备的处理能力和内存极其有限。选择加密算法时，哪个因素应该影响最大?

A manufacturer of battery-powered IoT sensors must implement encryption for data in transit but has extremely limited processing power and memory. Which factor should MOST influence the choice of cryptographic algorithm?

A. 为受限设备优化的轻量级密码学
B. 密钥很长的抗量子算法
C. 不管资源消耗如何，都选最强的可用算法
D. 为了向后兼容而使用老旧的 DES

---

49. 一家金融机构把其核心交易处理网络做了物理隔离，使它与互联网和任何其他网络都没有网络连接。应用的是哪个安全概念?

A financial institution physically isolates its core transaction-processing network so it has no network connection to the internet or any other network. Which security concept is being applied?

A. 微分段
B. 气隙
C. 屏蔽子网
D. 零信任

---

50. 数据中心管理员必须防止同在一个 VLAN 和子网内的两台虚拟机之间发生横向移动，而这两台机器之间的东西向流量又是应用正常运行所必需的。哪种控制最能达到这个目标?

A data center administrator must prevent lateral movement between two virtual machines that share the same VLAN and subnet, even though east-west traffic between them is required for the application to function. Which control BEST achieves this goal?

A. 以混杂模式部署基于网络的 IDS
B. 为每台虚拟机创建一个新的 VLAN
C. 在物理交换机上启用端口安全
D. 采用基于主机防火墙策略的微分段

---

51. 一家电商公司要求其 Web 服务器即使有一台发生故障也要保持可用，用户不能感觉到停机。哪种架构最能满足这一要求?

An e-commerce company requires its web servers to remain available even if one server fails, without users experiencing downtime. Which architecture BEST supports this requirement?

A. 每台服务器做全盘加密
B. 关机状态的气隙备份服务器
C. 带自动故障切换的主备负载均衡
D. 带手动重启流程的单一接入点

---

52. 公司想确保一次已签名的软件更新，日后不能被发布它的供应商否认。哪个密码学概念最能提供这种保证?

A company wants to ensure that a signed software update cannot later be disputed by the vendor who published it. Which cryptographic concept BEST provides this assurance?

A. 仅靠哈希的混淆
B. 通过数字签名实现不可否认性
C. 通过负载均衡实现可用性
D. 通过对称加密实现保密性

---

53. 一家电力公司为其 SCADA 控制系统维护一个完全隔离的网络，与企业 IT 网络没有任何物理或无线连接。这代表哪种安全控制?

A power utility maintains a completely isolated network with no physical or wireless connections to the corporate IT network for its SCADA control systems. Which security control does this represent?

A. 屏蔽子网
B. 气隙
C. 跳板机（jump server）
D. 虚拟专用网络

---

54. 对一栋智能建筑的安全评估发现，有几台物联网恒温器仍在使用出厂默认的管理员凭证，并与财务工作站连在同一个网段。哪项措施能解决最大的即时风险?

A security assessment of a smart building finds several IoT thermostats still using factory-default administrator credentials and connected to the same network segment as finance workstations. Which action addresses the GREATEST immediate risk?

A. 在移动应用中启用地理围栏
B. 在财务工作站上禁用 SNMP
C. 更改默认凭证，并把物联网设备放入隔离的 VLAN
D. 提高恒温器固件的更新频率

---

55. Web 管理员想为 TLS 客户端验证证书吊销状态，既不想让证书颁发机构（CA）看到单个客户端的浏览模式，也不想给 TLS 握手增加一次额外的往返。哪种方法最能满足这些要求?

A web administrator wants to verify certificate revocation status for TLS clients without exposing individual client browsing patterns to the certificate authority and without adding an extra round trip to the TLS handshake. Which approach BEST meets these requirements?

A. OCSP 装订（OCSP stapling）
B. 直接向 CA 发送标准 OCSP 查询
C. 证书吊销列表（CRL）检查
D. 证书固定（certificate pinning）

---

56. 在用于划分工业控制网络的普渡企业参考架构（Purdue Enterprise Reference Architecture）中，直接连接现场传感器和执行器的可编程逻辑控制器（PLC）和远程终端单元（RTU）通常位于哪一层?

In the Purdue Enterprise Reference Architecture used to segment industrial control networks, at which level do programmable logic controllers (PLCs) and remote terminal units (RTUs) that directly interface with field sensors and actuators typically reside?

A. 第 3 层，站点运营
B. 第 1 层，基本控制
C. 第 2 层，区域监督控制
D. 第 0 层，物理过程

通用安全概念

57. 变更咨询委员会正在审查一项请求：在定期维护窗口内部署一项关键的防火墙规则变更。如果变更导致意外的服务中断，变更请求中的哪一项对尽量缩短停机时间最重要?

A change advisory board is reviewing a request to deploy a critical firewall rule change during a scheduled maintenance window. Which element of the change request is MOST important for minimizing downtime if the change causes an unexpected service disruption?

A. 变更批准签字
B. 利益相关方影响分析
C. 回滚/回退计划
D. 沙箱测试结果

58. 数据中心安装了移动感应报警器，每当非工作时间在受限的服务器机房内检测到未经授权的移动时，就向安保人员报警。这套报警系统属于哪类控制?

A data center installs motion-activated alarms that alert security personnel whenever unauthorized movement is detected within a restricted server room after hours. Which type of control does this alarm system represent?

A. 预防性控制
B. 纠正性控制
C. 威慑性控制
D. 检测性控制

59. 数据中心管理员为一台关键数据库服务器部署了冗余电源、RAID 10 阵列和故障切换集群。管理员主要在解决 CIA 三要素中的哪一项?

A data center administrator deploys redundant power supplies, RAID 10 arrays, and a failover cluster for a critical database server. Which principle of the CIA triad is the administrator PRIMARILY addressing?

A. 不可否认性
B. 可用性
C. 完整性
D. 保密性

60. 公司要求，发起采购订单的员工不能与批准该订单付款的员工是同一个人。这执行的是哪条安全原则?

A company requires that the employee who initiates a purchase order cannot be the same employee who approves payment for that order. Which security principle is being enforced?

A. 职责分离
B. 最小权限
C. 强制休假
D. 岗位轮换

61. 在 AAA 安全模型中，哪个过程决定已通过验证的用户被允许在系统上执行哪些操作?

In the AAA security model, which process determines what actions an already-verified user is permitted to perform on a system?

A. 身份标识
B. 记账（accounting）
C. 身份验证
D. 授权

62. 一家组织迁移到这样的安全模型：每一个访问请求，无论来自内部员工还是外部合作伙伴，不管请求者位于哪个网络位置，都必须经过认证和授权。该组织采用的是哪种安全模型？

An organization migrates to a security model in which every access request, whether from an internal employee or an external partner, must be authenticated and authorized regardless of the requester's network location. Which security model has the organization adopted?

A. 零信任
B. 基于角色的访问控制
C. 纵深防御
D. 基于边界的防御

---

63. 攻击者截获银行应用服务器与其数据库之间的一笔转账请求，在交易完成前篡改了目标账号。CIA 三要素中的哪一项主要被破坏？

An attacker intercepts a wire transfer request between a bank's application server and its database, altering the destination account number before the transaction completes. Which tenet of the CIA triad has been PRIMARILY violated?

A. 保密性
B. 可用性
C. 不可否认性
D. 完整性

---

64. 在向生产服务器部署关键补丁之前，组织要求由一个指定的小组审查并签字批准。在变更管理流程中，这个小组的主要目的是什么？

Before deploying a critical patch to production servers, an organization requires review and sign-off by a designated group. What is the PRIMARY purpose of this group in the change management process?

A. 编写事件响应计划
B. 进行补丁的技术安装
C. 评估风险，批准或否决拟议变更
D. 进行年度安全意识培训

---

65. 在一次计划好的防火墙规则变更中，网络团队已批准的变更造成了影响客户服务的严重中断。按照标准的变更管理做法，为了把这次失败对业务的影响降到最低，实施之前本应准备好什么？

During a scheduled firewall rule change, the network team's approved change causes a critical outage affecting customer-facing services. According to standard change management practice, what should have been prepared BEFORE implementation to minimize the business impact of this failure?

A. 给安全团队用的事后事件报告模板
B. 列出所有受影响防火墙的更新后资产清单
C. 涵盖整个数据中心的修订版业务连续性计划
D. 有文档记录、并针对变更窗口测试过的回滚计划

---

66. 研究人员演示了可以构造出两个不同的可执行文件，产生完全相同的 SHA-1 摘要。当用 SHA-1 验证下载的软件包是否真实时，这种碰撞漏洞主要破坏了哪项安全属性？

Researchers demonstrate that two different executable files can be crafted to produce an identical SHA-1 digest. When SHA-1 is used to verify the authenticity of a downloaded software package, this collision vulnerability PRIMARILY undermines which security property?

A. 完整性
B. 授权
C. 保密性
D. 可用性

---

67. 在基于 NIST SP 800-207 模型的零信任架构中，哪个组件综合身份、设备状况和威胁情报等多个数据源来评估信任算法，并作出授予或拒绝访问某项资源的最终决定？

In a zero trust architecture based on the NIST SP 800-207 model, which component evaluates the trust algorithm using multiple data sources such as identity, device posture, and threat intelligence to render the final decision to grant or deny access to a resource?

A. 策略引擎（policy engine）
B. 持续诊断与缓解（CDM）系统
C. 策略执行点（policy enforcement point）
D. 策略管理器（policy administrator）

---

68. 一家金融服务公司希望在授予访问权限之前，访问决策能考虑用户所在的部门、所请求文件的敏感度分级、一天中的时间，以及设备的合规状态。哪种授权模型最能满足这一要求？

A financial services company wants access decisions to consider the user's department, the sensitivity classification of the requested file, the time of day, and the device's compliance status before granting access. Which authorization model BEST satisfies this requirement?

A. 基于属性的访问控制（ABAC）
B. 强制访问控制（MAC）
C. 基于角色的访问控制（RBAC）
D. 自主访问控制（DAC）

---

69. 一名新来的服务台技术人员，只被授予支持部门工作站的本地管理员权限，而不是整个域的管理员权限。这种配置体现了哪条安全原则？

A new help desk technician is granted local administrator rights to only the workstations in the support department rather than domain-wide administrator access. Which security principle does this configuration reflect?

A. 零信任
B. 职责分离
C. 最小权限
D. 纵深防御

---

70. 一位财务经理用自己的私钥对一笔转账批准进行数字签名，这样她日后就不能否认自己授权过这笔交易。这个场景最能说明哪个安全概念？

A finance manager digitally signs a wire transfer approval using her private key so that she cannot later deny having authorized the transaction. Which security concept does this scenario BEST illustrate?

A. 身份验证
B. 不可否认性
C. 保密性
D. 完整性

正确答案

1. D NetFlow 记录每次会话的元数据，如源和目的 IP、端口、协议、字节数和持续时间，能高效看出流量趋势，又不必存储完整内容。完整数据包捕获细节最全，但存储和处理成本太高，不适合在全企业持续做带宽趋势分析。DNS 日志只显示域名解析，看不出后续传输的数据量。Windows 安全事件日志记录的是主机上的认证和对象访问，不是网络带宽流量。

2. A 最少功能要求系统只运行实现预期用途所必需的服务、协议和账户，所以没用的 Telnet、FTP 服务和闲置本地账户会无谓地扩大攻击面，违反这条原则。最小权限限制的是账户或进程拥有的权限，不管运行了哪些服务。职责分离是把关键任务分给多人以防舞弊，和服务配置无关。纵深防御指在环境中叠加多层安全控制，不是针对单台主机的加固规则。

3. D 假阳性是扫描器报告了实际不存在的漏洞，正如这里人工核实后发现，尽管横幅信息有问题，安装的其实是已修补的版本。假阴性正好相反，是真实存在的漏洞没被发现。真阳性是扫描器正确发现了真实漏洞，真阴性是扫描器正确报告没有漏洞，这两项都和误读横幅的情况不符。

4. C 保管链记录持续、可核查地记下谁在何时接触过证据，证明证据没有被篡改，这对其在法律或纪律程序中被采纳至关重要。计算保险价值和确定部门费用是行政事务，与证据完整性无关。被扣押的设备要保持取得时的状态以供分析，不会安排例行维护，因为任何改动都会损害证据本身。

5. A 保管链是一份有据可查、不间断的记录，写明谁在何时因何经手证据，用来证明证据没有被改动，仍可在法律程序中被采纳。法律保全是为诉讼保存相关数据的通知，不是经手记录。数据保留策略规定数据保存多久，不记录谁接触过。易失性顺序决定在运行中的系统上采集证据的先后，与扣押后的保管追踪无关。

6. C 最小权限把每个账户限制在完成其工作所必需的访问权限内，只有在有正当理由时才临时授予提升的权限。职责分离是把关键任务分给多人以防舞弊，与限制个人访问级别是不同的控制。纵深防御是在整个系统里叠加多层安全控制，不管单个账户的权限。零信任是要求持续验证每个请求的更大的架构模型，最小权限只是它的一项支撑原则，不是题中描述的概念。

7. A 威胁狩猎是借助情报和分析师经验，以假设为导向，主动搜寻尚未被发现的威胁，这使它有别于纯被动的检测。漏洞扫描是找出系统中的已知弱点，不是查找正在发生的入侵迹象。自动化日志关联是 SIEM 基于规则的被动功能，没有人工提出假设并验证的过程。事件分级只在已有告警或已报告的事件之后才发生，而狩猎开始时并没有任何触发告警。

8. C 端点检测与响应（EDR）持续监控端点上的进程行为、命令行活动和内存操作，即使恶意文件从未落盘，也能标记异常的 PowerShell 执行和内存中的代码注入。基于签名的杀毒软件主要匹配已知的恶意特征；签名也可能发现驻留内存的威胁，但 EDR 的行为遥测更适合这种场景。网络防火墙在网络边界检查流量，看不到端点上的本地进程行为。DLP 代理的重点是防止敏感数据外泄，不是检测恶意执行行为。

9. C 全盘加密让磁盘上的所有数据在没有正确解密密钥时无法读取，所以即使硬盘被拆下并离线访问，被盗笔记本电脑里的数据仍然保密。网络分段限制网络中的横向移动，但硬盘被取出后它起不到保护作用。多因素认证保护的是登录，如果硬盘被拔出并挂载到别处，就可以绕过。IDS 检测可疑的网络活动，对被盗设备上的静态数据没有任何保护。

10. C 禁用不必要的服务、删除默认账户和关闭未使用的端口，都是在消除攻击者可能利用的入口，这正是缩小攻击面的定义。网络分段是把网络划分成相互隔离的区域，不是关闭单台主机上的功能。最小权限是把用户权限限制在完成任务所需的最低限度，不涉及服务配置。安全基线是记录在案的标准配置本身，而这里描述的是朝着该基线进行加固的行为。

11. A 易失性顺序按证据消失的快慢确定优先级；RAM 内容、活动的网络连接和运行中的进程在机器断电的瞬间就会丢失，所以必须最先获取。磁盘文件在关机后仍然存在，可以稍后处理。远程备份日志已经保存在主机之外，是最不易失的来源之一。打印的文档是静态的，根本不是时间敏感的证据，所以在开机状态下采集时优先级最低。

12. B 禁用不必要的服务并关闭不需要的端口，直接减少系统上可被利用的入口数量，这是加固的核心步骤。详细日志记录提高了检测时的可见性，但不会缩小攻击面。安装杀毒软件可以预防、检测和清除恶意软件，但不会消除暴露的服务。蜜罐是用来吸引攻击者以便研究的诱饵系统，不是针对生产服务器的加固措施。

13. B 保管链表单记录每个经手证据的人，以及每次移交的日期、时间和目的，有助于保持证据的完整性和可采纳性，但它本身并不能独立证明证据没有被改动。事件响应剧本指导响应行动，不追踪证据的经手情况。业务连续性计划针对中断期间的运营韧性，与取证证据无关。数据保留策略规定日志和数据保存多久，不追踪实物证据在保管人之间的流转。

14. D RFC 3227 把 CPU 寄存器和处理器缓存排在易失性顺序的第一位，因为处理器状态变化极快，断电即丢失。RAM 内容和运行中的进程，以及路由表和 ARP 缓存，属于紧随其后的同一大层级，与内核统计数据并列；RFC 没有规定这两项之间谁先谁后。本地磁盘上的临时文件通常排在这些易失性内存来源之后，不过它们在取证过程中也可能改变或消失。

15. D 动态 ARP 检测（DAI）根据受信任的 DHCP 监听绑定表来验证 ARP 数据包，并丢弃伪造的 ARP 响应，直接对付题中描述的 ARP 欺骗中间人攻击。用 VLAN 做网络分段只是限制广播域的范围，并不直接验证或阻止同一 VLAN 内的伪造 ARP 流量。禁用未使用的交换机端口只缩小物理攻击面，不涉及活动端口上的 ARP 验证。WPA3 加密保护的是无线流量，与有线网络中的 ARP 欺骗无关。

16. C 勒索软件加密受害者的文件，并索要付款（通常是加密货币）来换取解密密钥，正是题中的情形。间谍软件暗中收集用户数据，不加密文件，所以不符。Rootkit 的作用是向检测工具隐藏恶意进程，不会通过加密来勒索。逻辑炸弹是在特定条件或日期触发破坏性代码，其特征不是勒索。备份和离线恢复是减轻勒索软件影响的主要手段。

17. B 借口（pretexting）是编造一个可信的情境或虚假身份，这里是高管紧急被锁定，来操纵目标绕过正常的验证程序。尾随是实际跟在有权限的人身后通过上锁的门，这里没有发生。肩窥是用眼睛观察别人输入凭证，不是电话借口。翻垃圾是从丢弃物中翻找敏感资料，与这种通过电话进行的社会工程无关。

18. C 撞库是把已知的、之前泄露的用户名和密码组合拿去试多个不相关的服务，利用的是密码重复使用，与题中的攻击相符。密码喷洒则是用一个或几个常见密码去试很多用户名，以避免账户锁定，不使用已知有效的组合。暴力破解是系统地猜测各种密码组合，而不是重用泄露的凭证组合。字典攻击使用的是可能密码的词表，不是此前已确认有效的凭证组合。

19. D 勒索软件会加密受害者的文件并更改扩展名，然后显示勒索字条，要求付款（通常是加密货币）来换取解密密钥，与本题完全吻合。蠕虫不对，因为蠕虫是在网络中自我传播，本身并不加密文件或索要付款。Rootkit 不对，因为它的目标是隐蔽驻留和提升权限，不是加密文件。逻辑炸弹不对，因为它是在满足条件或到达日期时触发破坏性载荷，没有题中的勒索环节。

20. A 语音钓鱼是通过电话进行的语音形式的钓鱼，这里攻击者用一通实时电话说服员工说出敏感的一次性验证码，是典型的实时绕过 MFA 的手法。短信钓鱼不对，因为它指的是通过短信进行的钓鱼，不是电话。肩窥不对，因为它是从别人肩后用眼睛观察敏感信息，不是用言语套取。尾随不对，因为它指的是实际跟人进入受限区域，与本题无关。

21. C 水坑攻击（watering hole attack）是通过入侵某个特定群体常去的正规网站来攻击这个群体，然后只向目标受害者有条件地提供恶意内容，与本题完全吻合。误植域名（typosquatting）不对，因为它是注册拼写错误的域名来捕获输错网址的人，不是入侵一个常访问的正规网站。跨站脚本不对，因为它可能是所用的手段，但描述的是注入技术本身，不是题中所述的整体定向攻击策略。DNS 投毒不对，因为它篡改的是 DNS 解析记录，不是把条件载荷直接放在被入侵的正规网站上。

22. C 空闲时 CPU 持续高占用并明显发热，是加密挖矿恶意软件的典型迹象：它悄悄占用处理能力，为攻击者挖加密货币。防火墙规则变更会阻止或改变网络流量，不会让 CPU 飙高。SIEM 日志丢失与日志被篡改或日志服务中断有关，不是资源耗尽。非周期日志记录指日志条目的时间出乎意料，不是硬件性能症状，所以解释不了题中的现象。

23. A 网址嫁接（pharming）通过 DNS 层面的操纵，即使用户输入了正确的网址也会把他们引到恶意网站，这使它有别于误植域名，后者要靠用户输错域名才会被重定向。借口是基于编造情境或虚假身份的社会工程手法，不涉及 DNS 操纵。语音钓鱼是通过电话进行的语音钓鱼。因为题中明确说的是入侵 DNS 解析器，而不是用户出错或语音联系，所以网址嫁接才是准确的术语。

24. D 国家级高级持续性威胁（APT）组织拥有大量资金、定制的零日工具，以及长期隐蔽行动的耐心，目的是获取战略性的经济或政治利益，与这里八个月的潜伏期和有针对性的数据窃取相符。脚本小子没有开发零日漏洞的能力。黑客行动主义者通常是为了某个主张公开制造破坏或披露信息，不是悄悄长期窃取。无意的内部威胁是意外暴露，不是蓄意使用定制漏洞并躲避检测。

25. D 商业电子邮件入侵（BEC）是一种有针对性的攻击，利用被伪造或被入侵的高管邮箱账户，骗员工转账或提供敏感数据，与本题完全吻合，而且不需要恶意软件载荷。误植域名靠注册拼写错误的域名诱骗用户访问假网站，不是伪造的内部邮件。水坑攻击是入侵目标常访问的网站，与本题无关。撞库是用被盗的用户名和密码组合登录账户，不是通过社会工程骗人汇款。

26. D 内部威胁是指现任或前任员工滥用合法的访问权限或对内部系统的了解来造成伤害，符合本题中被解雇的管理员使用仍然有效的凭证的情形。黑客行动主义者不对，因为这类行为者出于政治或社会主张，而不是利用内部权限进行个人报复。国家级行为者不对，因为它涉及政府支持、资源多得多、带有战略意图的行动。脚本小子不对，因为这类行为者技术水平低，用现成工具，而不是利用合法的内部权限。

27. A 撞库是把先前不相关的数据泄露中被盗的用户名和密码组合拿到其他网站上试，利用的是密码重复使用，与本题完全吻合。暴力破解不对，因为它是系统地猜测未知的密码组合，而不是重放已知有效的凭证。密码喷洒不对，因为它是用少量常见密码去试很多账户，而不是已知的确切凭证组合。彩虹表攻击不对，因为它是离线还原密码哈希的技术，不是用泄露的明文凭证进行在线登录。

28. C 借口（pretexting）是编造虚假情境或身份，比如冒充审计员，来建立虚假的信任，操纵受害者披露敏感信息，与本题所述完全一致。诱饵不对，因为它是用有吸引力的实物或数字物品（如贴了标签的 U 盘）引诱受害者，而不是虚构身份。尾随不对，因为它是实际跟在有权限的人后面进入安全区域。等价交换不对，因为它是提供某项服务或好处来换取信息，本题中没有这一点。

29. B 风险容忍度定义的是针对某个具体、可衡量的风险指标所能接受的偏差程度，这里就是每年 5% 的中断概率阈值。风险偏好是更宏观、战略层面的表述，说明组织为实现目标愿意承担多大风险，不是一个具体的数值界限。风险登记册是列出已识别风险的记录工具，不是关于可接受阈值的政策表述。风险例外是针对某个具体情形、经正式批准的偏离政策，不是一个长期通用的阈值。

30. D 数据处理者仅代表数据控制者、并按其指示处理个人数据，而控制者决定处理的目的和方式，这里就是欧洲零售商。零售商才是控制者，不是 SaaS 公司。数据主体是个人数据所属的那个人，不是服务提供商。数据保护官是 GDPR 第 37 条对某些组织要求设立的内部或外聘监督角色，不是按他方指示处理数据的实体。

31. B 欧盟《通用数据保护条例》（GDPR）在第 17 条赋予数据主体被遗忘权（删除权），允许个人在特定条件下要求删除其个人数据。HIPAA 规范美国医疗行业的受保护健康信息，并不赋予这种范围的通用删除权。PCI DSS 是支付卡行业保护持卡人数据的标准，不是数据主体权利的框架。SOX 规范上市公司财务报告的准确性，与个人数据删除请求无关。

32. A 购买网络保险来抵补无法完全修复的风险所带来的经济损失，是风险转移的典型定义，即把财务影响转给第三方（保险公司）。风险缓解是增加技术或流程控制来降低可能性或影响，这里没有。风险规避是彻底取消有风险的活动，比如停用这套老系统，而公司并没有这样做。风险接受是不采取补偿措施地容忍风险，而这里公司是通过保单主动转移经济风险。

33. B SOC 2 Type II 评估控制在较长时期（通常 6 到 12 个月）内的运行有效性，正好满足客户对历史保证的需求，而不是只看某个时间点的快照。SOC 2 Type I 只评估某个时间点的控制设计，不能确认控制持续有效。SOC 1 关注与财务报告相关的控制，不涉及一般的安全、可用性或保密性原则。PCI DSS 合规证明只证明支付卡方面的合规，不涉及更广泛的长期安全运营。

34. D SOC 2 Type II 报告专门评估控制在规定的观察期（通常是六到十二个月）内是否有效运行，符合本题的要求。SOC 2 Type I 只评估控制在某个时间点的设计是否适当，不测试一段时期内的运行有效性。SOC 1 报告涉及服务机构对客户财务报表的影响所相关的控制，不涉及安全运营。ISO 27001 认证确认的是审核当日符合标准，它是一种认证，而不是对一段持续时期的鉴证。

35. B 审计权条款赋予组织合同上的权力，可以主动检查供应商的安全控制和合规证据，不需要事先征得供应商同意来安排时间，这对持续的第三方风险监督至关重要。保密协议只限制共享信息的披露。不可抗力条款针对双方都无法控制的事件（如自然灾害）下的责任。赔偿条款分配损失的经济责任，但不赋予审计访问权。

36. A 成熟的变更管理框架都有明确的紧急变更程序，允许在标准周期之外加快审查和审批，在紧迫性和问责之间取得平衡。即使时间紧迫，完全绕过审批也会破坏变更控制和审计记录。等待正常的 CAB 周期会让系统继续暴露在被利用的风险中，也无视了专为这种情况设立的紧急条款。通知用户是下游步骤，发生在变更经过正当渠道获批之后，而不是之前。

37. D 外部审计由组织之外的独立第三方进行，向监管机构、股东和其他利益相关方提供客观保证，符合聘请外部会计师事务所这一情形。内部审计由组织自己的审计部门进行，主要服务于内部管理层，而不是外部方。合规自评是没有独立核实的非正式内部审查。漏洞评估是找出技术系统的弱点，而不是评估财务控制的合规性。

38. A SOC 2 Type II 报告由独立审计师出具，评估供应商的控制在较长时期（通常六到十二个月）内的运行有效性，正好满足对持续保证的要求。自我声明问卷依赖供应商自己未经核实的说法，缺乏独立验证。渗透测试摘要评估的是某个时间点的技术可利用性，不评估信任服务准则下更广泛的控制环境。业务影响分析是内部规划文件，与外部供应商保证无关。

39. C 当可能性和影响都很低、控制成本超过潜在损失时，适合风险接受；管理层正式确认该风险，不再采取进一步行动。风险规避是完全取消相关活动，在风险敞口这么低的情况下没有必要。风险转移是把财务影响转给第三方，如保险，但这里风险敞口很低，接受才是最合适的应对。风险缓解是增加控制来降低可能性或影响，而题中说这不划算。

40. B 法律保全要求组织暂停正常的保留和销毁计划，保存可能与诉讼相关的记录，防止证据被毁（spoliation）。在保全期间删除数据是违法的，可能受到处罚。加密记录但继续按正常计划销毁，没有满足保存数据本身这一核心要求。记录的保管权仍在组织手中，而不是对方律师，这样才能在整个法律程序中保持站得住脚的保管链。

41. A 残余风险正是在 MFA 和分段等缓解控制措施实施之后剩下的风险，本题中就是仍然存在的会话令牌被窃取的可能。固有风险描述的是没有任何控制措施时的暴露程度，而不是 MFA 和分段已经到位之后的情形。次生风险指新控制措施本身引入了另一个新问题，例如 MFA 疲劳攻击，而不是原风险中未被解决的部分。控制风险指控制措施没有按预期发挥作用，不是控制措施本来就没打算堵住的缺口。

42. B SOC 2 Type II 报告证明控制在较长审查期（通常六到十二个月）内的运行有效性，而 SOC 2 Type I 只确认控制在某个具体时间点设计得当。SOC 1 报告涉及与财务报告相关的控制，不是信息安全。ISO 27001 证书确认组织维持着一套经认证的信息安全管理体系，但它本身并不像 SOC 2 Type II 那样提供对运行有效性的限定期间审计。

43. A 私有云提供专供单一组织使用的基础设施，无论部署在本地还是由第三方托管，该组织都拥有独占的控制权，并与其他租户隔离。公有云是通过互联网在许多客户之间共享基础设施。社区云由有共同关注点（如合规要求）的若干组织共享，不是单个公司。混合云是组合两种或更多部署模式，与题中独占、单租户的描述相矛盾。

44. B 虚拟局域网（VLAN）在第 2 层按逻辑划分广播域，管理员可以在同一套物理交换结构上隔离各个部门，它们之间的流量必须经过路由，因此可以被控制或阻止。VPN 是在互联网等不受信任的网络上保护流量，不是内部分段。NAT 为路由而转换 IP 地址，不是访问控制。负载均衡器在服务器之间分配流量，不会创建隔离的网络段。

45. C 证书错误说明客户端无法建立回溯到受信任根的信任链，也就是说信任库里缺少根 CA 证书；没有它，即使服务器证书本身有效，浏览器也无法验证签发链。私钥从不离开服务器，与客户端信任库无关。会话票据是 TLS 恢复会话用的，与 PKI 信任无关。对称会话密钥是在建立信任之后才协商的，不影响这个信任错误。

46. A 密码学哈希根据文件内容生成唯一的定长值，哪怕只改动一个比特，哈希值也会完全不同，所以与供应商公布的值一致，就能确认完整性。文件大小即使内容已损坏，也可能碰巧相同。对二进制的 ISO 数据做目视检查不现实，也发现不了细微的损坏。加密再解密测试的是密码运算，不是原始字节在加密前有没有被改动。

47. C DHE（及其椭圆曲线版本 ECDHE）在每次握手时生成全新的、仅限本次会话的密钥对，之后丢弃临时私钥，所以日后即使服务器的静态证书密钥被泄露，也无法解密之前截获的会话，这就是完美前向保密。静态 RSA 密钥交换用服务器的长期公钥加密预主密钥，所以一旦取得该私钥，就能追溯解密过去截获的所有会话。不带临时 Diffie-Hellman 的纯 PSK 交换会重复使用同一个共享密钥，没有前向保密。Kerberos 票据交换是认证协议，不是 TLS 密钥交换机制。

48. A 轻量级密码学专为以极小的计算开销、耗电和内存占用提供足够的安全性而设计，这对受限的嵌入式和物联网设备至关重要。不顾资源而选最强的算法，可能耗尽电池并导致性能故障。抗量子算法通常需要更大的密钥和更多的处理，受限设备目前负担不起。DES 已被弃用，在密码学上已被攻破，不管效率如何，安全性都不够。

49. B 气隙（air gap）是把系统或网络做物理隔离，与任何其他网络都没有有线或无线连接，因此针对该网段的远程网络攻击不可能发生。屏蔽子网仍然通过防火墙保持受控的网络连接，与真正的气隙不同。零信任是要求持续验证每个连接的访问理念，不是物理隔离。微分段是在已连接的网络内创建精细的逻辑区域，与完全没有连接正好相反。

50. D 微分段应用精细的、工作负载级别的防火墙策略，可以放行两台虚拟机之间确实需要的东西向流量，同时阻止未授权的横向移动，即使两台机器在同一个 VLAN 和子网中。为每台虚拟机新建 VLAN 会破坏同一子网的要求，而且难以扩展。混杂模式的 IDS 只检测流量，不阻止。端口安全控制的是物理交换机端口上的 MAC 地址，无法限制同一网段内两台虚拟机之间的应用层通信。

51. C 带自动故障切换的主备（active-passive）负载均衡会让一台备用服务器随时待命，主服务器故障时接管，以最小的中断支持高可用性。主主（active-active）配置是把流量分配给多台活动服务器。全盘加密保护的是保密性，不是可用性。带手动重启的单一接入点会造成停机，并形成单点故障。关机状态的气隙备份服务器无法自动切换，故障期间会发生中断。

52. B 数字签名使用签署者的私钥，所以只有该供应商才能生成这个签名；用供应商的公钥验证它，就能证明来源，并防止供应商否认是自己签的，这就是不可否认性。对称加密保护保密性，不能证明来源，而且依赖双方都可能使用的共享密钥。负载均衡解决的是正常运行时间，不是作者身份。仅靠哈希只能验证完整性，不能验证身份，因为谁都能计算哈希。

53. B 气隙把网络与所有其他网络（包括互联网和企业 IT）做物理和逻辑隔离，消除了远程攻击路径，这是关键 SCADA/ICS 环境常用的控制，因为这些环境更看重可用性和安全而不是连通性。屏蔽子网仍允许通过防火墙进行受控的对外连接。跳板机提供受控的访问点，但意味着存在连接。VPN 建立加密隧道，与隔离正好相反。

54. C 默认凭证加上与敏感的财务系统处在同一个扁平网络中，是被入侵和横向移动的最大即时风险；更改凭证并把物联网设备放入自己的 VLAN，能同时堵住认证缺口和网络暴露。提高固件更新频率是好习惯，但解决不了眼前的凭证和分段风险。在财务工作站上禁用 SNMP 修复不了物联网设备的漏洞。地理围栏与这个基于网络的风险无关。

55. A OCSP 装订由 Web 服务器定期向 CA 查询，并把带签名和时间戳的 OCSP 响应直接附在 TLS 握手中，客户端不需要联系 CA，既避免了向 CA 泄露客户端访问了哪些网站的隐私问题，也省去了额外的往返延迟。标准 OCSP 要求客户端实时查询 CA，会泄露浏览模式并增加延迟。CRL 体积大、更新不频繁，而且仍需要客户端自己去获取。证书固定管的是信任哪张证书，不是怎样传递吊销状态。

56. B 第 1 层（基本控制）是 PLC、RTU 和其他执行实时控制逻辑、并直接与第 0 层设备通信的控制器所在的位置。第 0 层是物理过程本身，即传感器、阀门和电机，而不是驱动它们的控制器。第 2 层负责区域监督功能，如 HMI 和汇总多个第 1 层控制器的 SCADA 监督软件。第 3 层负责全站范围的运营管理，如生产调度，比控制器本身离实时控制更远一层。

57. C 回滚计划规定了把系统恢复到上一个已知良好状态的具体步骤，直接决定中断发生后服务能多快恢复。影响分析说明谁会受影响，但没有给出恢复程序。批准签字是确认已获授权的治理形式，不是技术上的恢复手段。沙箱测试能事先降低失败的可能，但变更已经造成生产中断之后，它帮不上忙。

58. D 检测性控制在安全事件发生时或发生后识别并告警，移动感应报警器正是如此，在发生未经授权的移动时通知安保人员。预防性控制是一开始就阻止进入，如上锁的门或刷卡器。纠正性控制是在事件发生后恢复或修复系统，不只是告警。威慑性控制是让攻击者不敢尝试，如显眼的警示标志，而不是检测已经在进行的行为。

59. B 冗余电源、RAID 10 和故障切换集群都是消除单点故障，使系统在硬件故障时仍可访问，这正是可用性的定义。保密性不对，因为这些控制都不限制谁能查看数据。完整性不对，因为这些措施不验证数据是否被改动。不可否认性不对，因为它不是 CIA 三要素之一，涉及的是行为的证明，而不是正常运行时间，通常通过数字签名和日志来实现。

60. A 职责分离把关键任务分给多人，使任何一个人都无法独自完成整个高风险流程，从而减少舞弊和出错的机会。最小权限把用户的访问限制在其角色所需的范围内，但并不专门针对把一个流程分给两个人。岗位轮换是定期让员工换岗，以便日后暴露舞弊，不是拆分一笔交易。强制休假是让员工休假，以便别人检查他的工作，是检测性措施，而不是对职责的结构性拆分。

61. D 授权发生在身份验证之后，定义授予用户的具体权限或访问权利，通常通过基于角色的访问控制（RBAC）来实施。身份验证不对，因为它只通过凭证确认用户声称的身份。记账（accounting）不对，因为它是记录和跟踪用户活动以供审计，不做权限决定。身份标识不对，因为它只是最初的身份声明（如输入用户名），此时还没有任何验证。

62. A 零信任的原则是“永不信任，始终验证”，要求对每个访问请求持续进行认证和授权，不论它来自传统网络边界之内还是之外。基于边界的防御不对，因为用户一旦进入网络边界，它就默认信任，做法正好相反。纵深防御不对，因为它描述的是叠加多层控制，而不是一种具体的信任模型。基于角色的访问控制不对，因为它是零信任中使用的一种授权方法，而不是总体模型本身。

63. D 篡改传输中的数据属于对信息的未授权修改，这是完整性被破坏的定义。如果攻击者只是查看或窃取数据而没有改动，那才是保密性问题。可用性涉及拒绝访问或服务；交易仍然被处理了，只是数据被破坏，所以主要影响不是可用性。不可否认性不是 CIA 三个要素之一，它是相关的问责概念，指无法否认某项行为，虽然与这次攻击的取证有关，但这里直接被破坏的原则是数据完整性。

64. C 这描述的是变更咨询委员会（CAB），它的主要职责是在批准或否决拟议变更之前，评估其风险、影响和回滚计划，减少计划外的中断。进行技术安装不对，因为这属于系统管理员的任务，而不是审查委员会的。编写事件响应计划不对，因为那属于 IR 规划，是另一项治理职能。进行意识培训不对，因为那是与变更控制无关的运营安全控制。

65. D 有文档记录、并针对变更窗口测试过的回滚计划，在实施之前就会被评估，专为在变更失败时迅速恢复到先前已知良好的状态而设计，从而把停机降到最低。涵盖整个数据中心的修订版业务连续性计划有助于中断期间的连续性，但对撤销这次具体的防火墙变更不那么直接。资产清单有助于在变更请求中找出受影响的系统，但本身不能减轻变更失败的影响。事后事件报告模板是中断发生之后才用的被动文件，对故障本身起不到缓解作用。

66. A 哈希碰撞让攻击者可以用一个产生相同摘要的恶意文件替换合法文件，使哈希失去证明文件未被改动的作用，这正是完整性的定义。保密性涉及数据的未授权披露，碰撞不会影响它。可用性涉及系统的正常运行时间和可访问性，不是文件是否可信。授权管的是已认证的主体被允许做什么，与验证文件内容是否与原始状态一致无关。

67. A 策略引擎是策略决策点中的核心决策组件；它依据身份、设备合规性和威胁情报等输入运行信任算法，并输出允许或拒绝的决定。策略执行点是根据该决定建立或终止连接的把关者，但自己并不做决定。策略管理器生成会话凭证，把策略引擎的决定传达给执行点，但不独立评估信任算法。CDM 系统只是提供设备状况数据，作为输入之一交给策略引擎，本身不是决策者。

68. A ABAC 评估主体、资源和环境的多个动态属性（部门、文件分级、时间、设备合规性），生成实时的访问决策，是零信任架构的基础。RBAC 只考虑用户被分配的工作角色，缺乏题中所述的情境粒度。DAC 由资源所有者自行设置权限，没有评估多个环境属性的内置机制。MAC 使用管理员集中设定的固定分级标签和许可，不会动态考虑设备合规性或时间。

69. C 最小权限把用户的访问权限限制在完成其工作职能所需的最低限度，这与把技术人员限制在部门工作站、而不是整个域的完整权限相符。职责分离是把一项任务分给多人，不是限定一个人的访问级别。纵深防御是在系统中叠加多层独立的安全控制，不是为单个账户划定访问范围。零信任是要求对每个请求持续验证的更大的架构模型，与单纯减少授予的权限是不同的概念。

70. B 不可否认性使用与私钥绑定的数字签名等密码学机制来证明某项行为的来源，防止签署者日后否认自己参与。保密性不对，因为这个场景不涉及对未授权方隐瞒这笔转账。完整性不对，因为它只确保消息没有被改动，不能证明发送者要负责。身份验证是核实身份或消息来源，但不可否认性最具体地针对防止否认已签署的行为。

英文关键词

CIA triad	CIA 三要素	保密性、完整性、可用性，安全的三个目标。
authentication	身份验证、认证	核实用户的身份是否属实。
authorization	授权	决定通过认证的用户能做什么。
accounting	记账、审计	记录用户做过什么，AAA 的第三个 A。
non-repudiation	不可否认性、抗抵赖性	让人无法否认自己发送或签署过。
zero trust	零信任	默认不信任任何用户或设备，每次访问都验证。
least privilege	最小权限	只给完成工作所需的权限。
compensating control	补偿性控制	主要控制用不了时的替代办法。
change management	变更管理	系统改动的审批、测试和记录流程。
multifactor authentication (MFA)	多因素认证	用两种或更多不同类型的凭证登录。
threat actor	威胁行为者	发起或企图发起攻击的人或组织。
insider threat	内部威胁	来自内部人员或有内部权限的人的威胁。
attack surface	攻击面	攻击者可能进入的所有位置。
zero-day vulnerability	零日漏洞	厂商还没有补丁的漏洞。

social engineering	社会工程	通过欺骗人来获取信息或权限。
phishing	网络钓鱼	用假消息骗取凭证或诱导点击。
business email compromise (BEC)	商业电子邮件入侵	伪造或控制高管邮箱，骗取汇款或数据。
typosquatting	误植域名、仿冒域名	注册拼写相近的域名来骗人。
ransomware	勒索软件	加密数据并索要赎金的恶意软件。
indicator of compromise (IoC)	失陷指标	表明系统可能已被入侵的迹象。
mitigation	缓解措施	降低风险或减轻影响的做法。
hardening	系统加固	关掉不需要的服务，改掉不安全的设置。
SIEM (security information and event management)	安全信息与事件管理	汇总并关联多个来源的日志。
SOAR (security orchestration, automation, and response)	安全编排、自动化与响应	自动执行事件响应流程。
EDR (endpoint detection and response)	端点检测与响应	监视端点，可以隔离一台设备。
DLP (data loss prevention)	数据防泄漏	发现并阻止敏感数据外泄。
IDS / IPS (intrusion detection / prevention system)	入侵检测系统 / 入侵防御系统	IDS 发出警报，IPS 还能拦截。
incident response	事件响应	处理安全事件并恢复的流程。
containment	遏制	限制事件范围，防止扩散。
chain of custody	证据保管链	记录证据由谁、何时、为何经手。
false positive	误报、假阳性	发出警报，但实际没有问题。
encryption	加密	把数据变成没有密钥就读不懂的形式。
hashing	哈希、散列	生成数据的指纹，用来检查完整性。
digital signature	数字签名	证明签署者身份，且内容没有改动。
public key infrastructure (PKI)	公钥基础设施	签发、管理和吊销数字证书的体系。
CRL / OCSP (certificate revocation list / Online Certificate Status Protocol)	证书吊销列表 / 在线证书状态协议	CRL 是吊销名单，OCSP 查单张证书状态。
segmentation	网络分段	把网络分成多段，限制攻击者横向移动。
RPO (recovery point objective)	恢复点目标	最多能丢多少数据，用时间表示。
RTO (recovery time objective)	恢复时间目标	系统要在多久内恢复运行。
risk register	风险登记册	列出每项风险、负责人和应对办法的文件。
air gap	气隙	与所有其他网络物理隔离，没有任何连接。

least functionality	最少功能	系统只运行必需的服务、协议和账户。
order of volatility	易失性顺序	按消失快慢决定先收集哪种证据。
legal hold	法律保全	为诉讼要求暂停销毁相关记录的通知。
pretexting	借口式欺骗	编造情境或身份，骗对方绕过验证。
credential stuffing	撞库	用已泄露的账号密码组合去试其他网站。
risk appetite	风险偏好	组织愿意承担多大风险的整体态度。
risk tolerance	风险容忍度	针对具体指标可接受的偏差程度。
SOC 2 Type II report	SOC 2 Type II 报告	证明控制在一段时期内有效运行的审计报告。
microsegmentation	微分段	按工作负载划分细小区域，限制横向移动。

Examundo 是独立网站，与主办这些考试的机构没有隶属关系，也未获其认可。题目均为原创，不是考试真题。
examundo.tech/zh/comptia-security-plus/