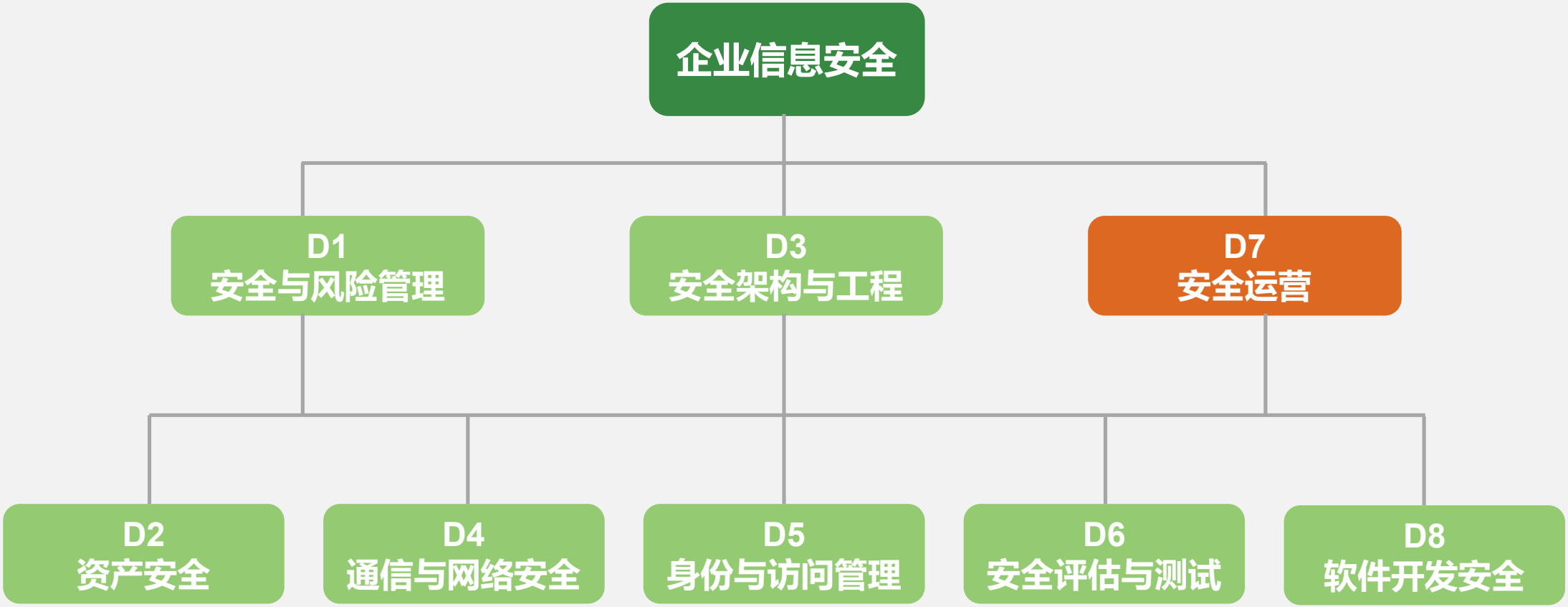

铭学在线课堂-CISSP认证
D7-运营安全
铭记初心，实现自我

知识架构


企业信息安全
D1
安全与风险管理
D3
安全架构与工程
D7
安全运营
D2
资产安全
D4
通信与网络安全
D5
身份与访问管理
D6
安全评估与测试
D8
软件开发安全

CBK学习目标

- 了解取证调查知识，以及有能力开展和支持取证调查
- 了解日志和监测还为信息技术基础设施的日常运营提供可视化展示
- 理解安全运营还涉及资源整个生命周期为其提供管理和保护
- 掌握灾难恢复
- 理解物理安全

本章知识架构


D7：运营安全
一、安全运营概述
1.1 理解和支撑调查
1.2 理解和应用基本的安全运营概念
二、操作安全实践
2.1 安全资源配置
2.2 检测和防御类措施
2.3 记录和监控活动实践
2.4 事件管理流程
三、灾难备份与恢复
3.1 灾难备份与恢复概述
3.2 容错、备份和恢复能力
3.3 灾难恢复计划制定
3.4 灾难恢复计划测试

本节目标

1.1 理解和支撑调查

- A、调查概述
- B、调查过程和证据

调查概述

- 调查可能是简短的、非正式的确定事件
- 当产生的威胁或造成的破坏足以严重到需要进行更正式的调查
- 调查的类型分为：
  - ✓行政调查
  - ✓犯罪调查
  - ✓民事调查
  - ✓监管调查

调查概述

- 事故调查员　经过专业的培训，并且拥有丰富的经验，能够发现其他人通常忽略的可疑或反常活动
- 调查员能够进行的各种评估

调查概述

- 计算机犯罪行为
  - ✓犯罪中的动机、机会和方式(Motive, Opportunity, And Means，MOM)。
  - ✓计算机犯罪调查员必须了解技术
  - ✓罗卡交换原则
  - ✓计算机犯罪的几种类型

调查过程和证据

调查过程和证据

- 证据的生命周期
- 证据：书面的、口头的、计算机生成的、视觉的或听觉的
- 法律所接受的证据包括以下特征：真实性、完整性、充足性和可靠性
- 需要证据保管链（监管链）的原因
- 一个问题是用户对隐私权的期望
- 必要时，寻求法律顾问的帮助

调查过程和证据

- 两种主要的监视类型：
  - 物理监视
  - 计算机监视
- 搜索和查封：在进行搜索和查封之前，执法机构必须拥有适当的原因，并且从法官或法庭处申请一张搜查许可证
- 访谈可能只在与法律顾问磋商后才会进行
- 审讯目的是获得用于审判的证据

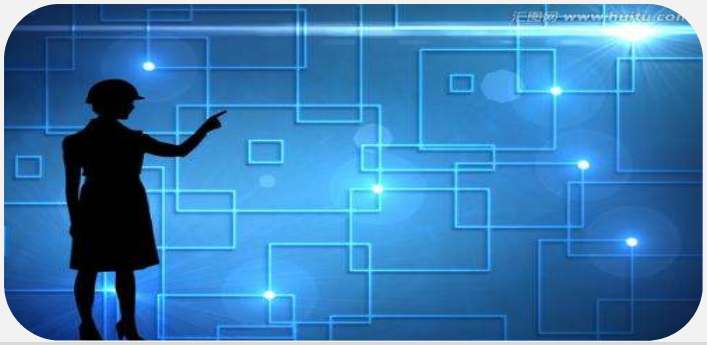
本节目标

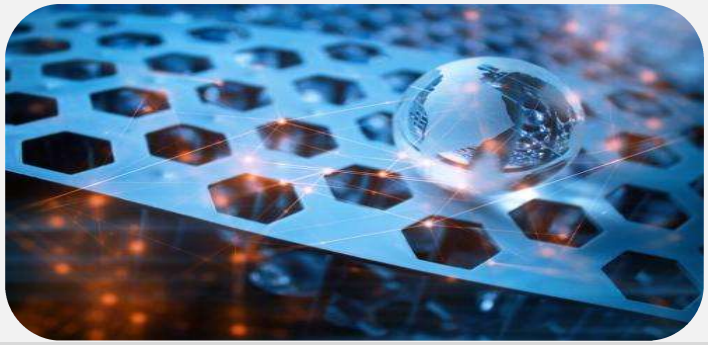
1.2 理解和应用基本的安全运营概念

- A、运营相关角色和职责
- B、安全运营相关概念

运营相关角色和职责

- 运营安全涉及配置、性能、容错、安全性以及问责和验证管理，其目的在于确保适当的操作标准与合规性要求得到满足
- 管理层负责雇员的行为和职责
- 操作部门的人员负责确保系统受到保护并在预期的方式下运行
- 应该研究任何不寻常或无法解释的事件、不定期的初始程序加载、偏离标准以及网络上其他奇怪或异常的条件。



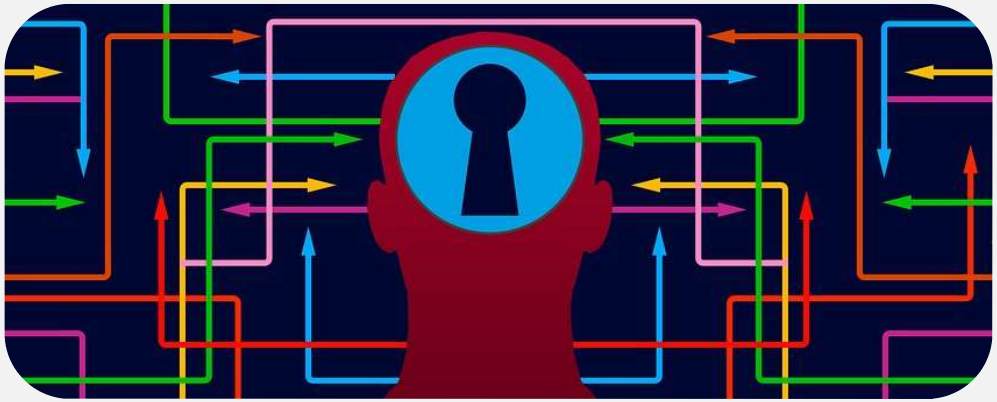


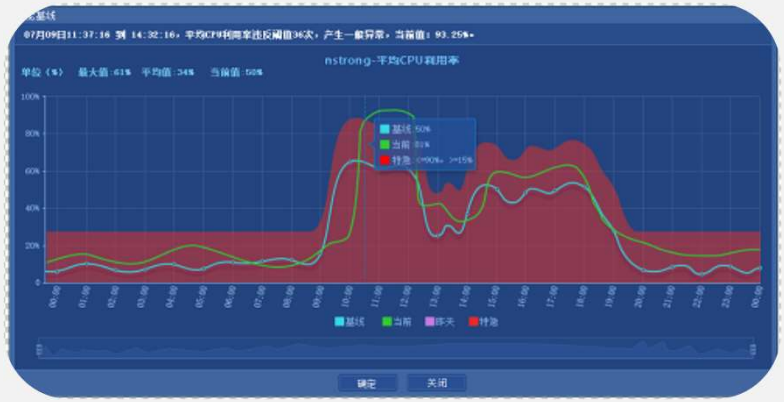
运营相关角色和职责

- 落实可问责性的好处：
  - ✓有助于确定是否确实发生违规
  - ✓系统和软件的重新配置是否有必要
  - ✓有助于捕获那些超出确定范围之外的活动
  - ✓审计需要作为日常工作开展，需要有人负责检查审计和日志事件。

运营相关角色和职责

- 为某些类型的错误预定义门限。
- 门限是违规活动的基线。
- 这条基线被称为一个阀值级别或限值级别(clipping level)





运营相关角色和职责

- 适当的安全控制和机制必须具有一定程度的透明性
- 不能让用户对控制了解太多
- 控制太过明显

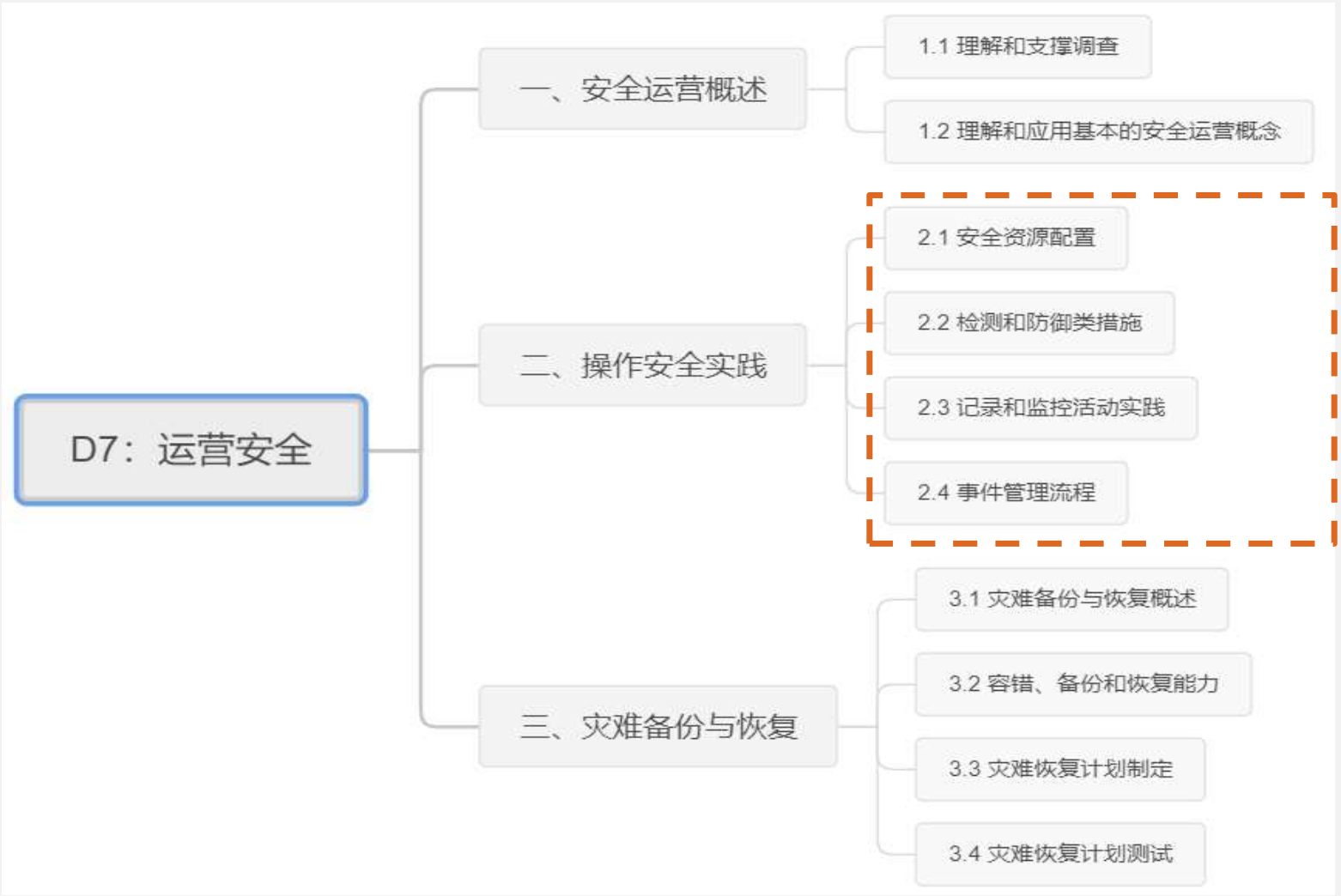
安全运营相关概念

- 知其所需和最小特权
- 权利(Entilement)
  - ✓聚合(Aggregation)
  - ✓信任传递(Transitive Trust)
- 职责分离 && 特权分离 && 任务分解
- 双人控制
- 岗位轮换
- 强制休假

安全运营相关概念

- 特权账户管理　确保员工没有超出所需权限，并且不会滥用这些权限
- 管理信息生命周期
- 服务水平协议(SLA)　　谅解备忘录 MOU
- 人员安全

本章知识架构


D7：运营安全
一、安全运营概述
1.1 理解和支撑调查
1.2 理解和应用基本的安全运营概念
二、操作安全实践
2.1 安全资源配置
2.2 检测和防御类措施
2.3 记录和监控活动实践
2.4 事件管理流程
三、灾难备份与恢复
3.1 灾难备份与恢复概述
3.2 容错、备份和恢复能力
3.3 灾难恢复计划制定
3.4 灾难恢复计划测试

本节目标

2.1 安全资源配置

- A、安全资源配置概述
- B、资产清单
- C、资产管理
- D、配置项管理和变更管理
- E、可信恢复
- F、输入和输出控制
- G、系统强化
- H、远程访问安全
- I、配置云资产

安全资源配置概述

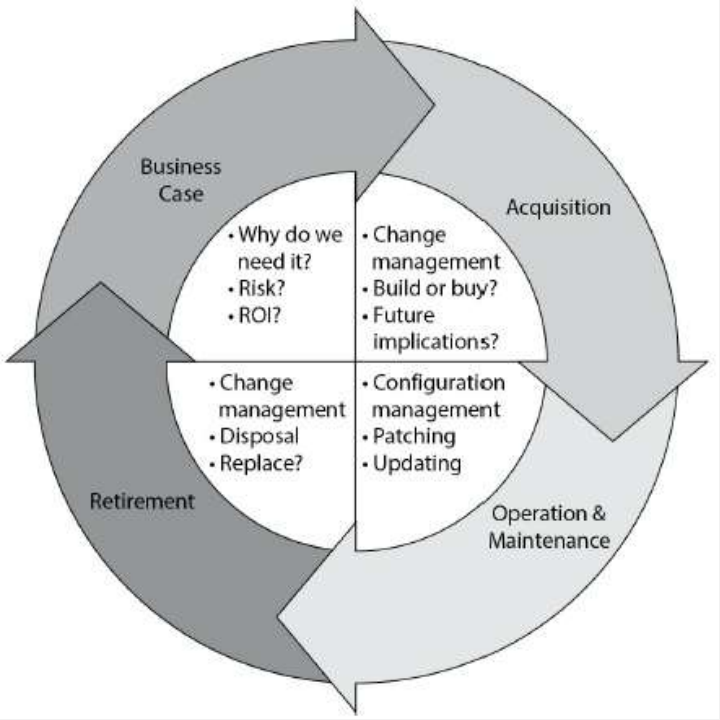
- 配置（Provisioning ）指为用户或用户群提供一种或多种信息服务所需的一系列活动，例如：
  - 对于电信服务供应商而言，它指通过布置电缆、安装客户端设备、配置服务以及设置账户等方式来提供特定服务(如DSL)的程序
  - 对于信息技术部门而言，它指在更广阔的企业环境中获取、配置和部署信息系统(如新服务器)
  - 对于云服务供应商而言，配置指的是自动启动物理服务器的新实例，这些服务器由信息技术部门提供
- 安全资源配置的核心是必须以安全方式提供这些服务

资产清单

- 保护我们的信息系统最重要的是要知道我们在防护什么。
- 跟踪硬件。
- 跟踪软件。

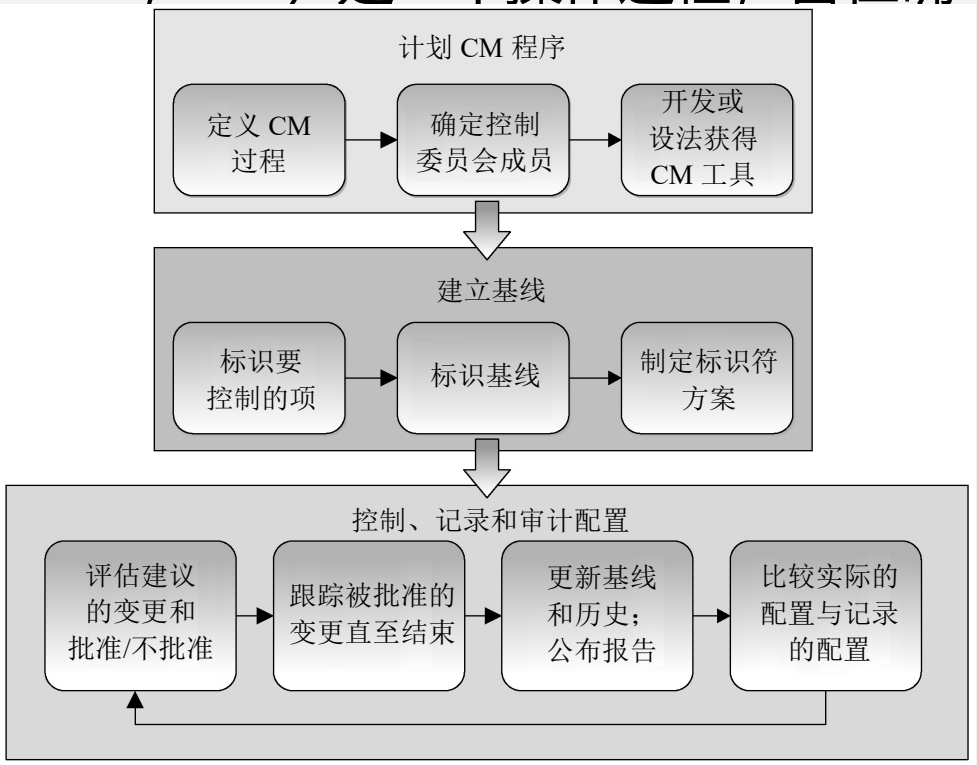
资产管理

- 资源配置只是资产管理生命周期过程中的一部分。
- 资产管理生命周期可分为四个阶段：业务案例、购置、运营和维护（O&M）以及报废



配置（项）管理和变更管理

- 配置（项）管理（Configuration Management，CM）是一个操作过程，旨在确保正确配置相应控制措施，并能及时响应
- 变更管理是一个业务流程，目的是专门用征



配置（项）管理和变更管理

- 变更管理控制提供一种流程， 实现控制、记录、跟踪和审计所有系统变更
- 变更管理流程：请求变更、审核变更、批准/拒绝变更、测试变更、安排并实施变更、记录变更
- 变更控制文档化：版本控制

可信恢复

- 当一个操作系统或应用程序崩溃或死机时，不应让系统处于任何类型的不安全状态
- 系统崩溃后应采取的正确步骤
- 在可信恢复进程中应该正确应对的安全问题

输入与输出控制

- 组织必须实施前面提到的所有控制，使它们继续以可预测的、安全的方式运行，从而确保系统、应用程序以及总体环境的可操作性。

系统强化

- 确保那些传输重要信息的网络物理组件的安全。
- 管理与保护工作站的最好方法是开发标准加固镜像，有时也被称为母盘（GM）
- 删除环境不需要的组件
- 使用最保守的设置进行配置

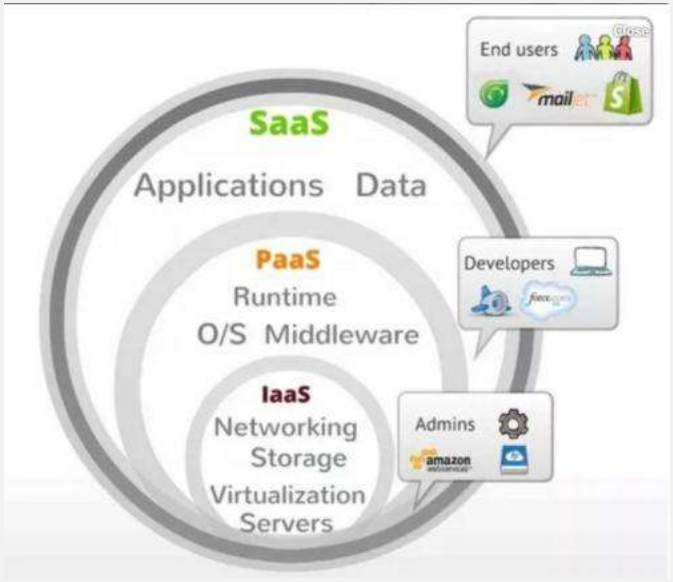
- 制定一个可接受的使用策略（AUP），防止未授权用户在环境中安装未授权软件

远程访问安全

- 为利用远程访问的优势而不必承担无法接受的风险，公司必须实施可靠的远程管理

配置云资产

- 云配置是为用户或用户群提供一种或多种新型云资产时所需的一系列活动
- 云计算一般分为三种类型的服务：基础设施即服务（IaaS）、平台即服务（PaaS）以及软件即服务（SaaS）



本节目标

2.2 检测和防御类措施

- A、常见攻击
- B、防火墙
- C、入侵检测与防御系统
- D、补丁管理、漏洞管理、反恶意软件
- E、沙箱、蜜罐、蜜网
- F、警示和白/黑名单
- G、外包服务

常见攻击

- 僵尸网
- 拒绝服务攻击
  - ✓SYN洪水（flood）
  - ✓Smurf 攻击和Fraggle攻击
  - ✓Ping洪水攻击
  - ✓死亡之Ping攻击
  - ✓泪滴攻击
  - ✓LAND攻击
- 零日利用、恶意代码、中间人攻击、蓄意破坏、间谍活动

防火墙

- 防火墙通过执行规则来操作
- 在操作上的挑战是，如何准确地跟踪当前的规则集，并制定一个程序来确定添加、修改或删除的规则
- 需要一个计划来定期评估防火墙防御的有效性
- D4中有详细描述

入侵检测与防御系统

- 主机的入侵检测系统（HIDS）、网络入侵检测系统（NIDS）和无线入侵检测系统（WIDS）
- 基于规则或异常的，或者是两者混合的
- 与其他任何检测系统一样，重要的是采取步骤使IDS或IPS降低差错率
- 减少错误的最重要的步骤是将系统基线化
- 进行广泛的配置管理

补丁管理、漏洞管理、反恶意软件

- 反恶意软件（俗称杀毒软件）旨在用来检测和消除恶意软件，包括病毒、蠕虫和木马
- 补丁管理是“为产品和系统识别、获取、安装、验证补丁”
- 漏洞管理是指定期识别漏洞、评估漏洞并采取措施减轻漏洞相关的风险

沙箱、蜜罐、蜜网

- 沙箱是一个应用程序的执行环境，它将执行代码与操作系统隔离，以防止危害安全行为的发生。
- 蜜罐是一种被开发出来的装置，目的是为了欺骗攻击者相信它是一个真实的生产系统，诱使对手对其进行攻击，然后通过监视被破坏的蜜罐，来观察和学习攻击者的行为。
- 蜜网的整个网络都旨在吸引攻击者
- “伪缺陷”、“填充单元”

警示和白/黑名单

- 警示向用户和入侵者宣传基本安全方针策略
- 白名单是一组已知良好的资源
- 黑名单是一组已知的不良资源

外包服务

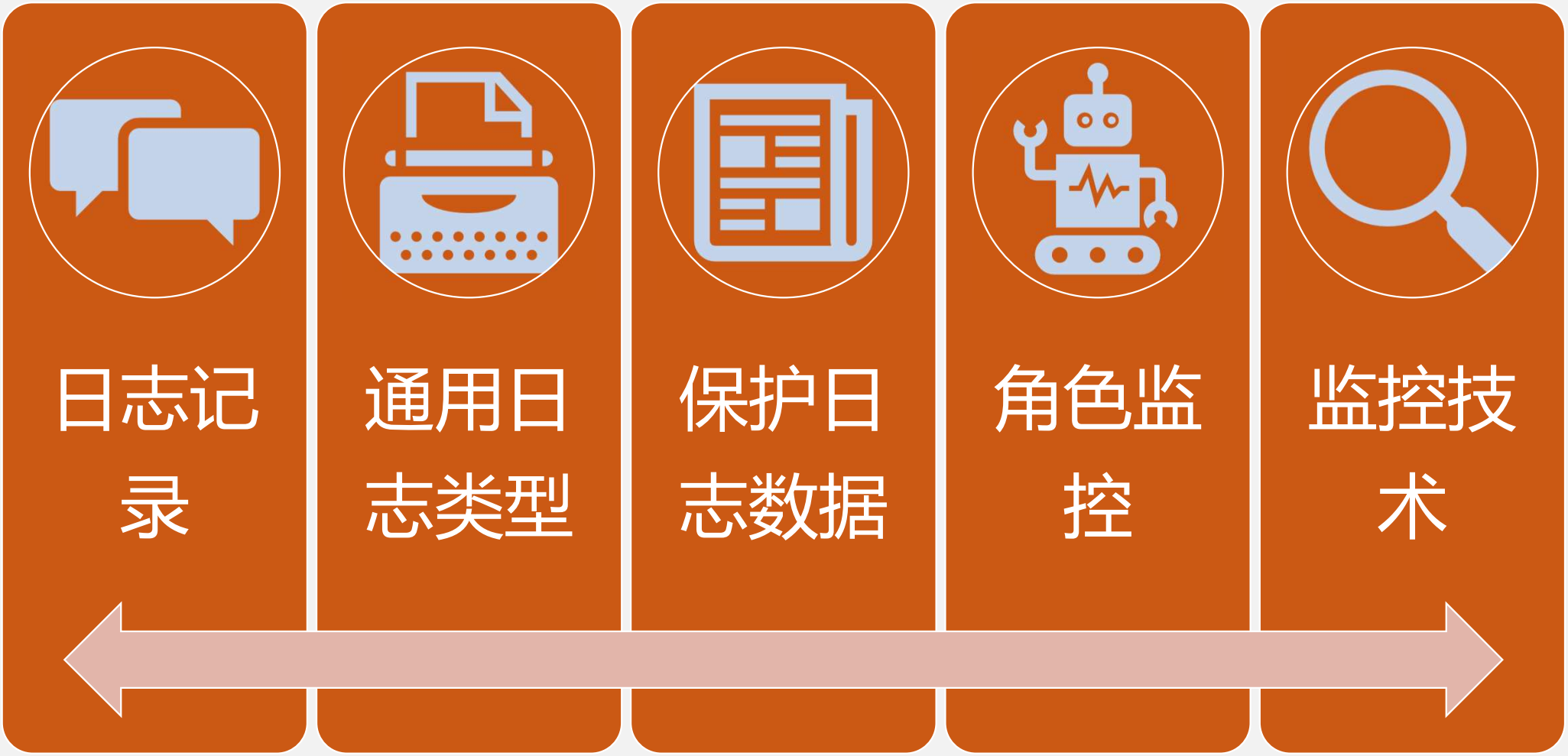
- 安全托管服务提供商（Managed Security Services Providers，MSSP）通常提供各种安全服务的专业机构，从解决方案到接管所有技术或物理安全控制措施的安装、操作和维护
- 在选择MSSP时，需要考虑以下因素：
  - ✓需求 在开始考察潜在MSSP时，确定你是否知道你的需求。
  - ✓理解 MSSP是否理解你的业务流程。
  - ✓声誉 需要花一些时间向一些安全专业人员了解MSSP的声誉
  - ✓成本 需要在MSSP服务价格和能支付的费用间做出抉择
  - ✓职责 但组织受到攻击时，尽量约定双方的职责，特别是一些在政府监管下的组织

本节目标

2.3 记录和监控活动实践

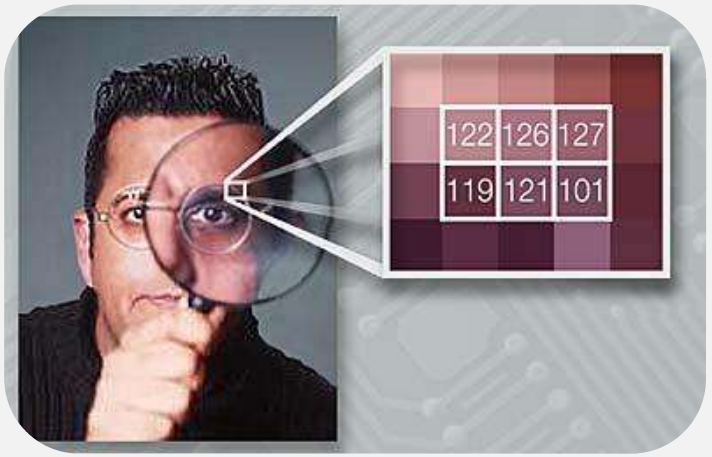
- A、日志记录和持续监测
- B、出口监控
- C、SIEM
- D、效果评价审计

日志和持续监测



出口监控

- 出口监测是指监测传出的流量， 以防止数据泄露， 也就是防止组织数据的未授权传输。
  - ✓ 数据泄露保护（DLP）
  - ✓ 隐写术
  - ✓ 水印



SIEM

- 安全信息和事件管理（SIEM）、安全事件管理（SEM）和安全信息管理（SIM），它们都是一样的
- 一种中央应用程序来自动监测网络上的系统

审计和评估有效性

- 组织将会通过审计环境的方式评估其安全策略和相关的访问控制,主要包括以下几个方面内容:

检验审计
访问审查审计
用户权限审计
特权组审计
高级别管理组
双重管理员账号
安全审计和审查
报告审计结果
保护审计结果
发布审计报告
使用外部审计师

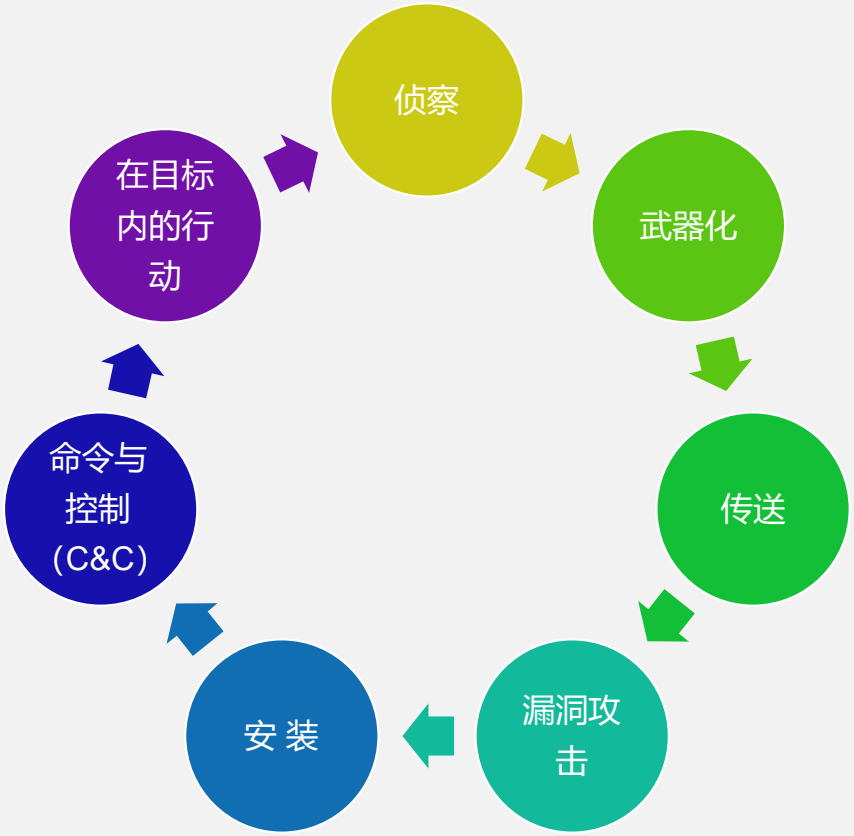
本节目标

2.4 事件响应流程

- A、网络杀伤链
- B、事件响应策略
- C、事件响应流程

网络杀伤链（The Cyber Kill Chain）

- 一个七个阶段的入侵模型



事故响应策略

- 为什么要做事故响应策略?
  - 所有公司都应当制订一个事故响应策略，以规定谁具有启动事故响应的权利，并且在事故发生之前建立支持性措施。
- 事故响应策略和事故管理包括什么?
  - 一个事件响应团队;
  - 一套标准措施，

事故响应流程

- 事件管理流程中的七个阶段：

检测 响应 缓解 报告 恢复 修复 学习

本章知识架构


D7：运营安全
一、安全运营概述
1.1 理解和支撑调查
1.2 理解和应用基本的安全运营概念
二、操作安全实践
2.1 安全资源配置
2.2 检测和防御类措施
2.3 记录和监控活动实践
2.4 事件管理流程
三、灾难备份与恢复
3.1 灾难备份与恢复概述
3.2 容错、备份和恢复能力
3.3 灾难恢复计划制定
3.4 灾难恢复计划测试

本节目标

3.1 灾难备份与恢复概述

- A、灾难的本质
- B、MTD、RTO、RPO、WRT
- C、危机管理
- D、应急通信
- E、工作组恢复

灾难的本质

- 灾难恢复计划围绕组织正常运营中断后，如何控制事件导致的混乱局面，并恢复到正常工作秩序
- 一旦IT无法支持关键任务进程，就需要通过DRP来管理还原和恢复过程。

MTD、RTO、RPO、WRT

- RTO值比MTD值小。RTO通常指使基础设施和系统恢复运行的时间，而WRT指恢复数据、测试流程以及使所有事情“活”过来可以进行生产的时间。
- 恢复点目标（Recovery Point Objective，RPO）指最大可容忍的数据丢失量，用时间来衡量
- 平均故障间隔时间（MTBF）是我们期望一台设备能可靠运行的估计时间
- 平均修复时间（MTTR）是指实际产生和发现故障后有人替换坏硬盘写入队列并完成在新硬盘上重写信息之间的时间间隔

危机管理、应急通信、工作组恢复

- 危机管理是一门科学和技术
- 灾难可能破坏一些或所有的正常通信手段
- 让工作组恢复到正常状态并且重新开始他们在日常工作地点的活动是非常重要的

本节目标

3.2 容错、备份和恢复能力

- A、保护硬盘驱动器
- B、高可用
- C、数据备份和恢复
- D、可替代的工作站点

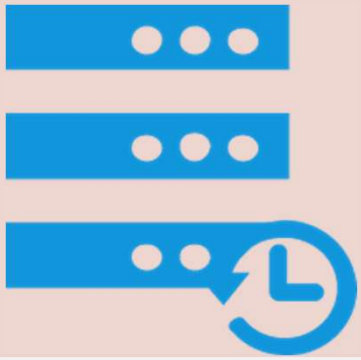
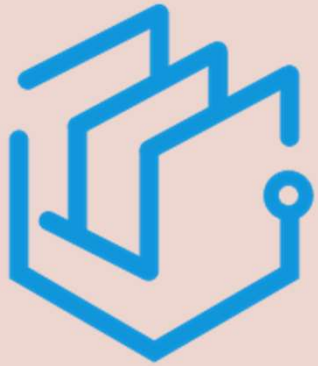
保护硬件驱动器

- RAID 包括两个或以上磁盘，即使其中一个磁盘损坏，大多数RAID也都能继续运行
- 一些常见配置如下：
  - ✓RAID-0也称为条带
  - ✓RAID-1也称为镜像
  - ✓RAID-5也叫作奇偶校验
  - ✓RAID-10也被称为RAID1+0或条带镜像

高可用

- 高可用性(HA)是保证一些业务 始终正常运行的一种技术和流程的结合
- 具体业务可能是：
  - ✓数据库
  - ✓网络
  - ✓应用程序
  - ✓电源

数据备份和恢复

完全备份 full backup	差量过程 differential process	增量过程 incremental process
		

现场和异地两处保留备份

应当有一个适当的方法从头开始备份或重新构建数据

数据备份和恢复

磁盘映像
disk shadowing

电子传送
electronic vaulting

远程日志处理
remote journaling

异步复制
asynchronous replication

同步复制
synchronous replication

可替代的工作站点

可替代的工作站点

- 三种基本可替代的工作站点

热站点（hot sit）

温站点（warm sit）

冷站点（cold sit）

可替代的工作站点

- 冗余站点
- 滚动热站点（rolling hot site）或移动站点
- 服务局和云计算
- 互惠协议

本节目标

3.3 灾难恢复计划制定

- A、为计划制定目标
- B、人员角色
- C、破坏评估
- D、恢复阶段
- E、BCP和DRP

为计划制定目标

- 建立目标对业务连续性和恢复计划尤为重要
- 实用的计划目标必须包括以下关键信息：

责任

权威

优先级

实现和测试

人员角色

- BCP（或DRP）协调员需要组建几个不同的团队，并对它们进行正确培训，一般包括：
  - ✓破坏评估团队
  - ✓法律团队
  - ✓媒体关系团队
  - ✓恢复团队
  - ✓重新部署团队
  - ✓重建团队
  - ✓救援团队
  - ✓安全团队

破坏评估

- 一旦发生灾难，还需要设立一个角色或建立一个团队来完成评估破坏工作
- 评估程序应当正确记录在文档中，应包括以下步骤:
  - ✓确定灾难的成因
  - ✓确定进一步破坏的可能性
  - ✓标识受到影响的业务功能和领域
  - ✓标识关键资源的可用程度
  - ✓标识必须立即替换的资源
  - ✓估计需要多久才能恢复关键功能
  - ✓如果还原过程超过了事先估计的MTD值，那么应立即声明为灾难，并且立即启动BCP
- 组织机构间的业务推动力和关键功能各不相同，不同组织机构具有不同准则

恢复阶段

- 恢复过程必须尽可能有组织地进行
- 书面过程十分关键，BIA期间关键功能及其资源会被标识
- 再造阶段（reconstitution phase）

BCP和DRP

- BCP团队完成下列步骤：
  1、提出连续性规划策略声明
  2、执行业务影响分析(BIA)
  3、确定和实现预防性控制
  4、制定恢复战略
  5、测试和培训
  6、持续维护计划

- DRP团队完成下列步骤：
  1、起始阶段
  2、启动阶段
  3、恢复阶段
  4、再造阶段
  5、附录

本节目标

3.4 灾难恢复计划测试

- A、灾难恢复计划测试方法
- B、了解如何维护灾难恢复计划
- C、了解通过保险降低灾难影响损失的相关内容

灾难恢复计划测试

- 通读测试
- 结构化演练
- 模拟测试
- 并行测试
- 完全中断测试

了解如何维护灾难恢复计划

- 随着组织需求的变化， 必须对灾难恢复计划进行修改以符合变化的需要

了解通过保险降低灾难影响损失的相关内容

- 承担全部风险往往非常危险，因此我们需要购买保险
- 网络保险(cyber insurance)是一种新型的保险项目
- 业务中断保险(business interruption insurance)


THANK YOU
感谢聆听
学习，为了更好的生活和工作