下列哪项不属于信息安全保障体系的纵深防御策略核心要素？

A.人员培训机制

B.区域边界防护

C.支撑性基础设施

D.网络流量监测

答案：D 解析：网络流量监测属于检测手段，不属于纵深防御核心要素（核心包括人员、边界、基础设施等）。

在P2DR动态安全模型中，决定防护时间的核心因素是：

A.漏洞扫描频率

B.入侵检测系统响应速度

C.防火墙规则更新周期

D.安全策略执行效率

答案：D 解析：P2DR 模型中，安全策略执行效率直接影响防护时间有效性。

下列加密算法中基于椭圆曲线离散对数难题的是：

A.RSA

B.ECC

C.AES

D.SHA-256

答案：B 解析：ECC（椭圆曲线加密）基于椭圆曲线离散对数难题。

某企业部署了基于角色的访问控制（RBAC），当员工岗位变动时，系统管理员应优先执行的操作是：

A.删除原有用户账号

B.修改用户所属角色

C.重置用户登录密码

D.审计用户历史操作

答案：B 解析：RBAC 中岗位变动应优先调整用户角色关联。

下列哪种攻击类型属于网络层DDoS攻击？

A.SQL注入

B.SYN Flood

C.XSS跨站脚本

D.CSRF请求伪造

答案：B 解析：SYN Flood 通过耗尽 TCP 连接资源实施 DDoS 攻击。

在Windows系统中防范UAF漏洞最有效的防护机制是：

A.DEP数据执行保护

B.杀毒软件实时监控

C.防火墙入站规则

D.用户账户控制(UAC)

答案：A 解析：DEP 通过阻止恶意代码在内存执行防御 UAF 漏洞。

数字证书中不包含的字段是：

A.证书持有者公钥

B.证书有效期

C.颁发机构私钥

D.数字签名算法

答案：C 解析：数字证书不包含颁发机构私钥（仅含公钥和签名信息）。

下列哪项技术可有效防御ARP欺骗攻击？

A.IP与MAC地址静态绑定

B.HTTPS协议加密

C.网络端口隐藏

D.流量镜像分析

答案：A 解析：静态绑定 IP 和 MAC 可防止 ARP 欺骗伪造地址。

根据《网络安全法》，关键信息基础设施运营者应当至少多久进行一次网络安全检测评估？

A.每月

B.每季度

C.每半年

D.每年

答案：D 解析：《网络安全法》规定关键设施每年至少一次检测评估。

在Linux系统中用于查看当前系统开放端口的命令是：

A.netstat -tuln

B.ifconfig -a

C.ps -aux

D.chmod 755

答案：A 解析：netstat -tuln 显示监听状态的 TCP/UDP 端口。

下列哪种安全模型采用"不上读、不下写"的访问控制原则？

A.BLP机密性模型

B.Biba完整性模型

C.Clark-Wilson模型

D.RBAC模型

答案：B 解析：Biba 模型基于“不上读、不下写”保护数据完整性。

在渗透测试过程中，用于识别Web应用隐藏目录的最佳工具是：

A.Nmap

B.DirBuster

C.Wireshark

D.Metasploit

答案：B 解析：DirBuster 通过字典爆破扫描 Web 隐藏目录。

我国信息安全等级保护第三级系统要求审计记录保存时间不得少于：

A.3个月

B.6个月

C.1年

D.3年

答案：B 解析：等保三级要求审计记录保存至少 6 个月。

下列哪项不属于软件安全开发生命周期（SDL）的核心阶段？

A.威胁建模

B.模糊测试

C.用户界面设计

D.安全编码规范

答案：C 解析：用户界面设计属于功能需求，非 SDL 安全阶段。

在PKI体系中，负责证书吊销列表（CRL）签发的是：

A.注册机构RA

B.证书颁发机构CA

C.目录服务LDAP

D.时间戳服务器TSA

答案：B 解析：CA 负责签发证书及 CRL（证书吊销列表）。

下列哪种协议通过封装HTTP流量实现VPN功能？

A.PPTP

B.L2TP

C.SSL/TLS

D.IPsec

答案：C 解析：SSL/TLS 协议通过封装 HTTP 实现 HTTPS 及 VPN。

在数据库安全管理中，防止SQL注入攻击最有效的措施是：

A.部署Web应用防火墙

B.使用参数化查询

C.限制数据库连接数

D.启用SSL加密传输

答案：B 解析：参数化查询预编译 SQL 语句，直接防御注入。

根据TCSEC标准，Windows NT系统属于哪个安全级别？

A.C1

B.C2

C.B1

D.B2

答案：B 解析：TCSEC 标准中 Windows NT 符合 C2 级（自主访问控制）。

在网络安全审计中，能够检测0day攻击的有效方法是：

A.特征码匹配

B.行为异常分析

C.日志完整性校验

D.协议合规检查

答案：B 解析：行为异常分析可检测未知攻击模式（如 0day）。

下列哪项技术通过修改内存地址空间布局防御缓冲区溢出？

A.DEP

B.ASLR

C.SEHOP

D.StackGuard

答案：B 解析：ASLR 通过随机化内存地址布局防御溢出攻击。

我国《密码法》规定用于保护不属于国家秘密信息的商用密码实行：

A.强制备案管理

B.分级分类管理

C.行政许可审批

D.自主研发管控

答案：B 解析：《密码法》规定商用密码实行分级分类管理。

在信息安全风险评估中，残余风险的计算公式是：

A.固有风险 × 控制有效性

B.潜在损失 ÷ 防护措施

C.威胁可能性 × 脆弱性影响

D.资产价值 × 暴露系数

答案：A 解析：残余风险=固有风险×控制有效性剩余部分。

下列哪种文件系统支持强制访问控制（MAC）？

A.FAT32

B.NTFS

C.ext4

D.SELinux

答案：D 解析：SELinux 支持强制访问控制（MAC）。

在无线网络安全中，WPA2协议使用的加密算法是：

A.RC4

B.TKIP

C.CCMP

D.DES

答案：C 解析：WPA2 使用 CCMP（AES 加密）替代 TKIP。

某公司发生数据泄露事件，根据应急预案首先应采取的措施是：

A.断开网络连接

B.备份系统日志

C.联系公关部门

D.报警立案侦查

答案：A 解析：数据泄露后立即断网可遏制进一步扩散。

下列哪项技术可有效防御跨站脚本攻击（XSS）？

A.输入内容过滤

B.HTTPS强制跳转

C.会话令牌加密

D.防火墙ACL规则

答案：A 解析：过滤用户输入内容可消除 XSS 攻击载体。

在数字取证过程中，对原始存储介质进行只读操作的主要目的是：

A.提高取证效率

B.保持证据完整性

C.避免病毒感染

D.节省存储空间

答案：B 解析：只读操作确保取证过程不破坏原始证据。

根据ISO/IEC 27001标准，信息安全管理体系（ISMS）建立的首要步骤是：

A.风险评估

B.制定安全策略

C.选择控制措施

D.管理评审

答案：B 解析：ISO 27001 要求首先制定安全策略明确目标。

下列哪种认证方式属于双因素认证？

A.指纹+虹膜识别

B.密码+短信验证码

C.门禁卡+电子签名

D.USB Key+PIN码

答案：B 解析：密码（知识）+验证码（持有物）为双因素。

在Linux系统中，用于查看进程打开文件的命令是：

A.lsof

B.top

C.netstat

D.ps

答案：A 解析：lsof 命令列出进程打开的文件及网络连接。

下列哪项协议通过三次握手建立TCP连接？

A.SYN→SYN/ACK→ACK

B.SYN→ACK→SYN/ACK

C.SYN→RST→ACK

D.SYN→FIN→ACK

答案：A 解析：TCP 三次握手流程：SYN→SYN/ACK→ACK。

在安全开发生命周期中，威胁建模阶段的主要产出物是：

A.攻击树分析报告

B.代码审计记录

C.渗透测试方案

D.用户需求文档

答案：A 解析：威胁建模阶段通过攻击树分析识别潜在风险。

下列哪种备份策略能最大限度减少数据恢复时间？

A.完全备份

B.增量备份

C.差异备份

D.镜像备份

答案：D 解析：镜像备份直接复制全盘数据，恢复最快。

根据《网络安全审查办法》，关键信息基础设施运营者采购网络产品和服务应当预判的风险不包括：

A.供应链中断风险

B.产品服务价格波动

C.数据泄露风险

D.关键信息被非法控制

答案：B 解析：价格波动属市场风险，不属安全审查范围。

在密码学中，能够同时实现机密性和完整性的技术组合是：

A.AES加密 + MD5哈希

B.RSA加密 + SHA-1签名

C.3DES加密 + HMAC认证

D.ECC加密 + CRC校验

答案：C 解析：3DES 加密保证机密性，HMAC 认证完整性。

下列哪项不属于网络安全应急响应的核心环节？

A.事件检测

B.影响评估

C.证据销毁

D.系统恢复

答案：C 解析：证据销毁会破坏取证链，非应急响应环节。

在虚拟化安全中，Hypervisor层面临的主要威胁是：

A.虚拟机逃逸

B.拒绝服务攻击

C.ARP欺骗

D.DNS劫持

答案：A 解析：虚拟机逃逸攻击可突破 Hypervisor 隔离。

我国网络安全等级保护2.0标准中，安全通信网络要求的控制点不包括：

A.网络架构优化

B.通信传输加密

C.网络设备冗余

D.网络流量清洗

答案：D 解析：流量清洗属于防护措施，非通信网络架构要求。

下列哪种攻击利用TCP会话劫持技术？

A.中间人攻击

B.泪滴攻击

C.Land攻击

D.Smurf攻击

答案：A 解析：中间人攻击通过劫持 TCP 会话窃取数据。

在数字水印技术中，鲁棒性指的是：

A.水印不可见性

B.抗篡改能力

C.快速检测速度

D.低计算资源消耗

答案：B 解析：鲁棒性指水印在篡改后仍能被检测的特性。

某企业部署了SIEM系统，其核心功能是：

A.漏洞扫描

B.日志聚合分析

C.网络流量监控

D.入侵防御阻断

答案：B 解析：SIEM（安全信息与事件管理）核心是日志聚合分析。

下列哪种协议用于安全电子邮件传输？

A.S/MIME

B.FTPS

C.SNMPv3

D.SSH

答案：A 解析：S/MIME 协议用于加密和签名电子邮件。

在云计算安全中，CSA提出的"云安全控制矩阵"包含的领域数量是：

A.11

B.13

C.15

D.17

答案：B 解析：CSA 云安全控制矩阵涵盖 13 个安全领域。

根据《个人信息保护法》，处理敏感个人信息需要取得的同意形式是：

A.口头同意

B.书面同意

C.单独同意

D.默示同意

答案：C 解析：《个保法》要求处理敏感信息需用户单独同意。

在逆向工程中，用于分析二进制文件函数调用关系的工具是：

A.IDA Pro

B.Wireshark

C.Nmap

D.Burp Suite

答案：A 解析：IDA Pro 用于反汇编和逆向分析二进制文件。

下列哪种技术可有效防御APT攻击？

A.终端杀毒软件

B.沙箱检测

C.防火墙ACL

D.漏洞补丁管理

答案：B 解析：沙箱检测未知文件行为可识别 APT 攻击特征。

在区块链技术中，保证数据不可篡改的核心机制是：

A.共识算法

B.哈希链结构

C.智能合约

D.非对称加密

答案：B 解析：哈希链确保区块链数据前后关联不可篡改。

我国《数据安全法》规定的数据分类分级原则不包括：

A.重要性原则

B.行业属性原则

C.安全风险原则

D.地域管辖原则

答案：D 解析：数据分类分级原则不包含地域管辖因素。

在物联网安全中，解决设备身份认证问题的关键技术是：

A.数字证书

B.设备指纹

C.物理不可克隆函数

D.生物特征识别

答案：A 解析：数字证书为物联网设备提供身份认证机制。

根据零信任安全模型，访问控制的决定因素不包括：

A.用户身份

B.设备状态

C.网络位置

D.数据密级

答案：C 解析：零信任模型不信任网络位置，动态验证访问权限。

在SSL/TLS协议握手过程中，用于协商加密套件的报文是：

A.Client Hello

B.Server Hello

C.Certificate

D.Server Key Exchange

答案：B 解析：Server Hello 报文由服务器发送，包含最终选定的加密套件，用于与客户端协商通信参数。

某金融机构发现内部员工通过VPN非法导出客户数据，最应优先强化的控制措施是：

A.部署网络行为审计系统

B.实施动态双因素认证

C.启用DLP数据防泄露

D.升级入侵防御系统规则

答案：C 解析：DLP（数据防泄露）可直接监控和阻断敏感数据外传，优先防止数据泄露。

下列哪项技术可有效缓解DNS缓存投毒攻击？

A.启用DNSSEC扩展协议

B.部署HTTPS严格传输安全

C.配置SPF记录验证

D.使用DNS over TCP

答案：A 解析：DNSSEC 通过数字签名验证 DNS 记录完整性，防止伪造响应污染缓存。

在可信计算体系结构中，负责建立信任链的核心组件是：

A.TPM安全芯片

B.可信引导程序

C.可信操作系统

D.可信应用程序

答案：A 解析：TPM 安全芯片提供硬件级信任根，用于存储密钥及度量系统启动完整性。

某云服务商采用虚拟化逃逸防护技术，其主要防御目标是：

A.防止虚拟机间流量嗅探

B.阻断跨虚拟机侧信道攻击

C.隔离宿主机与虚拟机通信

D.检测虚拟机异常资源占用

答案：B 解析：虚拟化逃逸防护主要防止攻击者利用漏洞从虚拟机突破到宿主机。

根据《数据安全法》，处理重要数据的系统应当至少满足的等级保护级别是：

A.第二级

B.第三级

C.第四级

D.第五级

答案：B 解析：《数据安全法》规定重要数据处理系统需满足等保三级及以上要求。

下列哪种攻击通过篡改内存指针实现任意代码执行？

A.Return-OrientedProgramming

B.Heap Spray

C.Format String Exploit

D.Integer Overflow

答案：A 解析：ROP 攻击通过篡改返回地址链调用现有代码片段实现任意执行。

在Kerberos认证协议中，用于加密会话密钥的组件是：

A.用户密码哈希

B.TGS的长期密钥

C.KDC的主密钥

D.票据授予票据

答案：B 解析：TGS 使用其长期密钥加密会话密钥，确保客户端与服务的通信安全。

某企业部署了基于深度学习的恶意代码检测系统，其核心优势在于：

A.实时特征码更新

B.未知威胁行为识别

C.多引擎协同分析

D.沙箱动态行为解析

答案：B 解析：深度学习通过行为特征识别未知恶意代码，不依赖已知特征库。

下列哪项不属于工控系统特有的安全威胁？

A.协议脆弱性利用

B.固件逻辑炸弹

C.时序攻击

D.缓冲区溢出

答案：D 解析：缓冲区溢出是通用漏洞，非工控系统特有威胁。

在零信任架构中，实施持续信任评估的关键技术是：

A.微隔离策略

B.用户实体行为分析

C.软件定义边界

D.动态访问控制

答案：B 解析：UEBA 通过分析用户行为基线检测异常，支撑动态信任评估。

根据ISO 27001标准，信息安全风险处置的优先顺序应为：

A.规避→转移→缓解→接受

B.缓解→转移→规避→接受

C.规避→缓解→转移→接受

D.转移→规避→缓解→接受

答案：A 解析：风险处置优先级为规避→转移→缓解→接受，优先消除风险源。

某Web应用使用JWT令牌进行身份验证，防范重放攻击的最佳措施是：

A.缩短令牌有效期

B.绑定客户端IP地址

C.增加随机数nonce字段

D.启用令牌吊销列表

答案：C 解析：nonce 字段确保每个令牌唯一性，防止重复使用攻击。

下列哪类攻击可绕过传统WAF的规则检测？

A.基于语法的SQL注入

B.盲注时间延迟攻击

C.堆叠查询注入

D.联合查询注入

答案：B 解析：盲注攻击无显式错误回显，传统 WAF 基于规则难以检测。

在安全开发生命周期（SDL）中，威胁建模阶段的主要输出物是

：

A.攻击面分析报告

B.安全需求规格书

C.渗透测试用例集

D.代码审计缺陷清单

答案：A 解析：威胁建模阶段输出攻击面分析，识别潜在威胁路径及应对措施。

某APT组织使用Cobalt Strike进行横向移动时，最可能利用的协议是：

A.SMB

B.HTTP

C.DNS

D.ICMP

答案：A 解析：Cobalt Strike 常用 SMB 协议通过 PsExec 等工具进行横向移动。

根据密码行业标准，SM4算法的工作模式中提供认证加密功能的是：

A.ECB模式

B.CBC模式

C.GCM模式

D.OFB模式

答案：C 解析：GCM 模式结合加密与认证功能，提供完整性保护和机密性。

在区块链智能合约安全审计中，最应重点检查的漏洞类型是：

A.整数溢出漏洞

B.重入攻击漏洞

C.时间戳依赖漏洞

D.未初始化存储指针

答案：B 解析：重入漏洞允许函数未完成时重复调用，导致资产重复转移。

某企业遭遇勒索病毒攻击，应急响应团队应首先执行的操作是：

A.断开受感染主机网络

B.备份加密文件样本

C.追踪比特币支付地址

D.分析病毒行为特征

答案：A 解析：隔离感染主机阻止病毒扩散为应急响应首要任务。

下列哪种技术可有效防御基于GPU的密码暴力破解？

A.密钥延伸算法

B.盐值混淆机制

C.多因子认证

D.会话令牌刷新

答案：A 解析：密钥延伸算法增加计算复杂度，减缓 GPU 暴力破解速度。

在Windows域环境中，防范Pass-the-Hash攻击的最佳实践是：

A.启用Credential Guard

B.限制本地管理员权限

C.强制定期密码修改

D.部署NTLMv2协议

答案：A 解析：Credential Guard 隔离凭据存储，防止内存中哈希被窃取。

某物联网设备采用TLS 1.3协议通信，其握手过程最少需要交换的报文数量是：

A.2

B.3

C.4

D.5

答案：A 解析：TLS 1.3 优化握手流程，仅需 1-RTT 完成密钥交换。

根据等级保护2.0要求，三级系统应具备的日志审计功能不包括：

A.审计记录完整性保护

B.审计进程独立运行

C.实时告警阈值设置

D.审计日志异地备份

答案：D 解析：等级保护三级要求日志留存 6 个月，但未强制要求异地备份。

在可信计算中，远程证明协议的核心功能是：

A.验证平台配置完整性

B.协商会话加密密钥

C.颁发数字身份证书

D.同步可信时间戳

答案：A 解析：远程证明通过可信度量值验证平台配置是否符合预期策略。

某企业使用SAML实现单点登录，身份提供者（IdP）向服务提供者（SP）传递的主要凭证是：

A.数字签名断言

B.OAuth令牌

C.Kerberos票据

D.JWT令牌

答案：A 解析：SAML 使用数字签名断言传递认证信息至服务提供方。

下列哪项技术通过修改进程内存页属性实现反调试？

A.代码段CRC校验

B.异常处理链劫持

C.NtSetInformationProcess

D.内存断点检测

答案：C 解析：NtSetInformationProcess 可修改内存页属性干扰调试器操作。

在云安全责任共担模型中，属于客户责任范畴的是：

A.物理基础设施维护

B.虚拟机监控程序更新

C.操作系统补丁管理

D.网络边界防火墙配置

答案：C 解析：客户负责云上操作系统、应用及数据的安全配置与维护。

某金融系统采用同态加密处理交易数据，其主要解决的问题是：

A.数据存储机密性

B.计算过程隐私保护

C.数据传输完整性

D.用户身份匿名性

答案：B 解析：同态加密支持密文计算，确保数据处理过程隐私不被泄露。

下列哪类攻击利用TCP序列号预测实现会话劫持？

A.中间人攻击

B.盲攻击

C.重放攻击

D.反射攻击

答案：B 解析：盲攻击通过预测 TCP 序列号伪造数据包劫持会话。

在移动应用安全检测中，检测HTTPS证书锁定机制是否生效的最佳方法是：

A.动态污点分析

B.中间人代理测试

C.反编译代码审计

D.网络流量镜像

答案：C 解析：代码审计可检查证书锁定逻辑是否在客户端硬编码实现。

根据《关键信息基础设施安全保护条例》，运营者应当至少每几个月开展一次网络安全检测评估？

A.3

B.6

C.12

D.24

答案：C 解析：条例规定关键设施运营者每年至少进行一次安全检测评估。

某工控系统使用Modbus协议，为防范非法指令注入应优先配置：

A.协议白名单过滤

B.流量基线分析

C.深度包检测规则

D.网络地址转换

答案：A 解析：协议白名单仅允许预设合法指令，阻断异常指令注入。

在量子计算威胁背景下，属于抗量子密码算法的是：

A.RSA-4096

B.ECC-secp521r1

C.Kyber

D.AES-256

答案：C 解析：Kyber 为基于格的抗量子密码算法，可抵御量子计算攻击。

某企业部署了全流量分析系统，能够有效识别的攻击特征是：

A.内存驻留型木马

B.无文件攻击载荷

C.横向移动行为轨迹

D.加密挖矿进程

答案：C 解析：全流量分析追踪主机间通信模式，识别横向移动行为特征。

在软件供应链安全中，SBOM（软件物料清单）的主要作用是：

A.记录第三方组件依赖关系

B.验证代码签名有效性

C.检测开源许可证冲突

D.追踪漏洞影响范围

答案：A 解析：SBOM 记录组件依赖关系，便于快速定位漏洞影响范围。

下列哪种技术通过干扰ROP链构造抵御内存攻击？

A.控制流完整性保护

B.地址空间布局随机化

C.堆栈金丝雀检测

D.数据执行保护

答案：A 解析：控制流完整性验证执行路径，阻止异常 ROP 链构造。

某Web应用使用OAuth 2.0授权码模式，防范CSRF攻击的关键措施是：

A.绑定state参数

B.限制redirect\_uri域名

C.缩短授权码有效期

D.启用PKCE扩展

答案：A 解析：state 参数绑定会话与请求，防止跨站请求伪造攻击。

在容器安全中，防止特权逃逸的最佳实践是：

A.启用只读根文件系统

B.限制capabilities权限

C.配置AppArmor策略

D.禁用共享命名空间

答案：B 解析：限制容器 capabilities 权限可最小化特权逃逸风险。

某APT攻击使用水坑攻击方式，其传播途径最可能通过：

A.恶意广告注入

B.供应链污染

C.合法网站挂马

D.鱼叉式钓鱼邮件

答案：C 解析：水坑攻击通过感染目标常访问的合法网站传播恶意代码。

在联邦学习框架中，保护参与方数据隐私的核心技术是：

A.同态加密

B.差分隐私

C.安全多方计算

D.可信执行环境

答案：C 解析：安全多方计算确保各参与方数据在加密状态下联合建模。

某企业实施红蓝对抗演练，蓝队进行网络杀伤链建模时，最应关注的阶段是：

A.武器化载荷投递

B.横向移动路径规划

C.命令与控制通道建立

D.目标数据渗出检测

答案：D 解析：检测数据渗出可及时阻断 APT 攻击最终阶段的敏感信息窃取。

根据GDPR规定，数据主体不具备的权利是：

A.数据可移植权

B.被遗忘权

C.数据收益分配权

D.拒绝画像权

答案：C 解析：GDPR 未赋予数据主体直接获得数据收益分配的权利。

在车联网安全中，CAN总线攻击的主要危害是：

A.远程控制车辆行驶

B.窃取用户隐私数据

C.篡改车载娱乐系统

D.干扰导航定位精度

答案：A 解析：CAN 总线攻击可发送伪造指令控制刹车、转向等关键系统。

某区块链项目采用PoS共识机制，其面临的主要安全风险是：

A.51%算力攻击

B.无利害关系攻击

C.双花攻击

D.自私挖矿攻击

答案：B 解析：PoS 中无利害关系攻击者可能同时参与多链验证谋取利益。

在ATT&CK框架中，防御规避战术对应的技术编号范围是：

A.TA0005

B.TA0007

C.TA0008

D.TA0011

答案：A 解析：TA0005 涵盖防御规避战术，如隐藏恶意代码、清除日志等。

某企业遭遇商业邮件诈骗（BEC），最有效的防护措施是：

A.部署邮件网关DLP

B.实施发件人策略框架

C.建立多级审批流程

D.培训员工社会工程意识

答案：C 解析：多级审批流程增加伪造邮件执行转账的操作难度。

下列哪项技术可检测基于进程空洞化的无文件攻击？

A.内存取证分析

B.文件系统监控

C.注册表变更审计

D.网络流量特征匹配

答案：A 解析：内存取证可检测未落地的恶意代码及进程空洞化注入痕迹。

在云原生安全中，服务网格（Service Mesh）提供的核心安全功能是：

A.微服务间mTLS通信

B.容器镜像漏洞扫描

C.工作负载身份管理

D.自动密钥轮换机制

答案：A 解析：服务网格自动管理微服务间 mTLS 加密通信，确保传输安全。

某智能合约存在重入漏洞，攻击者可利用的以太坊操作码是：

A.CALL

B.DELEGATECALL

C.CREATE

D.SELFDESTRUCT

答案：A 解析：CALL 操作码未校验重入状态，导致合约余额被重复提取。

在零信任架构中，实现动态访问决策的核心组件是：

A.策略执行点

B.策略管理平台

C.持续诊断缓解系统

D.身份治理引擎

答案：C 解析：持续诊断系统实时评估设备状态，动态调整访问权限策略。

在联邦学习场景中，实现参与方模型参数加密更新的最佳方案是采用：

A.差分隐私技术

B.同态加密技术

C.安全多方计算

D.可信执行环境

答案：B 解析：同态加密支持在加密状态下直接进行模型参数更新，无需解密，保障联邦学习隐私安全。

根据《关键信息基础设施安全保护条例》，运营者应至少每几个月开展一次网络安全检测和风险评估？

A.3

B.6

C.12

D.24

答案：B 解析：《关键信息基础设施安全保护条例》规定运营者应至少每 6 个月开展一次安全检测评估。

下列哪种攻击手法利用了HTTP协议的分块传输编码机制实现Webshell隐蔽通信？

A.HTTP慢速攻击

B.分块编码木马

C.请求走私攻击

D.反射型XSS

答案：B 解析：分块编码木马利用 HTTP 分块传输编码机制隐藏恶意载荷，规避传统检测。

在ATT&CK框架中，防御规避战术（Defense Evasion）对应的技术分类编号是：

A.TA0002

B.TA0005

C.TA0007

D.TA0011

答案：B 解析：ATT&CK 框架中防御规避战术对应 TA0005，涵盖绕过防御的技术手段。

某企业使用SDP（软件定义边界）架构，其核心安全机制体现在

：

A.动态端口隐藏

B.单包授权认证

C.双向证书校验

D.网络流量加密

答案：B 解析：SDP 通过单包授权（SPA）实现动态端口隐藏和身份认证，核心在于零信任访问控制。

针对区块链智能合约的重入攻击，最有效的防护措施是：

A.引入互斥锁机制

B.限制外部调用gas

C.采用检查-生效-交互模式

D.启用SafeMath库

答案：C 解析：检查-生效-交互（Checks-Effects-Interactions）模式可防止重入攻击中的状态不一致问题。

根据GDPR规定，数据主体不具备的权利是：

A.数据可移植权

B.反对自动化决策权

C.数据收益分配权

D.被遗忘权

答案：C 解析：GDPR 未赋予数据主体收益分配权，核心权利包括访问、删除等。

在容器安全中，防止容器运行时逃逸的关键配置是：

A.禁用特权容器

B.启用Seccomp策略

C.限制Capabilities

D.挂载只根文件系统

答案：A 解析：特权容器拥有宿主机内核权限，禁用可阻断容器逃逸攻击路径。

某APT组织利用PowerShell脚本进行内存驻留，检测此类攻击的最佳方法是：

A.静态特征码扫描

B.进程行为监控

C.日志聚合分析

D.网络流量镜像

答案：B 解析：PowerShell 内存驻留攻击无文件特征，需通过进程行为异常监控检测。

下列哪种技术可有效抵御基于GPU的彩虹表攻击？

A.PBKDF2密钥延伸

B.动态盐值混淆

C.硬件安全模块

D.会话令牌绑定

答案：A 解析：PBKDF2 通过多次哈希迭代增加计算时间，抵御 GPU 并行破解。

在零信任架构中，实现动态策略决策的核心组件是：

A.策略执行点

B.持续诊断系统

C.身份治理引擎

D.威胁情报平台

答案：C 解析：身份治理引擎动态评估用户行为和环境风险，生成实时访问策略。

针对工控系统的Modbus协议，防范非法指令注入应优先部署：

A.协议白名单过滤

B.深度包检测引擎

C.流量基线分析

D.工业防火墙规则

答案：A 解析：协议白名单仅允许合法 Modbus 指令，直接阻断非法指令注入。

量子计算背景下，下列哪种算法属于抗量子密码体系？

A.RSA-4096

B.ECC-secp521r1

C.Kyber

D.AES-256

答案：C 解析：Kyber 基于格密码学，可抵抗量子计算攻击，属 NIST 推荐抗量子算法。

某企业实施红队演练时，蓝队进行杀伤链建模最应关注的阶段是：

A.初始访问突破

B.横向移动路径

C.命令控制建立

D.数据渗出检测

答案：D 解析：数据渗出是攻击最终目标，蓝队需重点检测异常数据外传行为。

在云安全责任共担模型中，属于客户责任范畴的是：

A.物理设备维护

B.虚拟化层更新

C.操作系统补丁

D.应用访问控制

答案：C 解析：客户负责操作系统及应用的补丁管理，云服务商负责底层设施。

检测HTTPS中间人攻击的有效方法是验证：

A.证书颁发机构

B.证书密钥用法

C.证书吊销状态

D.证书指纹绑定

答案：D 解析：证书指纹绑定（Certificate Pinning）可防止中间人伪造合法证书。

某Web应用使用GraphQL接口，防范注入攻击需重点检查：

A.输入参数过滤

B.查询深度限制

C.类型系统校验

D.速率限制策略

答案：A 解析：GraphQL 注入需对输入参数进行严格过滤，防止恶意查询构造。

在可信计算中，实现运行时度量的关键技术是：

A.静态可信根

B.动态可信链

C.远程证明协议

D.安全启动机制

答案：B 解析：动态可信链在运行时持续度量组件完整性，确保执行环境可信。

根据等级保护2.0，三级系统应具备的审计功能不包括：

A.日志加密存储

B.实时告警阈值

C.审计进程独立

D.异地备份机制

答案：D 解析：三级系统要求日志保存 6 个月，异地备份非强制要求。

某物联网设备采用国密SM9算法，其密钥协商机制基于：

A.椭圆曲线配对

B.大整数分解难题

C.离散对数问题

D.格基数学难题

答案：A 解析：SM9 算法基于椭圆曲线配对，实现标识密码体系的密钥协商。

防范基于内存空洞化的无文件攻击，最有效的检测手段是：

A.进程行为监控

B.文件系统扫描

C.注册表审计

D.网络特征匹配

答案：A 解析：无文件攻击驻留内存，需监控进程内存异常行为及代码注入痕迹。

在车联网安全中，CAN总线协议的主要安全威胁是：

A.拒绝服务攻击

B.固件逻辑篡改

C.远程控制劫持

D.时序攻击

答案：C 解析：CAN 总线协议缺乏认证机制，攻击者可发送伪造指令远程操控车辆。

某区块链项目采用DPoS共识机制，其面临的主要风险是：

A.51%算力攻击

B.委托节点串谋

C.双花攻击

D.自私挖矿

答案：B 解析：DPoS 依赖委托节点验证，节点合谋可能导致共识机制失效。

根据ISO 27001，信息安全风险处置的优先顺序应为：

A.规避-转移-缓解-接受

B.缓解-转移-规避-接受

C.转移-规避-缓解-接受

D.规避-缓解-转移-接受

答案：A 解析：ISO 27001 优先规避风险，其次转移、缓解、接受。

在移动应用安全中，检测HTTPS证书锁定的最佳方法是：

A.动态污点分析

B.中间人代理测试

C.反编译审计

D.流量协议解析

答案：B 解析：中间人代理测试可验证客户端是否严格校验证书指纹。

某企业使用CASB解决方案，其核心功能不包括：

A.影子IT发现

B.数据分类识别

C.云配置核查

D.容器镜像扫描

答案：D 解析：CASB 聚焦云应用安全，容器镜像扫描属容器安全范畴。

在云原生安全中，服务网格（Service Mesh）提供的核心安全能力是：

A.服务间mTLS

B.密钥自动轮换

C.负载身份管理

D.漏洞扫描集成

答案：A 解析：服务网格通过 mTLS 加密微服务间通信，确保传输层安全性。

防御基于LLMNR协议的网络欺骗攻击，应优先配置：

A.协议禁用策略

B.响应包过滤

C.网络分段隔离

D.数字签名认证

答案：A 解析：禁用 LLMNR 协议可消除名称解析欺骗攻击面。

某智能合约存在时间戳依赖漏洞，攻击者可利用的以太坊操作码是：

A.TIMESTAMP

B.CALLVALUE

C.BALANCE

D.EXTCODESIZE

答案：A 解析：TIMESTAMP 操作码返回区块时间戳，依赖此值的合约易被操纵。

在零信任架构中，实施微隔离的最小粒度是：

A.虚拟机层面

B.容器实例级

C.进程通信级

D.用户会话级

答案：C 解析：微隔离细化至进程间通信，实现最小权限网络访问控制。

在抗量子密码体系中，基于格密码学的密钥交换协议主要防范的攻击类型是：

A.中间人攻击

B.量子傅里叶变换攻击

C.侧信道时间分析

D.代数结构分析

答案：B 解析：格密码抗量子特性主要防御量子傅里叶变换对离散对数的破解。

某企业零信任架构中，动态策略引擎因策略冲突导致业务延迟

，应优先优化的组件是：

A.用户实体行为分析模块

B.策略冲突消解算法

C.加密流量深度解析引擎

D.身份生命周期管理系统

答案：B 解析：策略冲突消解算法优化决策逻辑，减少业务延迟。

根据GDPR最新修订案，数据主体新增的核心权利是：

A.数据可移植权

B.算法透明解释权

C.数据收益分成权

D.紧急删除请求权

答案：B 解析：GDPR 新增算法透明解释权，要求自动化决策可追溯。

防御基于光纤分光窃听的物理层攻击，最有效的技术措施是：

A.量子密钥分发协议

B.全同态加密传输

C.光信号噪声注入

D.波分复用隔离技术

答案：A 解析：量子密钥分发（QKD）基于物理原理防止光纤分光窃听。

某区块链项目采用分片技术提升吞吐量，其面临的核心安全风险是：

A.跨分片双花攻击

B.委托节点合谋

C.智能合约逻辑漏洞

D.状态数据存储膨胀

答案：A 解析：分片技术中跨分片交易可能被恶意节点双花攻击。

在工控系统深度包检测中，误阻断合法Modbus指令的根本原因可能是：

A.协议指纹特征库版本滞后

B.时序完整性校验机制缺失

C.异常流量阈值设置不当

D.会话上下文跟踪失效

答案：A 解析：协议指纹库过时会导致深度包检测误判合法指令为异常。

检测容器镜像中恶意代码层的有效方法是：

A.动态沙箱行为监控

B.镜像哈希白名单校验

C.层级差分对比扫描

D.运行时内存取证分析

答案：C 解析：层级差分对比可发现镜像构建过程中注入的恶意代码层。

根据《关键信息基础设施安全保护条例》，运营者应至少每几个月开展供应链风险评估？

A.3

B.6

C.12

D.24

答案：C 解析：供应链风险评估需每年至少一次，与整体安全检测周期一致。

联邦学习中实现梯度参数隐私保护的关键技术是：

A.差分隐私噪声叠加

B.同态加密聚合

C.安全多方计算协议

D.可信执行环境隔离

答案：A 解析：差分隐私在梯度中添加噪声，防止通过参数反推原始数据。

某APT组织利用Windows COM劫持实现持久化，应急响应时应重点检查的注册表项是：

A.HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\CLSID

B.HKEY\_CURRENT\_USER\Environment

C.HKEY\_USERS\.DEFAULT\RunOnce

D.HKEY\_CURRENT\_CONFIG\System

答案：A 解析：COM 组件劫持常通过注册表 CLSID 项注入恶意代码实现持久化。

防御针对VoIP系统的DTMF注入攻击，应优先部署：

A.语音内容过滤系统

B.信令协议完整性校验

C.会话边界控制器

D.流量基线异常检测

答案：B 解析：DTMF 注入通过信令协议篡改，完整性校验可阻断非法指令。

在云原生服务网格中，实现服务间mTLS自动化的核心组件是：

A.Istio Pilot

B.Envoy代理

C.SPIFFE身份框架

D.Vault密钥管理

答案：A 解析：Istio Pilot 负责策略下发和证书管理，自动化服务间 mTLS 配置。

根据等级保护2.0标准，四级系统日志留存时间应不少于：

A.3个月

B.6个月

C.12个月

D.24个月

答案：B 解析：等级保护 2.0 要求四级系统日志留存至少 6 个月。

某智能合约存在预言机操纵漏洞，攻击者可利用的以太坊预编译合约是：

A.ecRecover

B.sha256

C.ripemd160

D.modexp

答案：D 解析：modexp 预编译合约可能被用于操纵预言机输入参数。

检测基于进程空心化的无文件攻击，最有效的技术手段是：

A.页表项完整性校验

B.系统调用序列分析

C.内存映射特征扫描

D.异常句柄链追踪

答案：C 解析：进程空心化修改内存映射，特征扫描可识别异常内存区域。

在车联网V2X通信中，防范虚假消息广播应采用的密码学机制是：

A.群签名方案

B.环签名混淆

C.基于属性的加密

D.零知识证明

答案：A 解析：群签名允许匿名认证消息来源，防止虚假消息广播。

某企业部署全流量分析系统，能够有效识别的攻击行为是：

A.基于DNS隧道的C2通信

B.内存马反射注入

C.ROP链堆喷射攻击

D.无文件PowerShell载荷

答案：C 解析：全流量分析可识别横向移动行为轨迹，如异常 SMB 协议通信。

根据ISO 27001:2025，信息安全事件分类新增的类别是：

A.供应链妥协事件

B.深度伪造内容传播

C.量子计算密钥破解

D.AI模型投毒攻击

答案：A 解析：ISO 27001:2025 新增供应链妥协事件分类，强化第三方风险管理。

防御针对TPM2.0的固件降级攻击，关键措施是：

A.启用Secure Boot验证

B.强制固件完整性度量

C.限制PCR寄存器访问

D.实施远程证明协议

答案：B 解析：强制固件完整性度量可阻止攻击者降级 TPM 固件版本。

在零信任架构中，实现持续身份验证的核心技术是：

A.自适应多因子认证

B.生物特征行为分析

C.硬件安全密钥绑定

D.风险评分动态调整

答案：D 解析：动态风险评分根据会话上下文持续调整认证强度，实现自适应访问控制。

在抗量子密码算法中，基于NTRU问题的密钥封装机制主要抵御的攻击类型是：

A.格基约简攻击

B.量子傅里叶变换攻击

C.侧信道时间分析

D.中间相遇攻击

答案：A 解析：基于 NTRU 问题的密钥机制属于格密码体系，主要抵御格基约简攻击。

某企业实施零信任架构时，发现微隔离策略影响业务连续性，最应优化的技术组件是：

A.动态访问控制引擎

B.用户行为基线分析

C.策略仿真验证模块

D.加密流量深度解析

答案：C 解析：策略仿真验证模块可测试策略对业务的影响，优化连续性。

根据GDPR最新修订案，数据主体新增的权利是：

A.数据可移植权

B.算法解释拒绝权

C.数据收益分成权

D.紧急数据删除权

答案：B 解析：GDPR 新增算法解释拒绝权，允许拒绝自动化决策。

防御基于物理层光缆窃听的攻击，最有效的防护措施是：

A.量子密钥分发

B.全同态加密传输

C.光纤振动监测

D.波分复用隔离

答案：C 解析：光纤振动监测能实时检测物理窃听行为。

某区块链项目采用分片技术提升性能，其面临的主要安全风险是：

A.跨分片双花攻击

B.51%算力集中化

C.智能合约重入漏洞

D.状态数据膨胀

答案：A 解析：分片技术可能因跨分片交易验证不完整导致双花攻击。

在ATT&CK框架中，初始访问战术对应的技术编号范围是：

A.TA0001

B.TA0003

C.TA0007

D.TA0011

答案：A 解析：ATT&CK 框架中初始访问战术编号为 TA0001。

某工控系统部署深度包检测时误阻断合法Modbus指令，根本原因可能是：

A.协议指纹特征库过时

B.时序完整性校验缺失

C.异常流量阈值过低

D.会话上下文跟踪失效

答案：A 解析：过时的协议特征库无法识别合法指令格式导致误阻断。

检测容器镜像中隐藏的恶意代码层，最有效的方法是：

A.动态行为沙箱分析

B.镜像哈希白名单校验

C.层级差分对比扫描

D.运行时内存取证

答案：C 解析：层级对比可发现恶意代码注入的镜像层差异。

根据《关键信息基础设施安全保护条例》，运营者应至少每几个月开展供应链安全风险评估？

A.3

B.6

C.12

D.24

答案：C 解析：条例明确要求每年至少开展一次供应链风险评估。

在联邦学习中，实现梯度隐私保护的关键技术是：

A.差分隐私澡声注入

B.同态加密参数聚合

C.安全多方计算协议

D.可信执行环境隔离

答案：A 解析：差分隐私通过添加噪声保护梯度数据隐私。

某APT组织利用Windows COM劫持进行持久化，应急响应时应重点检查的注册表项是：

A.HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\CLSID

B.HKEY\_CURRENT\_USER\Environment

C.HKEY\_USERS\.DEFAULT＼RunOnce

D.HKEY\_CURRENT＿CONFIG\System

答案：A 解析：COM 劫持常通过 CLSID 注册表项实现持久化。

防御针对VoIP系统的DTMF注入攻击，应优先部署：

A.语音内容过滤系统

B.信令协议完整性校验

C.会话边界控制器

D.流量基线异常检测

答案：C 解析：会话边界控制器可过滤异常 DTMF 信令。

在云原生安全中，实现服务网格间mTLS自动化的核心组件是：

A.lstio Pilot

B.Envoy代理

C.SPIFFE身份框架

D.Vault密钥管理

答案：A 解析：Istio Pilot 负责自动化 mTLS 策略配置。

根据等级保护2.0,四级系统日志留存时间应不少于：

A.3个月

B.6个月

C.12个月

D.24个月

答案：B 解析：等保 2.0 规定四级系统日志留存不少于 6 个月。

某智能合约存在预言机操纵沥洞，攻击者可利用的以太坊预编译合约是：

A.ecRecover

B.sha256

C.ripemd160

D.modexp

答案：A 解析：ecRecover 预编译合约可能被用于伪造签名。

检测基于进程空心化的无文件攻击，最有效的技术手段是：

A.页表项完整性校验

B.系统调用序列分析

C.内存映射特征扫描

D.异常句柄链追踪

答案：C 解析：内存特征扫描可识别空心化进程的异常映射。

在车联网V2义通信中，防范虚假消息广播应采用的密码学机制是：

A群签名方案

B.环签名混淆

C.基于属性的加密

D.零知识证明

答案：A 解析：群签名可验证消息来源真实性且保护身份隐私。

某企业部署全流量分析系统，能够有效识别的攻击行为是：

A.基于DNS隧道的C2通信

B.内存马反射注入

C.ROP链堆喷射攻击

D.无文件PowerShell载荷

答案：A 解析：全流量分析能识别 DNS 隧道的数据特征。

根据ISO 27001:2025,信息安全事件分类中新增的类别是：

A供应链妥协事件

B.深度伪造内容传播

C.量子计算密钥破解

D.AI模型投毒攻击

答案：A 解析：新版标准新增供应链安全事件分类。

防御针对TPM2.0的固件降级攻击，关键措施是：

A.启用Secure Boot验证

B.强制固件完整性度量

C.限制PCR寄存器访问

D.实施远程证明协议

答案：B 解析：强制固件度量防止降级到脆弱版本。

在零信任架构中，实现持续身份验证的核心技术是：

A.自适应多因子认证

B.生物特征行为分析

C.硬件安全密钥绑定

D.风险评分动态调整

答案：D 解析：动态风险评分实现持续身份验证决策。

某Web3应用使用zk-SNARKs实现隐私交易，其面临的主要安全威胁是：

A.可信设置后门

B.量子计算机破解

C.电路逻辑漏洞

D.椭圆曲线参数污染

答案：C 解析：zk-SNARKs 电路逻辑漏洞可能导致证明伪造。

根据《工业互联网安全分类分级管理办法》，三级企业应每年开展的安全评测次数是：

A.1

B.2

C.3

D.4

答案：B 解析：管理办法规定三级企业每年评测两次。

检测基于GPU的密码破解行为，最有效的监控指标是：

A.CUDA内核调用频率

B.显存带宽占用率

C.GPU温度异常波动

D.显存页错误计数

答案：A 解析：CUDA 调用频率突增提示密码破解行为。

某物联网设备采用LoRaWAN协议，防范重放攻击的关键机制是

A.帧计数器校验

B.动态会话密钥

C.消息完整性码

D.网络ID白名单

答案：A 解析：帧计数器防止重放旧数据包。

在红队演练中，绕过EDR监控的最佳技术路径是：

A.直接系统调用注入

B.反射式DLL加载

C.滥用合法签名进程

D.内存无文件驻留

答案：C 解析：滥用合法签名进程可绕过 EDR 监控。

防御针对SCADA系统的工控协议模糊测试，应优先配置：

A.协议格式白名单

B.输入数据范围限制

C.会话状态机校验

D.流量速率闽值

答案：A 解析：协议白名单过滤非法格式数据包。

某企业使用SASE架构，其核心安全能力体现在：

A.云原生代理链集成

B.全局策略统一编排

C.边缘计算威胁情报

D.零信任网络访问

答案：D 解析：SASE 核心能力为零信任网络访问控制。

根据NIST SP 800—207,零信任的七大支柱不包括：

A.设备态势感知

B.微隔离实施

C.自动化编排

D.数据分类标签

答案：D 解析：数据分类标签不属于零信任七大支柱。

检测基于HTTP/2的0day沥洞利用，最有效的防护层是：

A.协议规范化过滤

B.负载均衡器拆包

C.应用层语义分析

D.TLS终止代理

答案：C 解析：语义分析可识别 HTTP/2 协议层异常。

某区块链跨链桥遭遇治理攻击，根本原因是：

A.多重签名闽值过低

B.预言机数据篡改

C.智能合约权限溢出

D.共识机制中心化

答案：A 解析：多重签名阈值过低易引发治理攻击。

在可信执行环境(TEE)中，防范侧信道攻击的关键设计是：

A.内存加密总线

B.恒定时间算法

C.随机化内存布局

D.指令集隔离

答案：B 解析：恒定时间算法消除侧信道时间差异。

某APT组织利用Cobalt Strike Beacon进行横向移动，最可能滥用的Windows协议是：

A.WMI远程执行

B.SMB文件共享

C.RDP远程桌面

D.WinRM管理

答案：A 解析：WMI 协议常用于远程执行横向移动。

根据OWASP 2025十大API安全风险，新增的高危沥洞是：

A.过度数据暴露

B.权限提升链

C.影子API端点

D.批量分配攻击

答案：B 解析：OWASP 2025 新增权限提升链漏洞。

防御针对ML模型的对抗样本攻击，最有效的防护措施是：

A.输入数据归一化

B.梯度掩码混淆

C.对抗训练增强

D.模型蒸饱压缩

答案：C 解析：对抗训练增强模型鲁棒性。

某云服务商启用机密计算，其保护的核心对象是：

A静态存储数据

B.网络传输载荷

C.内存处理状态

D.持久化日志

答案：C 解析：机密计算保护内存数据处理状态。

在5G核心网中，实现用户面数据安全隔离的关键技术是：

A.网络切片

B.服务化架构

C.边缘计算

D.无线加密

答案：A 解析：网络切片实现用户面逻辑隔离。

根据PCI DSS 4.0，要求强制实施的控制措施是：

A.多因素认证全覆盖

B.持续沥洞扫描

C.加密传输默认启用

D.安全代码审查

答案：A 解析：PCI DSS 4.0 要求全面实施多因素认证。

检测基于Tor网络的隐蔽C2通道，最有效的分析方法是：

A.流量时序特征匹配

B.DNS解析模式识别

C.入口节点黑名单

D.电路建立行为建模

答案：D 解析：电路建立行为建模识别 Tor 特征。

某智能电网系统遭受FDl攻击，首要防护措施是：

A.状态估计残差检测

B.物理冗余传感器

C.通信链路加密

D.访问控制白名单

答案：A 解析：状态估计残差检测发现 FDI 数据异常。

在Post-QuantumTLS 1.3中，用于密钥交换的算法组合是：

A.Kyber + X25519

B.Dilithium + RSA

C.Falcon + ECDSA

D.SPHINCS + + EdDSA

答案：A 解析：NIST 推荐 Kyber+X25519 混合方案。

防御针对PLC的梯形图逻辑注入，应部署的工控安全组件是：

A.工业防火墙规则链

B.代码签名验证模块

C.操作指令白名单

D.变更管理系统

答案：B 解析：代码签名验证阻止未授权逻辑注入。

某企业实施SBOM（软件物料清单），主要解决的安全问题是：

A.许可证合规风险

B.供应链投毒攻击

C.第三方组件沥洞

D.代码签名伪造

答案：C 解析：SBOM 用于追踪第三方组件漏洞。

根据MITRE ATT&CK v15,新增的战术是：

A.凭证访问

B.影响操作

C.网络影响力

D.资源开发

答案：D 解析：ATT&CK v15 新增资源开发战术。

检测基于WASM的浏览器挖矿脚本，最有效的阻断方法是：

A.内存使用率监控

B.WebAssembly沙盒

C.行为启发式分析

D.加密流量解密

答案：C 解析：行为分析识别挖矿脚本特征。

某金融机构部署同态加密处理征信数据，主要解决的问题是：

A.数据存储机密性

B.计算过程隐私性

C.传输通道安全性

D.用户身份匿名性

答案：B 解析：同态加密保护计算过程数据隐私。

防御针对Al训练数据的投毒攻击，关键控制点是：

A.数据来源可信验证

B.特征工程降维处理

C.异常样本剔除算法

D.模型输出鲁棒性

答案：A 解析：验证数据来源防止投毒攻击。

在ISO 27001:2025中，新增的信息安全控制域是：

A.人工智能伦理治理

B.量子安全迁移

C.深度伪造防护

D.云原生配置管理

答案：B 解析：新增量子安全迁移控制域。

某车联网平台遭受OTA固件篡改，根本原因在于缺失：

A.安全启动链验证

B.加密签名校验

C.版本回滚保护

D.差分更新验证

答案：B 解析：缺失签名校验导致固件篡改。

根据NIST CSF 2.0,梭心功能中新增的环节是：

A.识别(Identify)

B.治理(Govern)

C.恢复(Recover)

D.保护(Protect)

答案：B 解析：CSF 2.0 新增治理核心功能。