

<b>保密性</b>	保护对信息的授权限制 访问与披露，包括保护手段 个人隐私和专有信息。注意—— 加密（传输中 - TLS）（静态数据 - AES - 256）
<b>诚信</b>	防止不当的信息修改或 破坏并包括确保信息 不可否认性和真实性。
<b>可用性</b>	确保及时可靠地访问和使用 授权用户的信息。

\*引用来源：<https://www.isc2.org/Certifications/CISSP/CISSP-学生术语表>

D.A.D.		
披露	改变	毁灭
相反的 保密性	正直的对立面	可用性的反义词

## 实现CIA——最佳实践

分离 职责	强制性的 假期	工作 旋转	最少 特权	需要 知道	双重控制
<b>可用性</b>					, SLA
<b>衡量指标：</b> RTO/MTD/RPO, MTBF					
国际航空运输协 会 (IAAAA)					
<b>识别</b>					唯一用户识别
<b>认证</b>					身份验证
<b>授权</b>					权限和许可的验证 已认证用户
<b>问责制</b>					只有授权用户才能访问和使用该系统。 系统相应地
<b>审计</b>					用于实现和达成目标的工具、流程和活动 保持合规

## 计划

类型	持续时间	示例
<b>战略计划</b>	最多5年	风险评估
<b>战术计划</b>	项目预算、人员配置等最多为1年。	
<b>运营计划</b>	几个月	修补计算机 更新AV签名 日常网络管理

## 风险管理

- 任何风险都无法完全避免。
- 风险可以被最小化并加以控制，以避免损害的影响。
- 风险管理是识别、评估、衡量、缓解或转移风险的过程。

\*引用：<https://resources.infosecinstitute.com/category/certifications-training/cissp/领域/安全与风险管理/>

解决方案——将风险控制在可容忍和可接受的水平。风险管理

约束条件——时间、预算

## 保护机制

分层	抽象概念	数据隐藏	加密
----	------	------	----

## 数据分类

这包括分析组织保留的数据，确定其重要性和价值，然后将其归类。

## 风险术语

<b>资产</b>	对公司有价值的东西。
<b>脆弱性</b>	一个弱点；缺乏保障措施
<b>威胁</b>	可能对资产全部或部分构成风险的事物
<b>威胁代理</b>	实施攻击的实体
<b>利用</b>	妥协的一个例子
<b>风险</b>	威胁发生的概率

引用：<https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/安全与风险管理/>

## 风险管理框架

预防性的 前ISO 27001标准	威慑 前ISO 27000标准	侦探	纠正性的	恢复
安全策略	安保人员	日志	警报	备份
监控摄像头	卫兵	监控摄像头	防病毒解决方案	服务器集群
回调	监控摄像头	入侵检测系统	入侵检测系统	容错驱动系统
安全意识培训	职责分离	蜜罐	业务连续性计划	数据库影子
岗位轮换	入侵报警系统	审计追踪		防病毒软件
加密	意识培训	强制休假		
数据分类	防火墙			
智能卡	加密			

## 风险管理框架类型

安全与风险管理

资产安全

安全工程

通信与网络安全

身份与访问管理

安全评估与测试

安全运营

软件开发安全

## 风险管理的6个步骤 管理框架

分类

选择

实施

评估

授权

监控器

## 威胁识别模型

<b>S.T.R.I.D.E.</b>	欺骗 - 篡改 - 抵赖 - 信息泄露 - 拒绝服务 - 权限提升
<b>D.R.E.A.D.</b>	损害 - 可重复性 - 可利用性 - 受影响程度 - 可发现性
<b>M.A.R.T.</b>	缓解 - 接受 - 拒绝 - 转移

灾难恢复 / 业务连续性计划
连续性计划目标
重要性声明
优先事项声明
组织声明
责任
紧急性与时间安排声明
风险评估
风险接受/缓解

## 法律类型

刑法
民法
行政法
综合犯罪控制法案 (1984年)
《计算机欺诈与滥用法案》 (1986年)
计算机安全法 (1987年)
政府信息安全改革法案 (2000年)
联邦信息安全管理法 (2002年)

## 知识产权

版权

商标

专利

商业机密

许可

分类级别	
军事部门	私营部门
绝密	敏感的
秘密	机密
机密	私人
敏感但未分类	公司受限的
	公司机密
未分类	公众

典型数据保留期限	
商业文件	7年
发票	5年
应付账款/应收账款	7年
人力资源 - 招聘	7年
人力资源 - 未聘用	3年
税务记录	4年
法律函件	永久地

数据安全控制	
使用中的数据	范围界定与定制化
静态数据	加密
流动的数据	安全协议，例如 https

数据所有权				
数据所有权	数据保管人	系统所有者	管理员	最终用户
最高层级/主要责任 数据 定义分类级别 定义控制措施以应对不同级别的问题 分类 定义基线安全标准 影响分析 决定何时销毁 信息	每日授权权限 确保遵守数据政策并 数据所有权指南 确保可访问性，维护并 监控安全 数据存档 数据文档 定期备份，恢复检查 验证 确保CIA 执行用户授权 实施安全控制措施	实施安全控制措施	授予权限 用于数据处理	Uses information for their job / tasks Adhere to security policies and guidelines

数据残留	
消毒	一系列删除数据的过程， 完全地
消磁	擦除磁带等介质上的数据，以确保不泄露信息。 可恢复的
擦除	文件或媒体的删除
覆盖	覆盖文件，粉碎
零填充	用零覆盖硬盘上的所有数据
毁灭	数据硬件设备的物理销毁
加密	使数据在没有特殊密钥的情况下无法读取。 算法

数据分类标准	
价值 - 有用性 - 年龄 - 关联性	
数据保留政策	
佛罗里达州电子记录与档案管理实践， 2010	
《欧洲文件保留指南》， 2012年	

标准	
美国国家标准与技术研究院 (NIST)	国家标准与技术研究院 技术
NIST SP 800系列	计算机安全在多个领域的应用
800-14 NIST SP	保障信息技术安全 系统
800-18 NIST	制定安全计划
800-27 NIST SP	实现安全的基线
800-88 NIST	卫生与处置指南 防止数据残留
800-137	持续监测计划：定义， 建立、实施、分析和报告
800-145	云计算标准
FIPS	联邦信息处理 标准

安全政策、标准与指南	
监管	法律和行业标准所要求的
咨询意见	非强制性，但建议执行
信息性的	作为他人的指导
信息 政策	定义信息处理和使用的最佳实践 安全策略：策略的技术细节 即系统安全策略：列出硬件/软件清单 使用政策及使用步骤
标准	定义使用级别
指南	非强制性标准
程序	执行任务和政策的流程
基线	最低安全水平

Domain 3: Security Engineering	
安全模型与概念	

安全模型	
------	--

矩阵 (访问控制模型) 提供访问权限，包括自主访问控制对不同对象的主题。  
读取、写入和执行权限，根据ACL定义为矩阵形式列和行为能力清单。

贝尔-拉帕杜拉 (保密模型) 无法读取更高安全级别的数据。（简称）简单的安全规则。定义安全级别的主体无法写入较低安全级别的对象。安全级别，除非它是一个受信任的主体。（也称为“\*属性”）（明文资产）的规则。

比巴 (诚信模型) 访问矩阵指定了自主访问控制。具有读写权限的主体在读写时进行操作。相同的安全级别（又称强星规则）宁静防止受试者安全等级的变化水平。

克拉克·威尔逊 (诚信模型) 无法从较低完整性级别读取数据（简称A.K.A）简单完整性公理。无法将数据写入完整性级别更高的对象。（又称“星号”完整公理）无法以更高的完整性调用服务。（又称“The”）调用属性。考虑阻止从低安全级别流向的信息。

布鲁尔和纳什 (又名中国墙) 模型 用户：一个活跃的代理转换过程（TP）：一种抽象操作，例如读取、写入和修改，通过实现。编程。

利普纳模型 商业模型（机密性与完整性）—BLP + Biba 规则1：转移访问权限、规则2：授予访问权限、规则3：删除访问规则4：读取对象、规则5：创建对象、规则6：摧毁对象、规则7：创造主体、规则8：摧毁

哈里森-鲁特-厄尔曼 模型 将对象执行的操作限制为已定义的操作。旨在维护完整性。

信息流模型 基于对象先前行为的动态访问控制行动。主体可以向客体写入数据，当且仅当主体具备相应权限。无法读取不同数据集中的另一个对象。防止对象之间的利益冲突。引用

SQL注入： 开源应用安全项目。OWASP 创建指南、测试程序和用于网络的实用工具安全。

OWASP十大安全风险 注入 / SQL注入、认证机制失效、敏感数据泄露暴露、XML外部实体、访问控制缺陷、安全配置错误、跨站脚本攻击 (XSS) 、不安全反序列化、使用已知漏洞的组件、日志记录和监控不足

跨站脚本攻击 (XSS) 通过输入失败的脚本进行攻击网页。

跨站请求伪造 攻击者利用HTTP网页的POST/GET请求来HTML表单利用用户名账户进行恶意活动。预防措施可以通过授予权用户账户来实施。这些操作。例如，在表单中使用随机字符串并存储它在服务器上。

SQL注入防护：验证输入和参数。

对称算法 密钥空间 =  $2^n$  (n为密钥位数)

密码学目标 (痛苦) P - 隐私 (保密性) A - 认证 I - 诚信 N - 不可否认性。

密码学的应用 密钥空间 =  $2^n$  (n为密钥位数)

哈希 单向函数，将消息转换为用于的哈希值通过比较发送方和接收方来验证消息的完整性价值观。

数字证书 一种用于验证证书持有者身份的电子文档。

明文 简单的短信。

密文 普通文本转换为特殊格式，使其无法阅读不使用密钥进行转换。

密码系统 用于加密的组件集合。包括算法、密钥和密钥管理功能。

密码分析 在不了解密钥的情况下破解解密文使用的加密系统。

加密算法程序 对明文进行加密，对密文进行解密。

密码学 隐藏通信信息的科学未经授权的接收者。

密码学 密码学 + 密码分析

解密 将消息转换为可读格式。

加密 将信息转换为不可读或无意义的。

一次性密码本 (OTP) 用单独的唯一密钥对所有字符进行加密。

关键聚类 不同的加密密钥生成相同的明文信息。

密钥空间 特定算法的所有可能密钥值。

算法 一种用于加密和解密过程的数学函数数据；又称密码。

密码学 加密科学。

转位 重新排列明文以隐藏原始信息；又称排列。

替代 在消息中交换或重复字符（1字节）与另一条消息。

弗南 一组随机且不重复字符的密钥。又称“One”。时间垫。

困惑 在每次加密循环中更改变密钥值。

扩散 改变密文中文明的位置。

雪崩效应 当密钥或明文的任何变化都会显著改变密文。

分裂的知识 职责分离与双重控制。

工作因素 破解加密所需的时间和资源。

随机数 任意数，用于为加密提供随机性功能。

分组密码 将明文分成块并应用相似的加密方法算法和密钥。

流密码 逐位加密——一次一位，对应数字进行加密密钥流。

翻垃圾箱 未经授权访问垃圾以寻找机密信息。

钓鱼攻击 发送伪造的消息，使其看起来来自可信来源。

社会工程学 误导他人提供机密信息。

脚本小子 一个中等水平的黑客，使用容易找到的现成代码。

互联网

MD2 128位哈希，18轮计算

MD4 128位哈希。3轮计算，512位块大小

MD5 128位哈希。4轮计算，512位块大小。默克尔-达姆加德构造

MDS 变量，0-65532比特，默克尔树结构

SHA-0 已淘汰，发现碰撞复杂度为 2^33.6 (近似值) 1小时 (在标准PC上) 已由NIST退役

SHA-1 160位MD，80轮计算，512位块大小。默克尔-达姆加德构造 (被认为不安全)

资金充足的攻击者

SHA-2 224, 256, 384和512位。64或80轮计算，512或1024块大小。默克尔-达姆加德构造

使用戴维斯-迈耶压缩函数

MD哈希算法

SHA-3 使用哈希函数来找出所使用的密钥。

SHA-4 通过逆向工程或暴力破解进行加密。

SHA-5 攻击者向另一个用户发送消息，期望该用户会将该消息作为密文转发。

SHA-6 攻击者试图诱骗用户，让他们尝试攻击者所提供的内容。

SHA-7 充另一个用户以获取所使用的加密密钥。

SHA-8 尝试所有可能的图案和组合，以找到正确的钥匙。

SHA-9 计算加密所需的执行时间和功耗设备。又称侧信道攻击

SHA-10 线性密码分析 使用线性近似法

SHA-11 密码学攻击

被动攻击 使用窃听或数据包嗅探来寻找或获取访问权限信息。

主动攻击 攻击者尝试不同的方法，例如修改消息或文件试图破解加密密钥、算法。

仅密文攻击 攻击者使用多个加密文本来找出所使用的密钥。

已知明文攻击 攻击者使用明文和密文来找出所使用的密钥。

选择明文攻击 通过逆向工程或暴力破解进行加密。

社会工程学 攻击者向另一个用户发送消息，期望该用户会将该消息作为密文转发。

暴力破解 尝试所有可能的图案和组合，以找到正确的钥匙。

差分密码分析 计算加密所需的执行时间和功耗设备。又称侧信道攻击

线性密码分析 使用线性近似法

代数攻击 利用已知单词来找密钥

频率分析 攻击者假设替换和置换密码使用的是重复模式密文中的模式。

生日攻击 假设找出两个具有相同哈希值的消息是比带有自身哈希值的消息更容易处理

字典攻击：使用字典中的所有单词来找出正确的密钥

重放攻击 攻击者反复发送相同的数据来欺骗接收者。

分析攻击 攻击者利用算法已知的弱点

统计攻击：攻击者利用算法已知的统计弱点。

因数分解攻击 通过使用RSA中大数因数分解的解决方案

反向工程学 使用加密设备解密密钥

硬件架构	
------	--

多任务处理 同时运行两个或多个任务。

多编程 同时运行两个或多个程序。

多处理 CPU由多个部分组成不止一个处理器

处理类型

单一国家 一个安全级别在...处时间。

多州 多重安全级别在一段时间。

固定 内置于软件中的ROM。

基础输入输出 系统 (BIOS) 用于的指令通过计算机加载操作系统。

移动安全 设备加密、远程擦除、远程锁定

内部锁 (语音、人脸识别、图案、PIN码)

密码 网络设备安全部署、资产跟踪 (IMIE) - 移动设备管理、可移动存储 (SD卡、Micro SD等)

物联网与互联网安全 网络分段 (隔离) - 遵循隔离 (VLAN) 、物理隔离 (网关) · 应用防火墙、固件更新

物理安全 内部威胁与外部威胁及应对措施

自然威胁 飓风、龙卷风、地震、洪水、海啸、火灾等

政治上有影响力 威胁、恐怖行动等

电力公用事业 基础设施普遍受损 (电力、电信、水、气等)

供应链威胁 人道灾害、破坏、蓄意破坏、欺诈、盗窃

主要来源 检查 液体、热量、气体、病毒、细菌、运动：(地震) 辐射等

自然灾害与控制措施 飓风、移动或检查位置、频率发生、影响、分配预算

洪水 架空地板服务器机房和存放计算机设备的办公室。

电气 UPS、现场发电机 修复内嵌温度传感器、服务器机房、通信冗余互联网连接、移动通信链路作为备用方案

温度 有线互联网

人为威胁 避开可能发生爆炸的区域

爆炸 例如：采矿、军事训练等等。

火 墙体至少2小时的防火等级，火灾报警器、灭火器

破坏行为 部署外围安全、加倍防护锁具、监控摄像头等

欺诈/盗窃 采取措施避免身体伤害访问关键系统。例如门禁指纹扫描

选址 物理的 安全目标 威慑犯罪活动——拖延入侵者 - 检测入侵者 - 评估情况 - 对应入侵

选址问题 可见性 - 外部实体 - 无障碍设施 - 施工 - 内部隔间

服务器机房安全 建筑物中部 (中间) 地板 - 单一入口门或入口点 - 火灾探测与抑制系统 - 架空地板 - 冗余电源供应器 - 坚固/不可损坏的门

围栏和盖茨 8英尺高并装有带刺铁丝网。遥控地下系统 - 隐蔽的门

周长入侵检测系统 红外传感器 - 机电式系统 - 声学系统 - 央视 - 智能卡 - 指纹/视网膜扫描

照明系统 持续照明 - 待机照明 - 可移动照明 - 应急照明

媒体存储 异地媒体存储 - 冗余备份与存储

电力 法拉第笼 + 白色噪音会导致信号干扰 - 控制区：法拉第笼 + 白色噪音

静态电力 使用防静电垫子、垫子和处理电气设备时佩戴腕带设备 - 监控与维护湿度水平。

暖通空调控制水平 高温 - 高湿度 - 低湿度

暖通空调指南 • 100°F 可能损坏存储介质例如磁带驱动器。

• 175°F 可能导致计算机和电气设备损坏。

• 350°F 可能导致火灾，原因是纸质产品。

• 暖通空调：UPS和浪涌保护器防止电池积聚。

• 噪声：电磁噪声干扰 (EMI) , 射频干扰

温度，湿度

• 计算机机房应保持 15°C 的温度。

C - 温度 23°C, 湿度 40-60% (湿度)

• 静态电压

• 40伏特损坏电路，1000伏特闪灼的显示器，1500伏特电压导致存储器丢失。2000伏特电压会造成这种情况。

## 领域4：网络与通信安全

## OSI参考模型

7层架构，允许层间变更，标准硬件/软件互操作性。

提示，OSI记忆法

似乎所有人都需要数据处理

P租赁DoNotThSausagePizzaA路

层	数据	安全
申请	数据	C, I, AU, N
演示文稿	数据	C、澳大利亚、加密
会话	数据	N
运输	片段	C, AU, I
网络	数据包	C, AU, I
数据链路	框架	C
物理的	比特	C

C=机密性, AU=认证, I=完整性, N=不可否认性

层(编号)	功能	协议	硬件/格式
物理 (1)	电信号 比特到电压		电缆, 集线器, USB, DSL 中继器, 自动柜 员机
数据链路 第二层	框架设置 错误检测与控制 检查数据包的完整性 目标地址, 帧 在MAC地址中使用IP地址 转换。	PPP - PPTP - L2TP - ARP - RARP - SNAP - CHAP - LCP - MLP - 帧中继 - HDLC - ISL - MAC - 以太网 - 令牌环 环网 - FDDI	第二层 开关 - 桥梁
网络 层	路由, 第三层交换, 分段, 逻辑的 地址。ATM。数据包。	ICMP - BGP - OSPF - RIP - IP - BOOTP - DHCP - ICMP	第三层 开关 - 路由器
运输	段 - 连接 定向的	TCP - UDP 数据报。 可靠的端到端传输 转移 - 细分 - 排序 - 以及错误检查	路由器—— VPN 专注的 rs - 网关
会话 层	数据、单工、半双工、全双工 重复的等价对等连接。	TCP - UDP - NSF - SQL - RADIUS - 以及 RPC - PPTP - PPP	网关
演示文稿 层	数据 压缩/解压缩 以及加密/解密	TCP - UDP 消息	网关
申请 层	数据	TCP - UDP - FTP - TELNET - TFTP - SMTP - HTTP CDP - SMB - SNMP - NNTP - SSL - HTTP/HTTPS。	网关

TCP/IP模型		
层次	行动	示例协议
网络访问	数据传输在此层完成	令牌环网 - 链中继 - 光纤分布式数据接口 (FDDI) • 以太网 • X.25
互联网	创建称为小数据块的数据。 要通过传输的数据报文 网络接入层	IP • RARP • ARP • IGMP • ICMP
运输	流量控制与完整性	TCP • UDP
申请	将数据转换为可读形式 格式	Telnet • SSH • DNS • HTTP • FTP • SNMP • DHCP

TCP三次握手		
SYN - SYN/ACK - ACK		
局域网拓扑结构		
拓扑学		
优点		
缺点		
巴士	• 易于设置	• 无冗余 • 单点故障 • 难以排查故障
戒指	• 容错性	• 没有中间点
开始	• 容错性	• 单点故障
网格	• 容错性	• 冗余 • 设置成本高

数字用户线路 (DSL) 的类型		
非对称数字用户线路 (ADSL)	• 下载速度高于上传速度 • 通过电话线最大距离可达5500米。 • 最大下载速度8Mbps, 上传速度800Kbps。	
速率自适应DSL (RADSL)	• 根据传输线路质量调整上传速度 • 在5500米以上距离, 最大下载速度为7Mbps, 上传速度为1Mbps。	
对称数字用户线路 (SDSL)	• 上行和下行传输速率相同。 • 距离6700米, 通过铜质电话电缆传输 • 最大下载速度2.3Mbps, 上传速度2.3Mbps。	
超高速率数字用户线路 (VDSL)	• 比标准ADSL更高的速度 • 最高下载速度52Mbps, 上传速度16Mbps, 最高可达1200米。 米制单位	
高比特率DSL (HDSL)	两对铜缆在3650米距离下的T1速度	
承诺 信息速率 (CIR)	服务提供商提供的最低保证带宽。	

局域网数据包传输		
单播	单源发送至单目的地	
组播	单源发送至多个目的地。	
广播	源数据包发送给所有目的地。	
载波侦听多路访问 接入 (CSMA)	一个工作站会不断重传帧, 直到到达目的地 工作站接收。	
带冲突的CSMA 检测 (CSMA/CD)	在检测到冲突时终止传输。用于 以太网。	
带冲突的CSMA 避免 (CSMA/CA)	在检测到繁忙传输后, 暂停并随后 随机间隔重传延迟传输至 尽量减少两个节点同时重传的情况。	
民意调查	发送者仅在轮询系统空闲时才发送。 目的地。	
令牌传递	发送方只有在收到表示可以发送的令牌时才能发送。 发送。	
广播域	接收广播的设备集合。	
冲突域	一组在运行过程中可能产生碰撞的设备 数据的同时传输	
第二层交换机	创建VLAN	
三层交换机	连接VLANs	

局域网/广域网介质		
双绞线	一对绞合铜线。用于以太网。Cat5/Se/6, Cat5 在100米距离内速度可达100Mbps。Cat5e/6的速度可达1000Mbps。	
非屏蔽双绞线 双绞线 (UTP)	对电磁干扰 (EMI) 的抵抗力较弱	
屏蔽双绞线 配对 (STP)	类似于UTP, 但包含保护屏蔽层。	
同轴电缆	用粗导线代替两根铜线。10BASE-T, 100BASE-T, 以及1000BASE-T。	
光纤	使用光作为介质来传输信号。长距离千兆速度。 距离更远。更多的错误和信号丢失。抗电磁干扰。多模光纤。 单模和多模。单模用于室外长距离传输。	
帧中继广域网	通过公共交换网络。通过中继实现高容错性 故障段恢复正常工作。	

安全网络设计——组件		
网络地址 网络地址转换 (NAT)	隐藏内部公网IP地址, 防止外部互联网访问	
端口地址 翻译 (PAT)	允许内部设备共享公共IP地址 使用ISP分配的给定单一公共IP地址的应用程序	
有状态NAT	跟踪源和目的地之间的数据包传输	
静态NAT	在两个终端之间分配一对一私有到公共IP地址 设备	
动态NAT	内部IP地址池映射一个或多个公共IP地址	

## 常见TCP协议

港口	协议
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
110	POP3
80	HTTP
143	IMAP
389	LDAP
443	HTTPS
636	安全LDAP
445	活动目录
1433	微软SQL
3389	RDP
137-139	NETBIOS

IP地址	
公网IPv4 地址空间	• A类: 0.0.0.0 - 127.255.255.255 • B类: 128.0.0.0 - 191.255.255.255 • C类: 192.0.0.0 - 223.255.255.255
私有IPv4 地址空间	• A类: 10.0.0.0 - 10.255.255.255 • B类: 172.16.0.0 - 172.31.255.255 • C类: 192.168.0.0 - 192.168.255.255
子网掩码	• A类: 255.0.0.0 • B类: 255.255.0.0 • C类: 255.255.255.0
IPv4	32位八位组
IPv6	128位十六进制

## 网络类型

本地区域 网络 (局域网)	地理距离和面积仅限于一个。 建筑物。通常使用铜线连接。 光纤技术
校园区域 网络 (CAN)	多栋建筑通过光纤连接或 无线
大都会 区域网络 (人)	城市内部的大都市网络跨度
广域网 网络 (广域网)	在大范围地理区域上互连局域网 例如, 国家或地区之间。
内网	私有内部网络
外联网	连接外部授权人员访问权限 内网
互联网	公共网络

## 网络方法与标准

软件 定义的	网络控制与分离 转发功能。
网络 (SDN)	特点——敏捷性、集中管理 程序化配置, 供应商中立。
融合 的协议	通过单一通道传输语音、数据、视频和图像 网络
媒体传输	

光纤通道	通过光纤连接或 无线
IP	
以太网	
Wi-Fi	
LTE	

多协议 标签 切换 (MPLS)	根据最短路径标签传输数据 代替网络IP地址。无需使用 路由表查找。





<tbl\_r cells="

### 三因素认证 (3FA)

知识因素	用户已知的事物
所有权因素	用户所拥有的东西，比如钥匙或令牌。
特征因素	用户特征，例如生物识别信息；指纹、面部特征扫描，签名。

#### 知识——类型/类别1——你所知道的东西

密码认证，以及诸如母亲婚前姓氏等秘密问题。  
最喜欢的食物、出生日期、键盘组合/PIN码。

#### 术语与概念

盐值哈希	在哈希处理之前添加到密码中的随机数据存储在服务器上的数据库中。用于替代可验证的明文存储，且无需泄露信息密码。
完成图。密码	字母数字组合，超过10个字符。包含一个大小写字母和数字的组合符号。
一次性密码 (OTP)	动态生成，用于一个会话或交易
静态密码	密码未更改。应避免这种情况。
认知密码	用于识别一个人的东西，例如宠物的名字。最喜好的颜色、母亲的娘家姓、出生地等等。
密码破解	未经授权访问密码文件
暴力破解攻击	多次尝试使用所有可能的密码或PIN码猜测密码的组合。
字典攻击	使用所有单词的暴力破解攻击类型词典。
社会工程学攻击	通过冒充用户身份来获取访问权限。通过社会工程手段获取合法用户凭证可信方或权威机构。
彩虹表	用于反转加密哈希的预计算表功能与破解密码。

#### 所有权——类型/类别2——你拥有的东西

同步令牌	定期创建密码。
异步令牌	根据挑战-响应生成密码技术
存储卡	一张包含用户信息的感应卡。
智能卡或集成电路卡片 (ICC)	一种包含芯片和存储器的卡片或加密狗，例如银行卡或信用卡。
名片	与硬件设备进行了刷卡操作。
非接触式卡片或感应卡	只需靠近阅读设备即可。
混合卡	允许卡片在接触式和非接触式两种方式下使用系统。
U盘	定制USB，包含访问凭证

静态密码令牌

最简单的安全令牌类型，其中密码是存储在令牌中。

挑战/回应e令牌

挑战必须通过正确的用户响应来应对。

#### 特征——类型/类别3——你所做的/你是的

生物识别技术允许用户根据

生理行为或特征。

• 生理特征，即虹膜、视网膜和指纹。

• 行为特征，即语音模式

#### 生理特征

指纹	扫描拇指或手指边缘。
手部几何学	尺寸、形状、骨长、指长或其他布局获取用户手的属性。
手部地形学	手部峰谷图案。
手掌或手部扫描	手掌指纹与手掌几何形状的结合。
面部扫描	面部特征，如骨骼、眼睛长度、鼻子、下巴形状等等。

视网膜扫描

视网膜血管扫描。

视网膜血管扫描

扫描瞳孔周围的彩色眼部分。

血管扫描

扫描用户手部或面部的静脉图案。

声纹

验证语音模式。

#### 扫描行为

签名动态：测量笔压和加速度。

按键动力学

扫描打字模式。

语音模式 / 打印

测量用户阅读特定内容的声纹模式词语。

生物识别考虑因素

在人类的一生中不会改变且独一无二。高准确率。

入学时间

生物识别系统使用的样本处理。

特征提取

从某个地方获取信息的过程采集的样本。

准确性

检查最重要的元素是否正确。

吞吐率

系统能够扫描和分析的速度。

错误拒绝费率 (FRR)

将被错误拒绝的有效用户的百分比。第一类错误。

误接受费率 (FAR)

将被错误接受为有效用户的百分比。第二类错误。

交叉误差汇率 (CER)

FRR等于FAR的点。这表示为一个百分比——CER越低越好。

生物特征扫描

有效性和准确性顺序：虹膜扫描·视网膜扫描·指纹·掌形·声纹·按键模式·签名动态。

### 术语学

访问	需要采取行动以允许对象之间的信息流动。
控制	为限制或允许访问系统而采取的安全措施。
主题	需要访问一个或多个对象的实体。
对象	由信息组成的实体。

### 访问与控制级别

集中式行政管理	只有一个组件可以控制访问。高度受限控制集中进行的层级。
去中心化行政管理	访问由信息所有者控制，可以更少一致的。
混合型	集中与分散的结合。

### 访问立场

单身签署加入 (单点登录)	• 又名联邦身份管理 • 优点：完整的密码管理，易于管理，速度更快 • 认证 • 缺点——所有系统可能被未经授权的人员入侵的风险 钥匙或钥匙的获取。
---------------	--

### 授权

#### 访问控制策略：授予用户的访问级别和控制权限。

分离的职责	为不同用户分配不同级别的访问权限保护隐私与安全。
双重控制	访问权限被授予两个或多个用户以执行特定功能。
分裂的知识	没有任何一个用户能够拥有执行任务所需的所有信息。
最小原则特权	用户被授予执行任务所需的小访问权限。
需要了解的内容	执行任务所需的最小知识水平。
无权限访问	用户未被分配对任何对象的访问权限。
目录服务	集中管理用户对象的数据库。即LDAP
Kerberos	客户端/服务器模型认证协议。 • 对称密钥加密技术 • 密钥分发中心 (KDC) • 机密性、完整性和认证，对称密钥加密术
领域	认证管理域。使用对称密钥密码学
KDC (密钥分布中心)	向客户发放服务器认证票据 • 存储网络中所有客户端和服务器的密钥。 • AS (认证服务器) • TGS (票据授予服务器)
凯尔伯罗斯登录过程	• 用户在客户端电脑/设备中输入用户名/密码。 • 客户端系统使用AES加密凭证后提交为KDC。 • KDC将输入的凭证与数据库进行匹配。 • KDC创建一个对称密钥和一个带有时间戳的TGT (票据授予票据)。客户端和Kerberos服务器使用。 • 密钥和TGT使用客户端密码哈希值进行加密。 • 客户端安装TGT并解密对称密钥使用哈希。

### 授权方法

自主访问控制 (DAC) • 强制访问控制 (MAC) • 基于角色的访问控制 (Role-BAC) • 基于规则的访问控制 (Rule-BAC)。

自主访问控制 (DAC)	使用访问控制列表 (ACL) 访问控制列表。
强制访问控制 (MAC)	根据安全标签授权主体。业主用于授予或拒绝访问权限其他用户。ACL定义了访问级别授予或拒绝给受试者。
角色访问控制 (RBAC)	基于任务的访问控制——主体需求根据对象的角色访问对象或分配的任务。
规则-BAC	使用一组规则或过滤器来定义什么可以在系统上完成或无法完成。
混合RBAC	受限的RBAC
基于晶格/标签	对象根据控制级别进行分类使用标签。
非自由裁量访问权限 / 强制访问控制	基于中央制定的政策权威。基于角色或基于任务。

### 授权方法/概念

受限接口应用	限制使用给定权限可执行的操作特权。
内容相关的	限制数据访问取决于内容本身。对象。
情境依赖的	在满足特定条件后授予用户访问权限。例如在特定日期/时间之后。
工作时间	情境依赖控制
最小权限	受试者只有在执行任务时才能接触到对象。他们需要拥有的东西。 • 不多不少！
职责分离职责与责任	任务被分配给两个或更多人执行。
用户问责制	审计与报告 · 漏洞评估 · 渗透测试 · 威胁建模
审计与报告	用户对其所采取的行为负责已完成。 需要监控以进行报告的事件：网络事件 · 应用事件 · 系统事件 · 用户事件 · 击键活动

### 访问控制类型

类型	范围/目的	示例
行政的控制装置	行政管理组织资产和个人。	数据分类，数据标签，安全意识培训。
逻辑 / 技术控制	限制访问。	防火墙、入侵检测系统/入侵防御系统，加密、生物识别、智能卡片和密码。
物理控制	保护组织基础设施和人员。	周界安全，生物识别与布线。

### 用户账户管理流程

定期审查用户账户并更改密码，通过程序跟踪访问授权，定期验证账户的活跃状态。

### 访问控制要求

CIA三要素：机密性 - 完整性 - 可用性 (参见第1领域作弊)  
床单！！！)

#### 身份管理

IAAA——身份识别 - 认证 - 授权 - 责任。	• 用户身份注册验证并添加系统标识符。 • 为用户分配适当的控制权限 • 常用用户ID或用户名。
识别	• 为用户分配适当的控制权限 • 常用用户ID或用户名。
认证	• 用户验证流程 • 常用密码
授权	• 定义用户访问的资源
问责制	• 负责控制的人员，使用日志。

### SESAME (欧洲安全应用系统)

#### 多供应商环境

公钥密码学仅验证初始段，而不验证其余部分。  
验证完整消息。使用了两个独立的票据，其中一个用于认证和其他一项定义了用户的访问权限。

## 软件测试

静态测试	被动测试代码而不运行代码：语法检查、代码审查与走查。例如：工具利用可利用的缓冲区溢出漏洞来自开源软件源代码
动态测试	使用运行环境进行分析和测试。用于第三方提供的测试软件，无访问软件代码。例如，跨站脚本攻击。SQL注入
模糊测试	使用特定输入进行动态测试的类型 在压力/负载下检测缺陷。例如，输入无效测试参数
变异 / 随机模糊测试	使用已修改的输入值进行测试。
代际 / 智能模糊测试	输入预期输入模型。
误用案例测试	评估已知风险和攻击的脆弱性。
接口测试	评估软件模块的性能与...相比 接口规范以验证工作正常运行状态。
应用程序编程接口 (API)	测试API以验证Web应用程序是否满足所有安全需求需求。
用户界面 (UI)	包括图形用户界面 (GUI) 和命令行界面 (CLI)。用户回顾接口与需求规范。
物理接口	例如，在ATM机、读卡器等物理设备中等等。
单元测试	测试系统的一小部分以测试单元是适合集成到最终产品中。
集成级别测试	程序之间的数据和控制传输接口。
系统级测试	验证系统是否具备所有所需的规格和条件功能。

## 日志管理系统

OPSEC流程	分析日常运营并审查可能的攻击采取对策。
渗透测试	从黑客的角度测试网络安全。
端口扫描器	检查计算机中开放的任何端口或端口范围。
零环	系统的内部代码。
运营保障	验证软件是否符合安全要求。
监督模式	在内部保护环中运行的进程。

## 威胁评估建模

步幅	评估针对应用程序或操作系统的威胁系统。
欺骗	使用虚假身份获取系统访问权限。 可以使用IP/MAC地址、用户名、无线网络SSID。
篡改	导致传输中或存储中的数据未经授权被修改存储。导致完整性受损以及可用性。
否认	拒绝攻击者执行的行动或活动。
信息披露	私人/机密或受限信息的分布向未经授权的第三方披露信息。
权限提升	攻击导致权限级别在有限时间内提升用户账户。
定期监测 关键绩效和 风险指标包括	未修复漏洞和被利用的数量 账户、漏洞解决时间、检测数量 软件缺陷等
漏洞扫描	自动探测系统、应用程序和网络。
TCP SYN 扫描	发送一个设置了SYN标志的报文。也称为半开放扫描。
TCP连接扫描	当运行扫描的用户没有权限时执行。 运行半开放扫描所需的权限。
TCP ACK 扫描	发送一个设置了ACK标志的数据包。
圣诞扫描	发送一个设置了FIN、PSH和URG标志的报文。
被动扫描	检测无线网络中的非法扫描设备。
认证扫描	用于访问配置文件的只读账户。

## 软件开发安全最佳实践

WASC	Web 应用安全联盟
OWASP	打开Web应用程序安全项目
BSI	“内置安全”倡议
IEC	国际电工委员会

## 安全测试

为了确保安全控制措施得到正确应用并有效使用。自动化扫描，漏洞评估和手动测试。

### 软件威胁

病毒	隐形病毒 · 多态病毒 · 宏病毒 · · 间谍软件/广告软件 · 僵尸网络 · 蠕虫病毒
Rootkit	内核模式rootkit · 引导程序rootkit · 用户模式rootkit · 虚拟根套件 · 固件根套件
源代码问题	缓冲区溢出 · 权限提升 · 后门
恶意软件防护	防病毒软件 · 反恶意软件 · 安全政策

### 考虑因素

- 资源可用性
- 被测系统的关键性和敏感性水平
- 技术故障
- 控制配置错误导致安全漏洞
- 安全攻击风险
- 性能变化的风险
- 对正常运营的影响

### 验证与确认

- 验证——SDLC设计输出符合需求
- 验证——测试以确保软件满足需求

### 安全软件

- 反恶意软件和反病毒——扫描并记录恶意软件和病毒检测结果
- IDS/IPS = 实时和混杂模式监控攻击
- 基于网络的入侵检测系统
- 本地网络监控和被动及头部级别扫描。不进行主机级别扫描。

- 基于主机的

- 使用事件日志监控主机
- 入侵防御系统 (IPS) —— 攻击检测与防御
- 远程访问软件应通过VPN访问
- 漏洞评估软件——应更新并打补丁
- 路由器——基于策略的访问控制

### 日志

网络流量	网络流量捕获
审计日志记录	与硬件设备登录和访问相关的事件
网络时间协议 (NTP)	应在整个网络中同步以确保正确性 日志和设备流量中的时间是一致的。
系统日志	设备事件消息日志标准。
事件类型	错误、警告、信息、成功审计、失败
简单网络管理协议 (SNMP)	支持思科等不同设备。

### 监控与审计

定义一个裁剪级别。又称基线。

- 审计追踪——事件/交易日期/时间，事件的作者/所有者
- 可用性——日志归档
- 日志分析——检查日志

### 代码审查与测试

由代码编写者/开发者以外的其他人检查代码以发现错误

法根检查——步骤	规划 · 概述 · 准备 · 检查 · 反工 · 后续跟进
代码覆盖率报告	测试代码结构的详细信息
用例	测试代码占总用例的百分比
代码审查报告	手动代码测试报告创建
黑盒测试	外部测试，不测试内部结构
动态测试	运行时测试代码
白盒测试	通过访问代码和内部结构进行详细测试
CVE	常见漏洞与暴露字典
CVSS	通用漏洞评分系统
NVD	国家漏洞数据库
回归测试	验证测试所需的安装是否没有出现问题 运行系统中的任何问题
集成测试	使用两个或多个组件一起测试

领域7：安全运营		CISSP 快速参考表系列																					
<h3>事故现场</h3> <p>为场景 · 事故环境保护 · 分配ID及可能情况 证据来源 · 收集证据 · 避免或最小化证据 污染</p> <p>洛卡德的 交换 原则 在犯罪中，嫌疑人会留下一些东西并带走一些东西。 一些东西。这些残留物可以用来识别嫌疑人。</p>		<h3>证据特征</h3> <table border="1"> <tr><td>足够</td><td>有效性是可以接受的。</td></tr> <tr><td>可靠</td><td>一致的事实。证据未被篡改或修改。</td></tr> <tr><td>相关</td><td>合理的事实，以及犯罪行为、手段和方式的证据，事件文档</td></tr> <tr><td>允许的</td><td>合法取得的证据</td></tr> </table>		足够	有效性是可以接受的。	可靠	一致的事实。证据未被篡改或修改。	相关	合理的事实，以及犯罪行为、手段和方式的证据，事件文档	允许的	合法取得的证据												
足够	有效性是可以接受的。																						
可靠	一致的事实。证据未被篡改或修改。																						
相关	合理的事实，以及犯罪行为、手段和方式的证据，事件文档																						
允许的	合法取得的证据																						
<h3>现场证据</h3> <p>原始证据 · 最可靠且在审判中使用 · 原始文件——例如法律合同 · 无副本或复印件</p> <p>· 不如原始证据那样具有权威性和可靠性。次级证据 · 例如：原件的副本、证人证言。证据 · 如果已有原始证据，相同内容的次级证据则无效。</p>		<h3>审讯与询问</h3> <p>采访 收集事实以确定事件的相关事项。</p> <table border="1"> <tr><td>审讯</td><td>通过证据收集方法获取供词。 · 流程：准备问题和主题，总结信息</td></tr> <tr><td>意见规则</td><td>证人仅就案件的事实作证，不能作为证据使用。</td></tr> <tr><td>专家证人</td><td>可用作证据。</td></tr> </table>		审讯	通过证据收集方法获取供词。 · 流程：准备问题和主题，总结信息	意见规则	证人仅就案件的事实作证，不能作为证据使用。	专家证人	可用作证据。														
审讯	通过证据收集方法获取供词。 · 流程：准备问题和主题，总结信息																						
意见规则	证人仅就案件的事实作证，不能作为证据使用。																						
专家证人	可用作证据。																						
<p>直接证据：无需辅助支持即可证明。例如，证人通过自身五种感官提供的证词。确凿证据：无法被反驳，是条件性证据，不需要其他辅助证据。佐证证据：不能直接证明某一事实，但可用于佐证其他证据。· 例如：证人通过自身五种感官提供的证词。· 确凿证据：无法被反驳，是条件性证据，不需要其他辅助证据。· 佐证证据：不能直接证明某一事实，但可用于佐证其他证据。· 用于佐证其他证据。</p>		<h3>网络分析</h3> <p>利用现有控制措施来检查安全漏洞事件。例如：入侵检测系统/入侵防御系统 (IDS/IPS) 、防火墙日志</p> <ul style="list-style-type: none"> <li>· 软件分析：对事件发生时正在运行的应用程序进行取证调查。</li> <li>· 硬件/嵌入式设备分析：例如个人电脑和智能手机的评测</li> </ul>																					
<h3>传闻证据</h3> <p>· 证人听到的他人所讲述的内容</p>		<h3>适用法律</h3> <ul style="list-style-type: none"> <li>· 普通法系 - 美国、英国、澳大利亚、加拿大</li> <li>· 民法 - 欧洲、南美洲</li> <li>· 伊斯兰教及其他宗教法律 - 中东、非洲、印度尼西亚、美国</li> </ul> <table border="1"> <tr><td>法律的三个分支</td><td> <ul style="list-style-type: none"> <li>· 立法：成文法——制定法律</li> <li>· 执行官：行政法——执法</li> <li>· 法律：解释法律</li> </ul> </td></tr> <tr><td>法律类别</td><td> <ul style="list-style-type: none"> <li>· 刑法——违反政府法律将导致后果通常监禁</li> <li>· 民法——对个人或组织的侵权行为导致损害或损失。造成经济损失处罚。</li> <li>· 行政/监管法——行业如何运作，组织和官员应当采取行动。惩罚可以监禁或罚款</li> </ul> </td></tr> <tr><td>统一计算机 信息 交易法 (统一计算 机交易法)</td><td>计算机相关行为通用框架 商业交易。联邦法律，例如软件的使用许可</td></tr> <tr><td>计算机犯罪法 三种伤害</td><td> <ul style="list-style-type: none"> <li>· 未经授权的入侵</li> <li>· 未经授权的更改或销毁</li> <li>· 恶意代码</li> </ul> </td></tr> <tr><td>可采证据</td><td> <ul style="list-style-type: none"> <li>· 相关、充分、可靠，不必如此。 有形的</li> </ul> </td></tr> <tr><td>传闻</td><td>· 二手数据不得在法庭上使用</td></tr> <tr><td>诱惑</td><td>· 诱使入侵者进入的行为是否属于法律上的诱捕行为，就像在……中那样? 蜜罐</td></tr> <tr><td>诱捕</td><td>· 诱导犯罪的非法行为，个人所犯下的 最初没有犯罪意图</td></tr> </table>		法律的三个分支	<ul style="list-style-type: none"> <li>· 立法：成文法——制定法律</li> <li>· 执行官：行政法——执法</li> <li>· 法律：解释法律</li> </ul>	法律类别	<ul style="list-style-type: none"> <li>· 刑法——违反政府法律将导致后果通常监禁</li> <li>· 民法——对个人或组织的侵权行为导致损害或损失。造成经济损失处罚。</li> <li>· 行政/监管法——行业如何运作，组织和官员应当采取行动。惩罚可以监禁或罚款</li> </ul>	统一计算机 信息 交易法 (统一计算 机交易法)	计算机相关行为通用框架 商业交易。联邦法律，例如软件的使用许可	计算机犯罪法 三种伤害	<ul style="list-style-type: none"> <li>· 未经授权的入侵</li> <li>· 未经授权的更改或销毁</li> <li>· 恶意代码</li> </ul>	可采证据	<ul style="list-style-type: none"> <li>· 相关、充分、可靠，不必如此。 有形的</li> </ul>	传闻	· 二手数据不得在法庭上使用	诱惑	· 诱使入侵者进入的行为是否属于法律上的诱捕行为，就像在……中那样? 蜜罐	诱捕	· 诱导犯罪的非法行为，个人所犯下的 最初没有犯罪意图				
法律的三个分支	<ul style="list-style-type: none"> <li>· 立法：成文法——制定法律</li> <li>· 执行官：行政法——执法</li> <li>· 法律：解释法律</li> </ul>																						
法律类别	<ul style="list-style-type: none"> <li>· 刑法——违反政府法律将导致后果通常监禁</li> <li>· 民法——对个人或组织的侵权行为导致损害或损失。造成经济损失处罚。</li> <li>· 行政/监管法——行业如何运作，组织和官员应当采取行动。惩罚可以监禁或罚款</li> </ul>																						
统一计算机 信息 交易法 (统一计算 机交易法)	计算机相关行为通用框架 商业交易。联邦法律，例如软件的使用许可																						
计算机犯罪法 三种伤害	<ul style="list-style-type: none"> <li>· 未经授权的入侵</li> <li>· 未经授权的更改或销毁</li> <li>· 恶意代码</li> </ul>																						
可采证据	<ul style="list-style-type: none"> <li>· 相关、充分、可靠，不必如此。 有形的</li> </ul>																						
传闻	· 二手数据不得在法庭上使用																						
诱惑	· 诱使入侵者进入的行为是否属于法律上的诱捕行为，就像在……中那样? 蜜罐																						
诱捕	· 诱导犯罪的非法行为，个人所犯下的 最初没有犯罪意图																						
<h3>资产管理</h3> <p>可用性保护 · 授权与完整性 · 冗余与容错 · 备份与恢复系统 · 身份与访问管理</p>		<h3>数据丢失防护 (DLP)</h3> <p>扫描数据以查找关键词和数据模式。在事件发生前进行保护。 基于网络的数据在传输中。扫描所有外发数据以寻找异常。将数据丢失防护 (DLP) 部署在网络边缘，以扫描所有外发数据。基于终端的数据在使用中。扫描所有内部终端用户工作站、服务器和终端DLP设备。</p>																					
<h3>入侵检测与防御系统 (IDS &amp; IPS)</h3> <p>IPS (入侵防御系统)</p>		<h3>数字数据状态</h3> <p>静态数据：存储在设备或备份介质上的数据。传输中的数据：当前正在通过网络或在设备的动态RAM中传输、准备被读取、更新或处理的数据。使用中的数据：正在被输入、处理、使用或修改的数据。</p>																					
<p>入侵检测系统 (IDS) 检测系统</p> <p>IPS (入侵检测) 预防系统</p>		<h3>备份类型</h3> <table border="1"> <tr><td>完整</td><td>所有文件已备份，归档位和修改位将被删除</td></tr> <tr><td>增量式</td><td>上次完整备份后更改的备份文件，归档位已删除。</td></tr> <tr><td>差分</td><td>仅备份已修改的文件，不要删除归档位。 需要最后一次完整备份和最后一次增量备份以完成恢复。</td></tr> <tr><td>冗余服务器</td><td>例如，RAID，通过增加磁盘来提高容错能力。</td></tr> <tr><td>服务器集群</td><td>一组同时处理流量的服务器。</td></tr> </table>		完整	所有文件已备份，归档位和修改位将被删除	增量式	上次完整备份后更改的备份文件，归档位已删除。	差分	仅备份已修改的文件，不要删除归档位。 需要最后一次完整备份和最后一次增量备份以完成恢复。	冗余服务器	例如，RAID，通过增加磁盘来提高容错能力。	服务器集群	一组同时处理流量的服务器。										
完整	所有文件已备份，归档位和修改位将被删除																						
增量式	上次完整备份后更改的备份文件，归档位已删除。																						
差分	仅备份已修改的文件，不要删除归档位。 需要最后一次完整备份和最后一次增量备份以完成恢复。																						
冗余服务器	例如，RAID，通过增加磁盘来提高容错能力。																						
服务器集群	一组同时处理流量的服务器。																						
<h3>防火墙</h3> <p>HIDS (基于主机的入侵检测系统)</p> <p>网络入侵检测系统 (N) (基于网络的入侵检测系统)</p>		<h3>灾难恢复测试</h3> <p>桌面检查审查计划内容 桌面演练：灾难恢复团队成员聚集并模拟灾难场景 模拟测试：比角色扮演更为激烈，所有支持人员和技术人员会面并针对灾难模拟进行练习 人员被转移到备用站点并开始工作</p> <p>对关键系统进行并行测试操作，同时原站点继续运行</p> <p>全面实施人员被转移到备用站点，并开始对所有系统进行测试运行，主站点则被关闭。</p>																					
<h3>分层恢复</h3> <p>类型</p> <p>1. 手动 2. 自动恢复</p>		<h3>系统故障类型</h3> <ul style="list-style-type: none"> <li>· 系统重启</li> <li>· 紧急重启</li> <li>· 系统冷启动</li> </ul>																					
<h3>数据销毁与再利用</h3> <p>对象重用 数据残留 清理 净化 毁灭</p>		<h3>BCP计划制定</h3> <table border="1"> <tr><td>定义连续性 战略</td><td> <ul style="list-style-type: none"> <li>· 计算：保护策略——硬件、软件、通信链路、应用程序、数据</li> <li>· 设施：使用主要或备用/远程站点建筑</li> <li>· 人员：运营与管理</li> <li>· 物资与设备</li> </ul> </td></tr> <tr><td>角色与 职责</td><td> <ul style="list-style-type: none"> <li>· BCP委员会：高级职员、业务部门、信息系统、安全管理员、来自各部门的官员</li> <li>· 中央电视台</li> </ul> </td></tr> <tr><td>物理安全</td><td> <ul style="list-style-type: none"> <li>· 围栏-小网格和高目数</li> <li>· 报警器</li> <li>· 入侵检测：机电式、光电式、被动红外式、声学检测</li> <li>· 运动：波形运动探测器，接近探测器</li> <li>· 锁具：防爆锁、密码锁、密码锁、设备锁、预设/普通门锁、可编程锁具锁，耙锁</li> <li>· 审计追踪：日期和时间戳、成功/失败尝试、尝试者、被尝试者已授予/修改的访问控制</li> <li>· 安全门禁卡：身份证、刷卡卡、智能卡</li> <li>· 无线接近卡：用户激活或系统感应场供电设备</li> </ul> </td></tr> </table>		定义连续性 战略	<ul style="list-style-type: none"> <li>· 计算：保护策略——硬件、软件、通信链路、应用程序、数据</li> <li>· 设施：使用主要或备用/远程站点建筑</li> <li>· 人员：运营与管理</li> <li>· 物资与设备</li> </ul>	角色与 职责	<ul style="list-style-type: none"> <li>· BCP委员会：高级职员、业务部门、信息系统、安全管理员、来自各部门的官员</li> <li>· 中央电视台</li> </ul>	物理安全	<ul style="list-style-type: none"> <li>· 围栏-小网格和高目数</li> <li>· 报警器</li> <li>· 入侵检测：机电式、光电式、被动红外式、声学检测</li> <li>· 运动：波形运动探测器，接近探测器</li> <li>· 锁具：防爆锁、密码锁、密码锁、设备锁、预设/普通门锁、可编程锁具锁，耙锁</li> <li>· 审计追踪：日期和时间戳、成功/失败尝试、尝试者、被尝试者已授予/修改的访问控制</li> <li>· 安全门禁卡：身份证、刷卡卡、智能卡</li> <li>· 无线接近卡：用户激活或系统感应场供电设备</li> </ul>														
定义连续性 战略	<ul style="list-style-type: none"> <li>· 计算：保护策略——硬件、软件、通信链路、应用程序、数据</li> <li>· 设施：使用主要或备用/远程站点建筑</li> <li>· 人员：运营与管理</li> <li>· 物资与设备</li> </ul>																						
角色与 职责	<ul style="list-style-type: none"> <li>· BCP委员会：高级职员、业务部门、信息系统、安全管理员、来自各部门的官员</li> <li>· 中央电视台</li> </ul>																						
物理安全	<ul style="list-style-type: none"> <li>· 围栏-小网格和高目数</li> <li>· 报警器</li> <li>· 入侵检测：机电式、光电式、被动红外式、声学检测</li> <li>· 运动：波形运动探测器，接近探测器</li> <li>· 锁具：防爆锁、密码锁、密码锁、设备锁、预设/普通门锁、可编程锁具锁，耙锁</li> <li>· 审计追踪：日期和时间戳、成功/失败尝试、尝试者、被尝试者已授予/修改的访问控制</li> <li>· 安全门禁卡：身份证、刷卡卡、智能卡</li> <li>· 无线接近卡：用户激活或系统感应场供电设备</li> </ul>																						
<h3>灾难恢复规划</h3> <p>灾难恢复过程</p>		<h3>证据生命周期</h3> <table border="1"> <tr><td>1. 发现</td><td></td></tr> <tr><td>2. 保护</td><td></td></tr> <tr><td>3. 录音</td><td></td></tr> <tr><td>4. 收集与识别</td><td></td></tr> <tr><td>5. 分析</td><td></td></tr> <tr><td>6. 储存、保存、运输</td><td></td></tr> <tr><td>7. 到庭出庭</td><td></td></tr> <tr><td>8. 归还给主人</td><td></td></tr> </table>		1. 发现		2. 保护		3. 录音		4. 收集与识别		5. 分析		6. 储存、保存、运输		7. 到庭出庭		8. 归还给主人					
1. 发现																							
2. 保护																							
3. 录音																							
4. 收集与识别																							
5. 分析																							
6. 储存、保存、运输																							
7. 到庭出庭																							
8. 归还给主人																							
<p>· 与其他团队的协作 · 欺诈与犯罪：例如破坏公物、抢劫 · 资金拨付 · 记录计划 - 所需文件 · 激活与恢复程序 · 计划管理 · 人力资源参与 · 成本 · 内部/外部沟通 · 团队成员的详细计划</p>		<h3>配置管理 (CM)</h3> <p>一个ITILv2和一个ITSM流程，用于跟踪所有单独的配置项 (CI)</p> <table border="1"> <tr><td>配置项目 (CI)</td><td>版本：CI的状态，配置——组件的集合 制造另一个CI的CI</td></tr> <tr><td>建筑</td><td>使用组件CI的构建列表组装组件</td></tr> <tr><td>文物</td><td>恢复程序。例如系统重启。应予以访问 由授权用户从授权终端访问。</td></tr> </table>		配置项目 (CI)	版本：CI的状态，配置——组件的集合 制造另一个CI的CI	建筑	使用组件CI的构建列表组装组件	文物	恢复程序。例如系统重启。应予以访问 由授权用户从授权终端访问。														
配置项目 (CI)	版本：CI的状态，配置——组件的集合 制造另一个CI的CI																						
建筑	使用组件CI的构建列表组装组件																						
文物	恢复程序。例如系统重启。应予以访问 由授权用户从授权终端访问。																						
<p>· 生命周期响应能力 · 事件响应与处理 · 恢复 · 反馈 缓解限制事件的影响。</p>		<h3>事件响应</h3>																					
<h3>根本原因分析 (RCA)</h3> <p>故障树分析 (FTA)：采用布尔逻辑的自上而下的演绎式故障分析。</p> <table border="1"> <tr><td>失效模式和 失效模式与影响分析 (FMEA)</td><td>对尽可能多的组件、总成和部件进行审查 尽可能识别潜在故障的子系统模式。</td></tr> <tr><td>帕累托分析</td><td>审视主要可能的原因并加以应对首先。</td></tr> <tr><td>原因映射</td><td>将个体因果关系连接起来，以形成整体。 对问题中因果关系系统的洞察。</td></tr> </table>		失效模式和 失效模式与影响分析 (FMEA)	对尽可能多的组件、总成和部件进行审查 尽可能识别潜在故障的子系统模式。	帕累托分析	审视主要可能的原因并加以应对首先。	原因映射	将个体因果关系连接起来，以形成整体。 对问题中因果关系系统的洞察。	<h3>灾难恢复方法</h3> <table border="1"> <tr><td>热站点</td><td>系统与网络活动的实时镜像 同步运行。最大限度地减少干扰和停机时间。</td></tr> <tr><td>冷站</td><td>一个配备电力和暖通空调系统的替代工作空间，但没有硬件。所有恢复工作都将依赖技术人员。</td></tr> <tr><td>温备站点</td><td>一种折衷的解决方案，包括骨骼硬件，软件和连接功能以恢复关键功能。</td></tr> <tr><td>服务局</td><td>与服务局签订合同以提供备份服务。</td></tr> <tr><td>多个中心 / 站点</td><td>多数据中心之间的流程</td></tr> <tr><td>滚动/移动站点</td><td>移动房屋或暖通空调车。</td></tr> <tr><td>恢复时间 目标 (RTOs)</td><td> <ul style="list-style-type: none"> <li>· 热站点RTO：5分钟或数小时</li> <li>· 温备站点RTO：1-2天</li> <li>· 移动站点RTO：3-5天</li> <li>· 冷站点的恢复时间目标 (RTO)：1至2周</li> </ul> </td></tr> </table>		热站点	系统与网络活动的实时镜像 同步运行。最大限度地减少干扰和停机时间。	冷站	一个配备电力和暖通空调系统的替代工作空间，但没有硬件。所有恢复工作都将依赖技术人员。	温备站点	一种折衷的解决方案，包括骨骼硬件，软件和连接功能以恢复关键功能。	服务局	与服务局签订合同以提供备份服务。	多个中心 / 站点	多数据中心之间的流程	滚动/移动站点	移动房屋或暖通空调车。	恢复时间 目标 (RTOs)	<ul style="list-style-type: none"> <li>· 热站点RTO：5分钟或数小时</li> <li>· 温备站点RTO：1-2天</li> <li>· 移动站点RTO：3-5天</li> <li>· 冷站点的恢复时间目标 (RTO)：1至2周</li> </ul>
失效模式和 失效模式与影响分析 (FMEA)	对尽可能多的组件、总成和部件进行审查 尽可能识别潜在故障的子系统模式。																						
帕累托分析	审视主要可能的原因并加以应对首先。																						
原因映射	将个体因果关系连接起来，以形成整体。 对问题中因果关系系统的洞察。																						
热站点	系统与网络活动的实时镜像 同步运行。最大限度地减少干扰和停机时间。																						
冷站	一个配备电力和暖通空调系统的替代工作空间，但没有硬件。所有恢复工作都将依赖技术人员。																						
温备站点	一种折衷的解决方案，包括骨骼硬件，软件和连接功能以恢复关键功能。																						
服务局	与服务局签订合同以提供备份服务。																						
多个中心 / 站点	多数据中心之间的流程																						
滚动/移动站点	移动房屋或暖通空调车。																						
恢复时间 目标 (RTOs)	<ul style="list-style-type: none"> <li>· 热站点RTO：5分钟或数小时</li> <li>· 温备站点RTO：1-2天</li> <li>· 移动站点RTO：3-5天</li> <li>· 冷站点的恢复时间目标 (RTO)：1至2周</li> </ul>																						
<h3>RAID、SAN和NAS</h3>		<h3>媒体分析</h3> <p>计算机取证分析的一部分，用于从存储介质中识别和提取信息。例如：磁性介质、光学介质、内存 (如 RAM)。</p>																					
<h3>可采证据</h3> <p>与事件相关。证据必须合法获得。</p>		<h3>数字取证</h3> <p>证据的五条规则：真实可信 · 准确无误 · 完整全面</p> <ul style="list-style-type: none"> <li>· 令人信服 · 可接受的</li> </ul>																					
<h3>调查 - 致 确定嫌疑人</h3> <p>类型： 运营 · 刑事 · 民事 · 电子取证</p>		<h3>安全事件与 活动管理</h3> <p>(SIEM)</p> <table border="1"> <tr><td>日志审查自动化</td><td></td></tr> <tr><td>实时分析发生的事件</td><td></td></tr> <tr><td>关于系统</td><td></td></tr> </table>		日志审查自动化		实时分析发生的事件		关于系统															
日志审查自动化																							
实时分析发生的事件																							
关于系统																							
<h3>交易冗余 实施</h3> <p>电子封存 · 远程日志记录 · 数据库影子</p>		<h3>安全事件与 活动管理</h3> <p>(SIEM)</p> <table border="1"> <tr><td>日志审查自动化</td><td></td></tr> <tr><td>实时分析发生的事件</td><td></td></tr> <tr><td>关于系统</td><td></td></tr> </table>		日志审查自动化		实时分析发生的事件		关于系统															
日志审查自动化																							
实时分析发生的事件																							
关于系统																							
<h3>系统加固</h3> <ul style="list-style-type: none"> <li>· 卸载不必要的应用程序</li> <li>· 禁用不必要的服务</li> <li>· 拒绝不需要的端口</li> <li>· 外部存储设备限制</li> <li>· 监控与报告</li> <li>· 漏洞管理系统</li> <li>· IDP/IPS：攻击特征引擎应定期更新</li> </ul>		<h3>灾难恢复术语与概念</h3> <p>MTTF 平均故障间隔时间 MTTR 平均修 复时间 MTBF (平均故障间隔时间)， MTTF + MTTR 事务冗余 电子存储 · 远程日志记录 · 数据库 实现影子追踪</p>																					
<h3>业务连续性规划</h3>		<h3>业务连续性 计划 (BCP)</h3> <p>涉及业务的保存与恢复问题。 事件发生时 对正常业务运营的中断。</p>																					
<h3>业务影响 分析 (BIA)</h3>		<h3>业务影响 分析 (BIA)</h3> <p>评估IT中断影响的过程。 BIA是BCP的一部分</p>																					
<h3>灾难恢复计划 (DRP)</h3>		<h3>灾难恢复计划 (DRP)</h3> <p>需要采取的步骤和行动框架 实现业务连续性和灾难恢复 目标。 最终目标——恢复正常运营——规划 灾前必须进行准备和发展——BIA 应该完整</p>																					
<h3>业务连续性 步骤</h3>		<h3>业务连续性 步骤</h3> <p>1. 范围与计划启动 2. BIA - 评估破坏性流程的影响 3. 业务连续性计划制定 —— 利用业务影响分析 (BIA) 制定BCP (业务连续性计划) 测试 4. 计划批准与实施 —— 管理 批准</p>																					
<h3>可信恢复</h3>		<h3>可信恢复</h3> <p>违规确认 确认系统故障期间未发生安全漏洞。</p> <p>失败准备 备份关键信息以实现恢复</p> <p>系统恢复 操作系统或应用程序发生故障后，系统应该足够稳定，以确保系统处于正常运行状态。 安全状态</p>																					

## Domain 8: Software Development Security

软件开发生命周期 (SDLC)	
理解并贯穿整个软件开发过程的安全性 生命周期 (SDLC)	
开发方法论	
构建与修复 瀑布 V形 原型制作 增量式 螺旋 快速 申请 发展 (RAD) 敏捷	
<ul style="list-style-type: none"> <li>没有关键架构设计</li> <li>问题出现时立即解决</li> <li>没有正式的反馈循环</li> <li>被动反应而非主动应对</li> </ul> <p>线性顺序生命周期</p> <p>每个阶段在继续之前都已完成</p> <p>在周期内没有正式的方式进行变更</p> <p>项目在收集反馈和重新启动之前结束</p> <p>基于瀑布模型</p> <p>每个阶段在继续之前都已完成</p> <p>每个阶段后的验证与确认</p> <p>没有风险分析阶段</p> <p>快速原型制作——快速样品测试当前方案</p> <p>项目 · 进化式原型设计——逐步改进 一种设计</p> <p>操作原型——渐进式改进 用于生产</p> <p>多个周期 (~ 多个瀑布)</p> <p>随时以不同阶段重新开始</p> <p>易于引入新需求</p> <p>向软件提供增量更新</p> <p>迭代式</p> <p>开发过程中的风险分析</p> <p>未来信息和需求，用于风险评估分析</p> <p>允许在开发早期进行测试</p> <p>快速原型制作</p> <p>专为快速开发而设计</p> <p>分析和设计迅速展示出来</p> <p>测试和需求经常被重新审视</p> <p>总称 - 多种方法</p> <p>强调效率和迭代开发</p> <p>用户故事描述了用户做了什么以及为什么这样做</p> <p>原型被分解为单个特征</p>	
DevOps (开发与运维)	
软件开发·质量保证·IT 运营	
软件开发方法	
数据库系统	
数据库	定义数据的存储与操作
数据库管理系统 (DBMS) 管理 系统	软件程序控制对存储数据的访问 在数据库中。
数据库管理系统类 型	分层式·网络·网格·面向对象 · 关系型
DDL	数据定义语言定义了结构和 模式 DML
Db 度数	表中的属性 (列) 数量
元组	行
DDE	动态数据交换
DCL	数据控制语言。SQL 的子集。
语义完整性	确保数据之间的语义规则得到执行 类型
参照完整性	所有外键都引用现有的主键
候选键	一个属性，它是某个范围内的唯一标识符。 给定表中，其中一个候选键变为 主键和其他的是备选键
主键	独特的数据识别
外键	对包含主键的另一张表的引用 主键。外键与主键的关联被称为 参照完整性。
数据库管理系统术语	<ul style="list-style-type: none"> <li>错误的摘要·脏读·丢失 更新</li> <li>动态生命周期对象：开发的对象 面向对象的软件使用 编程环境</li> <li>ODBC - 开放数据库连接。数据库 应用程序之间通信的功能 无需程序即可访问不同类型的数据库 代码</li> <li>数据库污染——数据混杂问题 不同的分类级别</li> <li>数据库分区——拆分单个数据库 将数据库分割成多个具有独特内容的部分</li> <li>多实例化——同一表中存在两个或多个相同行。 关系数据库表看起来是相同的 主键和表中的不同数据。</li> </ul>

编程语言类型		数据仓库与数据挖掘		变更管理流程	
机器语言	处理器直接指令——二进制表示法	数据仓库	整合来自多个来源的数据。	请求控制	建立组织框架，使用户能够 请求修改，进行成本/效益分析 管理，以及开发人员的任务优先级排序
组装语言	使用符号和助记符来表示二进制代码—— ADD、PUSH和POP	数据挖掘	将数据整理成更便于开展业务的格式 基于内容的决策。	改变控制	建立组织框架，使开发人员能够 在实施之前创建并测试解决方案。 生产环境。
高水平语言	处理器无关的编程语言——使用 IF、THEN 和 ELSE 语句作为 代码逻辑的一部分	聚合	将来自不同来源的信息进行整合的行为。	发布控制	发布前变更审批
非常高水平语言	第四代语言进一步减少了代码量 所需——程序员可以专注于算法。 Python、C++、C#和Java	推理	信息拼凑过程	配置管理流程	
自然语言	第五代语言使系统能够学习和 自主变化——人工智能	访问控制	<ul style="list-style-type: none"> <li>内容依赖访问控制：访问权限基于内容而定。 数据的敏感性</li> <li>上下文相关访问控制：通过访问控制实现权限管理 位置、一天中的时间以及之前的访问历史。</li> </ul>	软件版本控制 (SVC)	一种存储和跟踪变更的方法论 软件
数据库架构与模型		访问控制机制	<ul style="list-style-type: none"> <li>数据库视图：用户或组可以查看的数据集合</li> <li>数据库锁：防止同时访问</li> <li>多实例化：防止数据干扰违规行为 在数据库中</li> </ul>	配置识别	软件和硬件的标签 具有唯一标识符的配置
关系模型	使用属性 (列) 和元组 (行) 来 整理数据	原子性	如果所有操作未完成，则回滚数据库。 交易必须全部完成，否则就不完成。	配置控制	验证软件版本的修改 遵守变更控制和 配置管理策略。
层次化的模型	父子结构。一个对象可以有一个子对象。 多个孩子或无子女。	一致性	通过保持事务的一致性来维护完整性	配置审计	确保生产环境是 与会计记录一致
网络模型	类似于层次模型，但对象可以拥有 多个父母。	隔离	交易与其他交易保持独立，直到..... 完成	能力成熟度模型	
面向对象模型	具备处理多种数据类型的能力 并且比关系型数据库更具动态性。	耐用性	已提交的事务无法回滚	反应性的	1. 启动——非正式流程， 2. 可重复的——项目管理流程
对象关系型模型	面向对象与关系型数据库的结合 模型。	A · C · I · D		主动的	3. 定义——工程流程、项目规划， 质量保证，配置管理实践 4. 管理——产品和流程改进 5. 优化——持续流程改进
数据库接口语言		传统SDLC		项目管理工具	
开放数据库连接性 (ODBC)	通过API进行本地或远程通信	步骤	分析、高层设计、详细设计、施工 测试、实施	甘特图	展示关系的条形图类型 项目与时间表之间的协调。
Java数据库连接性 (JDBC)	连接数据库的Java API， 发出查询和命令等	阶段	<ul style="list-style-type: none"> <li>启动：可行性分析、成本分析、风险分析 管理层批准，基本安全控制</li> <li>功能分析与规划：需求 定义、审查拟议的安全控制措施</li> <li>系统设计规范：详细设计规范， 检查安全控制措施</li> <li>软件开发：编码、单元测试、原型设计 验证、确认</li> <li>验收测试与实施：安全性 测试，数据验证</li> </ul>	项目评估 复习技巧 (计划评审技术)	用于衡量项目进度的工具 软件开发产品的 能力 用于计算风险。
X ML	DB API 允许 XML 应用程序进行交互 与更传统的数据库相比	面向对象技术 (OOT) —— 术语学		面向对象设计的阶段	
对象链接与 嵌入数据库 (OLE) DB	是ODBC的替代品	对象既包含数据，也包含操作这些数据的指令。 关于数据。		OORA (需求) 分析	定义对象和交互的类别
知识管理		封装	数据存储为对象	OOA (分析)	识别常见的类和对象 任何领域中的应用——过程 发现
专家 系统	两个主要组成部分：“知识库”和 推理引擎 · 运用人类推理 · 基于规则的知识库 · 如果-那么语句 · 干扰系统	信息	通知对象执行某个操作。	OOD (设计)	对象是类的实例
专家 系统 (二) 模式	<ul style="list-style-type: none"> <li>前向推理：从已知事实出发并应用推理。 推理规则，以提取更多数据单元，直到它达到目标。 目标。自下而上的方法。广度优先搜索 战略</li> <li>逆向推理：从目标开始，逐步进行。 通过推理规则反向推导得出... 支持目标所需的事实。自上而下 方法。深度优先搜索策略。</li> </ul>	方法	对对象执行操作以响应某个事件 信息。	面向对象编程 (OOP)	介绍对象和方法
神经的 网络	通过观察事件积累知识， 测量他们的投入和产出，然后进行预测 成果并通过多次迭代不断改进 随着时间的推 移。	行为	对象响应a所显示的结果 信息。其特征由其方法所定义，这些方法是..... 对象内定义的函数和子程序 班级。	ORB (对象请求代理) 经纪人	作为中间件定位器和分发者工作 为了这些物品
隐蔽通道 (存储与定时)		班级	定义行为的方法集 物体	CORBA (公共对象请求代理架构) 对象请求	使用ORB的架构和标准 允许不同的系统和软件在...上运行 相互连接的系统
可执行内容 移动代码	ActiveX控件、Java小程序、浏览器脚本	对象	包含方法的类的实例	凝聚力	
病毒	在宿主的帮助下传播	继承	子类访问父类的方法	凝聚力	独立工作，无需他人帮助 程序 · 高内聚——无集成或交互 与其他模块一起 · 低内聚性——与其他事物有交互作用 模块 · 耦合——对象之间的交互程度
蠕虫	无需宿主帮助即可传播	多个 继承	从多个父母继承特征 班级	病毒类型	
逻辑炸弹/代码 炸弹	在特定事件发生时运行	多实例化	同一关系数据库中的两行或更多行 表中的主键元素似乎完全相同 但包含不同的数据	引导扇区	引导记录感染程序，获得最高权限 访问权限，并且可能是最具破坏性的
缓冲区溢出	内存缓冲区耗尽	抽象	对象用户不需要了解这些信息 关于这个物体是如何运作的	系统感染器	感染可执行系统文件、BIOS和系统 命令
后门	恶意代码在后端安装 前端用户的帮助	进程隔离	为进程分配独立的内存空间 操作系统发出的指令和数据。	UEFI	感染系统预装的UEFI (固件)
隐蔽通道	未经授权的信息收集	可信计算机基 (TCB)		伴侣	病毒存储在除特定位置以外的其他地方 主系统文件夹。例如：NOTEPAD.EXE
僵尸网络	僵尸代码曾导致数千台设备被入侵 系统论	所有硬件、固件和/或软件组件的集合，这些组件是 对其安全至关重要。任何在此方面的妥协都可能危及系统。 安全。		隐身	对文件或引导扇区的任何修改都被隐藏了 由病毒引起
特洛伊木 马	表面上看起来像恶意代码的代码，或者 表现为有害或必要的代码	输入/输出 运营	可能需要与更高层次的环进行互动 保护——此类通信必须 监控中	多部分	感染引导扇区和可执行文件
安全评估与测试术语		执行域 切换	调用其他应用程序的应用程序或 其他领域的服务	自我混淆	试图通过更改来躲避反病毒软件 对其自身代码的编码，也称为“混淆”
跨站请求 伪造 (CSRF / XSRF)	浏览器网站信任被利用，试图通过..... 强制提交经过认证的请求至 第三方网站。	内存保护	监控内存引用以验证 存储中的机密性和完整性	多态的	病毒在传播过程中会改变“混乱”模式
跨站脚本攻击 (跨站 脚本攻 击)	使用输入来模拟用户的浏览器 从可信站点执行不可信代码	流程激活	监控寄存器、进程状态信息， 以及漏洞的文件访问列表	居民	程序加载到内存时按需加载
会话劫持	试图获取先前已认证的 不强制浏览器请求的会话 提交	反病毒类型		主引导程序 记录/扇区 (MBR)	感染系统的可启动部分
SQL注入	通过Web应用程序直接攻击数据库	渗透测试	识别和确定的过程 系统漏洞的真实性质	基于签名	
热修复 / 更新 / 安全修复	更新操作系统和 应用	补丁管理 系统	管理补丁的部署到... 防止已知的攻击途径	基于启发式方法	
服务包	完整操作系统的补丁集合 系统	开放系统	具有已发布API的系统——第三方可以 使用系统	保护环	
		封闭系统	专有系统——无第三方 参与	第0层	操作系统内核
		开源	源代码可以查看、编辑和 免费分发或注明出处或收费分发	第一层	操作系统中除内核之外的部分
		API 密钥	用于访问API。高度敏感 - 同上 作为密码	第二层	I/O驱动程序和实用工具
				第三层	应用程序和程序