# 基础安全

## 理解

基础安全对象是基础资产，分为基础资源或基础服务，围绕着资产生命周期展开。

基础资源通常有 服务器，域名等。

基础服务有网络，数据库，管道，OSS仓库等。

基础安全建设中公有云及私有云的异同分别是

异：公有云存在资源过期问题，私有云不存在过期问题。公有云在硬件层没有实现隔离，私有云在硬件层面实现了隔离。私有云可在硬件层面实现安全加固，公有云硬件层面安全是统一的。公有云使用的主机是虚拟化后的主机，网络隔离为逻辑隔离，私有云主机为物理机，需自行建设虚拟化，网络隔离可实现物理隔离及逻辑隔离。

同：在技术体系及管理体系可进行的安全建设都是相同的。如监控，如HIDS，如操作审计，如权限管理。

基础安全中，纯技术体系的内容比较多，效果很显著。管理方面的内容比较少。

落地基础安全建设，安全介入生命周期的管理流程，在应用生命周期的各阶段对其进行安全检查与保护。

体系建设完成后，需要对实际运行效果负责。可以从资产发现时间、安全培训效果、安全事件出现次数、安全检查频率、修复时间、安全流程自动化程度等指标判断薄弱环节。

基础安全包含管理体系，技术体系，运营体系。

理念：微隔离

## 人选要求

基础安全对能力没什么要求，因为变化较少，内容也简单。有经验照搬就行。

经验要求，有经验当然更好，但是没经验也没关系，有能力可以快速上手与学习。

## 落地

基础资产跟服务的梳理：发现所有基础资产跟基础服务。建设资产发现机制跟能力

状态调研：调研安全建设状态，评估完成度，高优先级的东西是否覆盖了。

决策工作内容：做不做，做什么，怎么做

一般是先进行纯技术体系的落地，然后是运营体系，然后是管理体系。

### 技术体系

资产发现

评估检查

隔离划分

渗透测试

安全加固，这部分，大多靠乙方的安全产品，如IDS，IPS，HIDS，网络防护墙，各种硬件盒子设备。

感知

审计

监控

### 安全运营初步建设

安全培训，持续运营，自动化，处理漏洞及问题。积累数据，根据数据持续优化。

### 管理体系

生命周期安全管理：权限、占用

基线设置管理

安全配置

安全培训

## 细节见excel文档