# 以下哪些措施可以有效预防病毒、蠕虫和特洛伊木马的感染？（ ）

A、使用最新的防病毒软件

B、定期扫描系统

C、限制用户的权限

D、教育用户识别恶意软件

**正确答案：** ABCD

# 病毒、蠕虫和特洛伊木马的攻击方式有哪些不同？（ ）

A、病毒通常感染文件，蠕虫自我复制，特洛伊木马隐藏在合法软件中

B、病毒和蠕虫可以通过网络传播，而特洛伊木马通常需要用户执行

C、病毒和特洛伊木马可能会导致系统崩溃，而蠕虫主要消耗网络资源

D、所有上述描述都是正确的

**正确答案：** ABC

# 如何应对恶意软件的变异？（ ）

A、使用具有启发式检测的防病毒软件

B、定期更新病毒数据库

C、实施强制性的系统更新

D、使用沙箱技术进行测试

**正确答案：** ABCD

# 以下哪些行为可能会导致恶意软件的感染？（ ）

A、下载不明来源的软件

B、点击电子邮件中的不明链接

C、从不更新操作系统和软件

D、使用弱密码

**正确答案：** ABC

# 恶意软件防御策略应该包括哪些方面的内容？（ ）

A、预防措施

B、检测机制

C、响应计划

D、恢复流程

**正确答案：** ABCD

# 恶意软件的清除过程中，哪些步骤是关键的？（ ）

A、隔离受感染的系统

B、使用防病毒软件进行深度扫描

C、移除恶意软件文件

D、恢复受影响的系统文件

**正确答案：** ABCD

# 如何确保恶意软件防御策略的有效性？（ ）

A、定期测试防御措施

B、监控恶意软件的活动

C、更新防御策略以适应新威胁

D、培训用户识别和应对恶意软件

**正确答案：** ABCD

# 恶意软件攻击的哪些方面可以作为防御的切入点？（ ）

A、攻击者的入口点

B、恶意软件的传播机制

C、攻击者的心态

D、恶意软件的执行环境

**正确答案：** ABCD

# 在恶意软件防御中，如何平衡安全性和系统性能？（ ）

A、使用高效的防病毒引擎

B、优化扫描和处理时间

C、监控系统性能

D、根据系统的重要性调整安全策略

**正确答案：** ABCD

# 恶意软件防御中，如何利用蜜罐技术？（ ）

A、收集恶意软件样本

B、分析恶意软件行为

C、吸引攻击者远离关键资产

D、测试和验证防御措施

**正确答案：** ABCD

# 恶意软件防御中，如何降低零日攻击的风险？（ ）

A、定期更新软件和系统

B、使用未知威胁检测技术

C、限制系统的暴露面

D、全面禁止网络访问

**正确答案：** ABCD

# 恶意软件防御中，如何提高用户的警觉性？（ ）

A、定期发送安全警告

B、开展安全意识培训

C、设置明显的警告标志

D、禁止所有外部电子邮件

**正确答案：** ABCD

# 恶意软件防御中，如何利用大数据技术提高防御能力？（ ）

A、分析异常流量模式

B、识别潜在的恶意行为

C、实时监控和警报

D、预测未来的威胁

**正确答案：** ABCD

# 勒索软件的主要目的是什么？（ ）

A、窃取敏感信息

B、破坏系统功能

C、迫使受害者支付赎金

D、所有上述目的

**正确答案：** ABC

# 勒索软件通常通过哪些方式传播？（ ）

A、网络共享

B、电子邮件附件

C、恶意网站

D、USB驱动器

**正确答案：** ABCD

# 以下哪些是勒索软件的特点？（ ）

A、加密受害者数据

B、显示勒索信息

C、要求支付赎金

D、具有自我销毁功能

**正确答案：** ABC

# 勒索软件防御策略应该包括哪些方面？（ ）

A、备份重要数据

B、使用防病毒软件

C、定期更新软件和系统

D、教育用户识别恶意软件

**正确答案：** ABCD

# 如何防止勒索软件感染？（ ）

A、避免打开不明链接和附件

B、使用强大的密码

C、启用自动更新

D、定期扫描系统

**正确答案：** ABCD

# 勒索软件的清除步骤通常包括哪些？（ ）

A、隔离受感染系统

B、停止勒索软件运行

C、解密被加密的数据

D、修复系统漏洞

**正确答案：** ABCD

# 面对勒索软件攻击，受害者应该如何应对？（ ）

A、不要支付赎金

B、立即关闭网络连接

C、通知相关安全机构

D、寻求专业帮助

**正确答案：** ABCD

# 以下哪些措施可以减少勒索软件攻击的风险？（ ）

A、使用最新的操作系统和软件

B、定期备份重要数据

C、限制用户权限

D、开展安全意识培训

**正确答案：** ABCD

# 如何确保勒索软件防御策略的有效性？（ ）

A、定期测试防御措施

B、监控勒索软件的活动

C、更新防御策略以适应新威胁

D、培训用户识别和应对勒索软件

**正确答案：** ABCD

# 计算机病毒的主要传播途径有（ ）

A、电子邮件

B、网络

C、存储介质

D、文件交换

**正确答案：** ABCD

# 勒索软件的赎金通常要求以哪种形式支付？（ ）

A、比特币

B、电汇

C、礼品卡

D、所有上述形式

**正确答案：** ABC

# 勒索软件攻击前通常会进行哪些侦察活动？（ ）

A、网络扫描

B、社会工程学攻击

C、系统测试

D、数据泄露

**正确答案：** ABC

# 以下哪些措施可以帮助防止勒索软件的传播？（ ）

A、使用防火墙

B、更新操作系统和应用程序

C、关闭不必要的系统服务

D、限制对内部网络的访问

**正确答案：** ABCD

# 勒索软件的清除过程中，哪些步骤是关键的？（ ）

A、隔离受感染的系统

B、使用防病毒软件进行深度扫描

C、移除勒索软件文件

D、恢复受影响的系统文件

**正确答案：** ABCD

# 勒索软件防御中，哪些实践可以提高应急响应的效率？（ ）

A、建立快速的通信渠道

B、预先准备应急响应计划

C、进行定期的应急响应演练

D、指定专门的应急响应团队

**正确答案：** ABCD

# 勒索软件防御中，如何确保防御措施适应新的威胁环境？（ ）

A、持续学习和研究

B、与安全社区合作

C、定期更新防御策略

D、保持对最新安全技术的关注

**正确答案：** ABCD

# 勒索软件攻击的哪些方面可以作为防御的切入点？（ ）

A、攻击者的基础设施

B、勒索软件的下载和执行

C、数据的加密和传输

D、攻击者的社交工程技巧

**正确答案：** ABCD

# 在勒索软件防御中，如何平衡安全性和系统性能？（ ）

A、使用高效的防病毒引擎

B、优化扫描和处理时间

C、监控系统性能

D、根据系统的重要性调整安全策略

**正确答案：** ABCD

# 勒索软件防御中，如何利用蜜罐技术？（ ）

A、收集勒索软件样本

B、分析勒索软件行为

C、吸引攻击者远离关键资产

D、测试和验证防御措施

**正确答案：** ABCD

# 数据安全能力成熟度模型的安全能力维度包括（ ）

A、组织建设

B、制度流程

C、技术工具

D、人员能力

**正确答案：** ABCD

# 数据权限申请、审批、使用、展示数据需（ ）原则

A、看看就行

B、敏感信息脱敏

C、随便发生

D、遵循最小化够用

**正确答案：** BD

# 数据安全中的数据指什么（ ）

A、数字

B、设计文档

C、客户信息

D、企业组织机构

**正确答案：** ABCD

# GB/T31168《信息安全技术云计算服务安全能力要求》提出的安全要求是通常情况下云服务商应具备的基本安全能力。在具体的应用场景下，云服务商有可能需要对这些安全要求进行调整。调整的方式有（ ）。

A、删减

B、补充

C、忽视

D、替代

**正确答案：** ABD

# GB/T31168《信息安全技术云计算服务安全能力要求》规定的安全计划所包含的内容包括但不限于（ ）。

A、云平台的基本描述

B、所采取的安全措施的具体情况

C、对云服务商新增的安全目标及对应的安全措施的说明

D、对客户安全责任的说明，以及对客户应实施的安全措施的建议

**正确答案：** ABCD

# 在不同情况下，实施云计算安全措施的主体可能包括（ ）。

A、云服务商

B、客户

C、云服务商和客户共同承担

D、其他组织承担

**正确答案：** ABCD

# 去标识化的目标包括：（ ）

A、删除所有标识符

B、数据重标识风险尽可能低

C、将数据尽可能泛化处理

D、数据尽可能有用

**正确答案：** BD

# 重标识的主要方法有：（ ）

A、分离

B、泛化

C、关联

D、推断

**正确答案：** ACD

# 数据时效性一般要求包括（ ）

A、制定数据存储时效性管理策略和规程

B、明确存储数据分享、禁止使用和数据清除有效期，具备数据存储时效性授权与控制能力

C、具备数据时效性自动检测能力

D、建立过期存储数据的安全保护机制

**正确答案：** ABD

# 在国际标准化组织（ISO）出版物类型中，技术规范（TS）指（1），公开可用规范（PAS）指（2），技术报告（TR）指（3）。（ ）

A、当所讨论的技术主题仍在开发中，或者由于任何其他原因，将来有可能但不是立即能达成可发布的国际标准时发布的出版物

B、技术委员会或分委员会收集的数据不同于能作为国际标准正式发布的数据时发布的出版物

C、制定完整的国际标准之前作为中间规范发布的出版物

D、技术委员会或分委员会下工作组层面提交的出版物

**正确答案：** ABC

# ISO/IECJTC1/SC27/WG4是安全服务与控制工作组，涵盖的主题域包括（ ）等。

A、供应链安全

B、鉴别机制

C、事件管理

D、应用安全

E、网络安全

**正确答案：** ACDE

# 信息安全治理过程包括（ ）。

A、评价

B、指导

C、监督

D、沟通

**正确答案：** ABCD

# 哪些是最终发布的国际标准出版物类型？（ ）

A、TR

B、FDIS

C、Amd

D、Cor

**正确答案：** ACD

# 信息安全管体系（ISMS）标准族包括（ ）。

A、术语标准

B、要求标准

C、指南标准

D、行业特定指南标准

E、特定控制指南标准

**正确答案：** ABCD

# 根据《网络安全法》，国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的（ ）。

A、国家标准

B、行业标准

C、团体标准

D、地方标准

**正确答案：** AB

# 根据《网络安全法》，国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建（ ）的网络空间，建立多边、民主、透明的网络治理体系。

A、和平

B、安全

C、开放

D、合作

**正确答案：** ABCD

# 《网络安全法》要求，网络产品、服务应当符合相关国家标准的强制性要求。在此基础上，法律提出了以下具体要求（ ）。

A、网络产品、服务的提供者不得设置恶意程序

B、网络产品、服务的提供者应当为其产品、服务持续提供安全维护

C、网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即向社会公布

D、网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意

**正确答案：** ABD

# 根据《网络安全法》，以下产品中，（ ）不必在安全认证或者检测合格后方可销售或者提供

A、通用网络设备

B、未有国家标准的强制性要求的产品

C、不在目录中的产品

D、网络安全专用产品

**正确答案：** ABC

# 《网络安全态势感知技术标准化白皮书（2020版）》的编制单位包括：（ ）

A、公安部第一研究所

B、公安部第三研究所

C、新华三技术有限公司

D、中国电子技术标准化研究

**正确答案：** BCD