FREEBUF | 企业安全 俱乐部

等保2.0下企业信息安全防护体系建设

何勇亮　高级等级测评师

2019企业安全俱乐部　等保专场

目录

WHO AM I

高级等保测评师

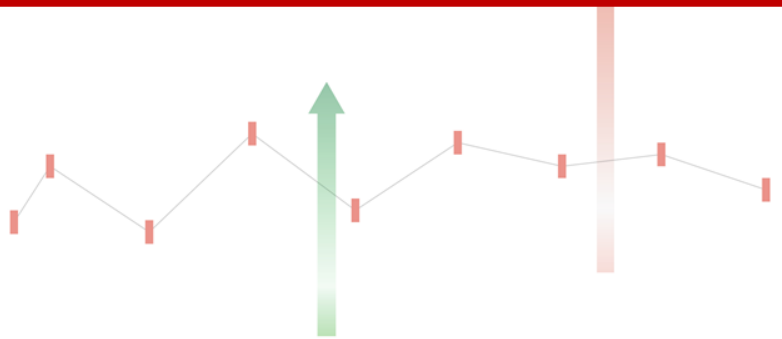
CISP、CISSP、CISAW、PMP

等级保护测评、渗透测试
网络安全咨询、风险评估

Wechat：unicotech

Part 1

网络安全新形势

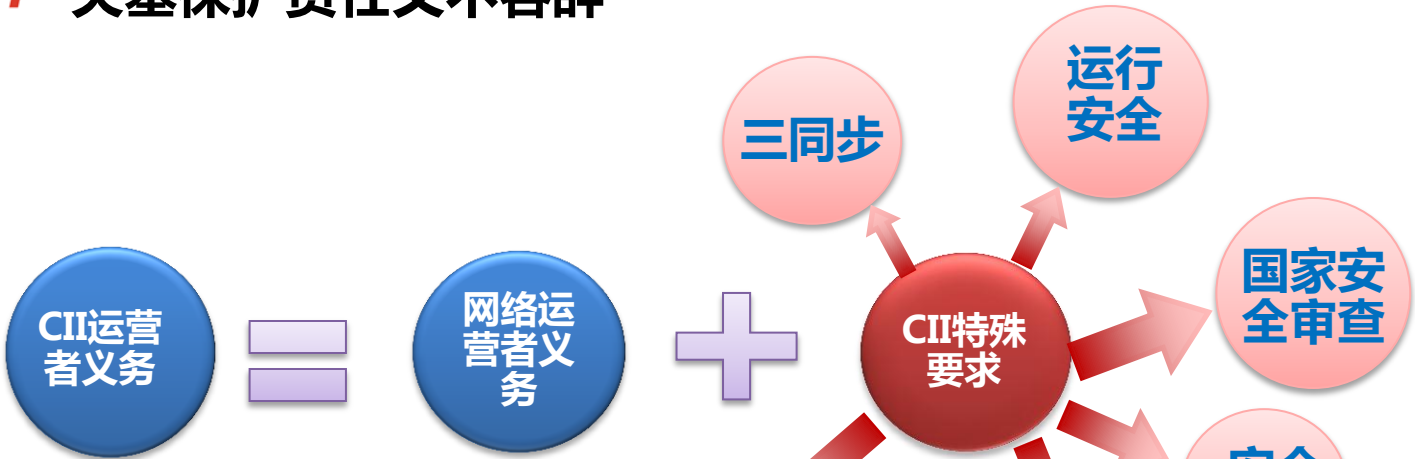


等级保护进入2.0时代

二个全覆盖

1. 覆盖全社会
2. 覆盖所有保护对象

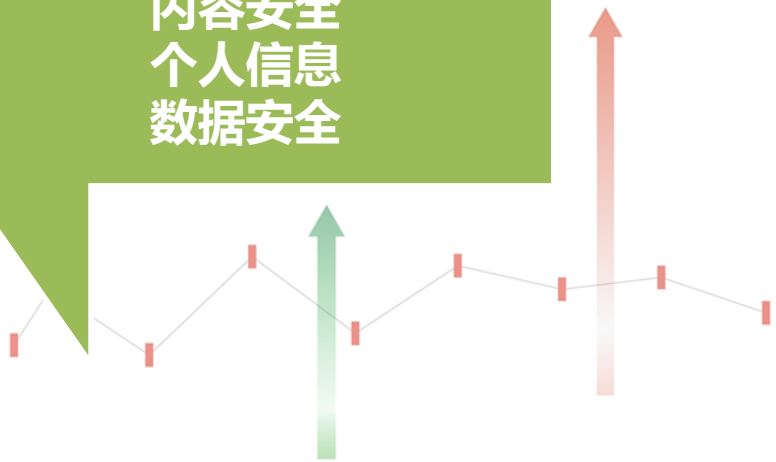
关基保护责任义不容辞


CII运营者义务
=
网络运营者义务
+
CII特殊要求
三同步
运行安全
国家安全审查
安全保密
数据存储
检测评估
监管配合

新技术新应用新风险

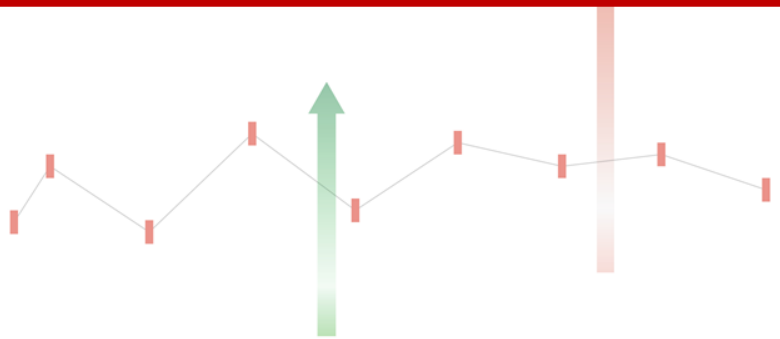
云计算
移动互联网
工业控制系统
物联网
大数据

APT攻击
无线安全
内容安全
个人信息
数据安全

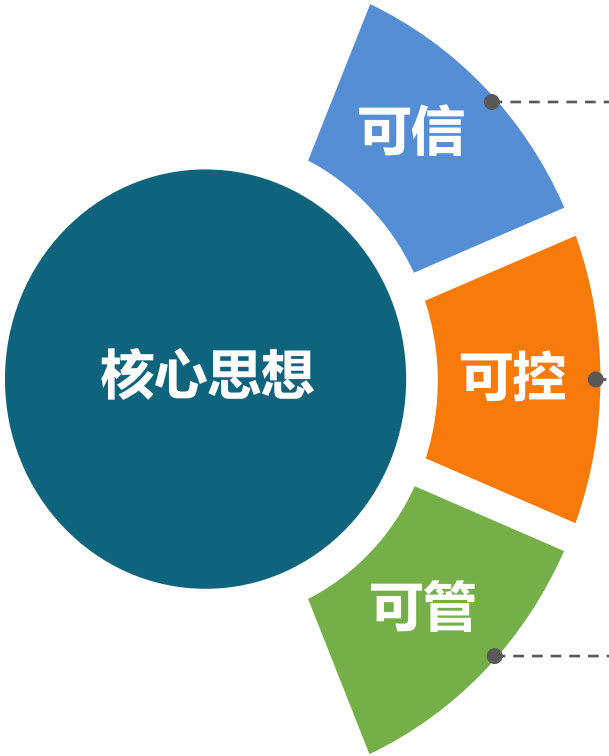


Part 2

等级保护新要求



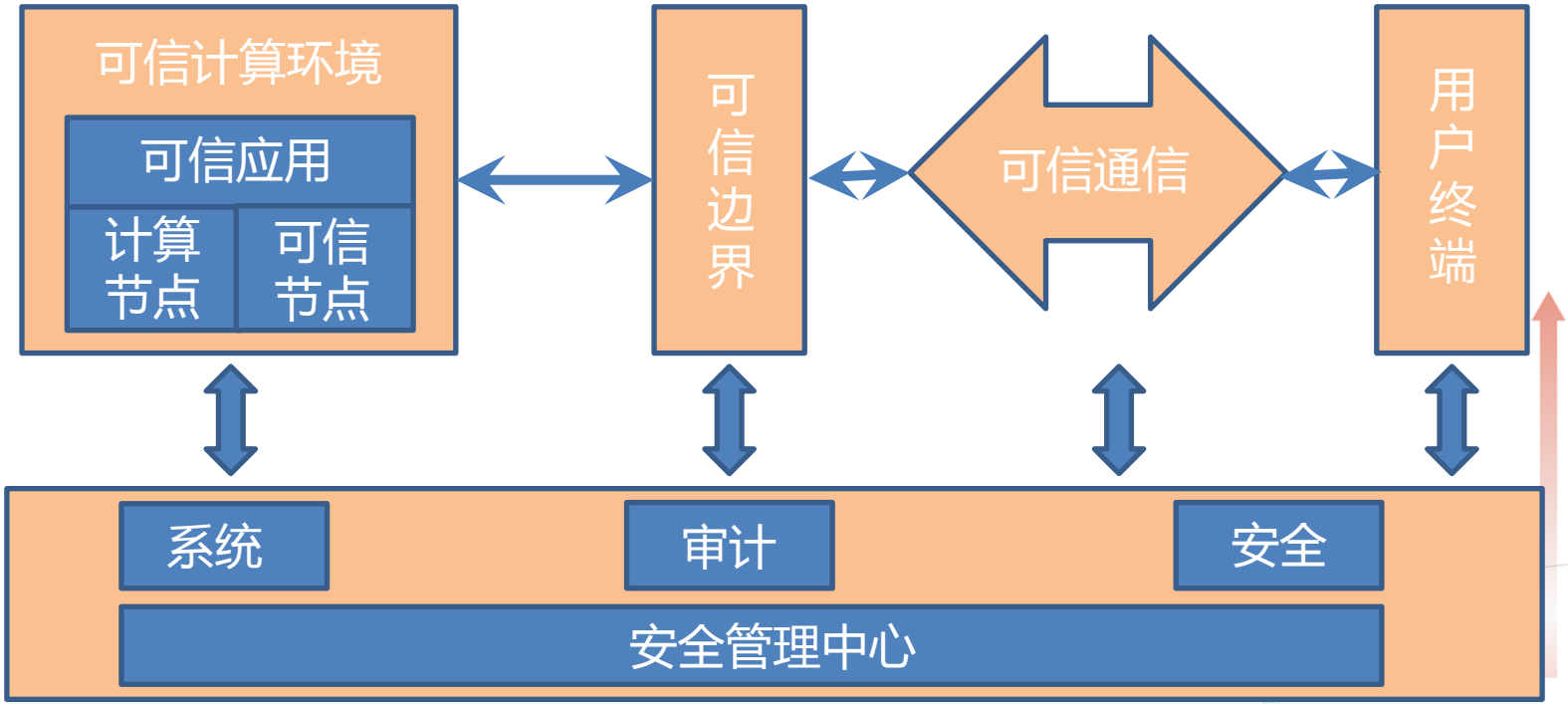
等保2.0建设核心思想



- 以可信计算为基础，构建可信的执行环境
- 以访问控制技术为核心，实现多层防护，纵深防御
- 构建集中管理平台，实现系统、审计、安全的集中管控。

等保技术防护框架

以可信计算为基础构建**多重防护**框架



强化态势感知能力

《习近平在网信工作座谈会上的讲话》

…全天候全方位感知网络安全态势。**知己知彼，才能百战不殆。**

…感知网络安全态势是最基本最基础的工作。

《习近平在国家安全工作座谈会上的讲话》

….加强网络安全预警监测，确保大数据安全，实现全天候全方位感知和有效防护。

安全区域边界

入侵防范：应采取技术措施对网络行为进行分析，实现对网络攻击特别是**新型攻击行为**的分析。

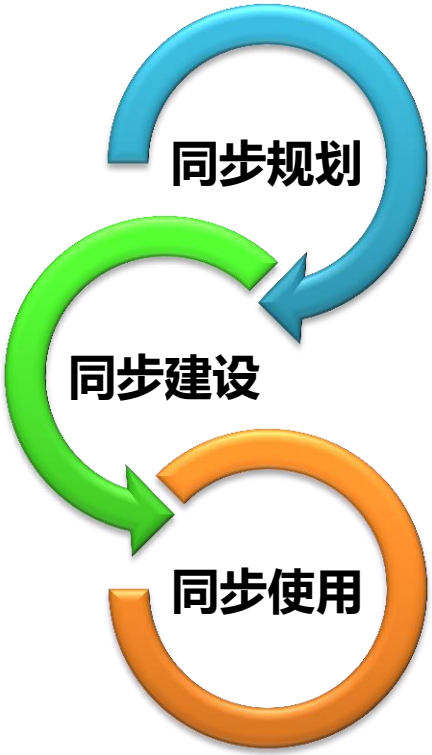
安全计算环境

入侵防范：应能够检测到对重点节点进行**入侵的行为**，并在发生严重入侵时间时提供报警。

安全管理中心

集中管控：应能对网络中发生的各类安全事件进行**识别、报警和分析**。

安全建设三同步



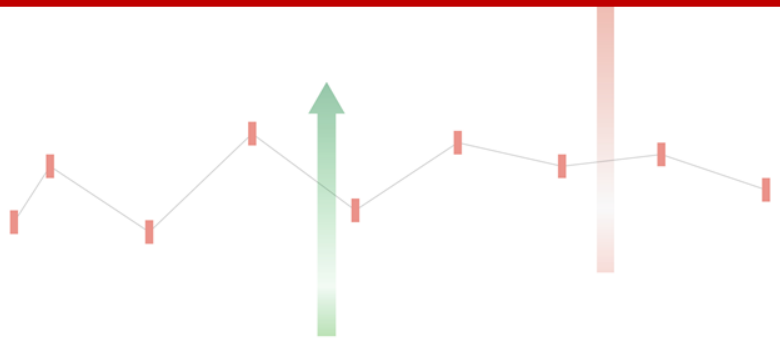
- 同步分析安全需求
- 同步定义安全要求

- 同步设计体系架构
- 同步落实安全措施

- 同步启用安全措施
- 同步运营安全措施

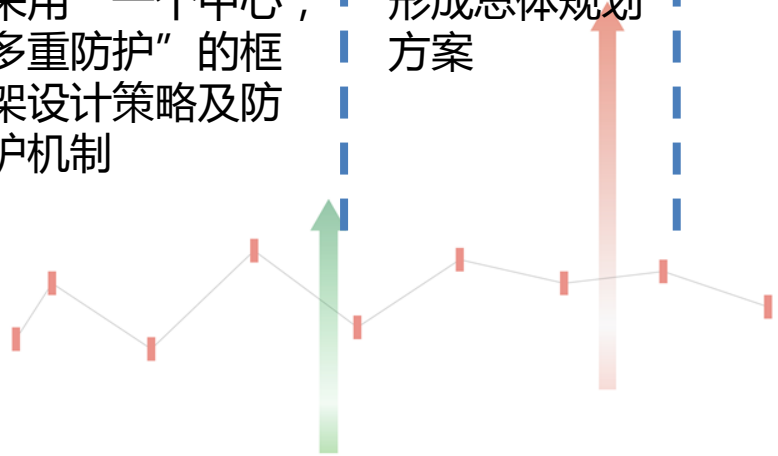
Part 3

从测评角度看企业信息安全体系

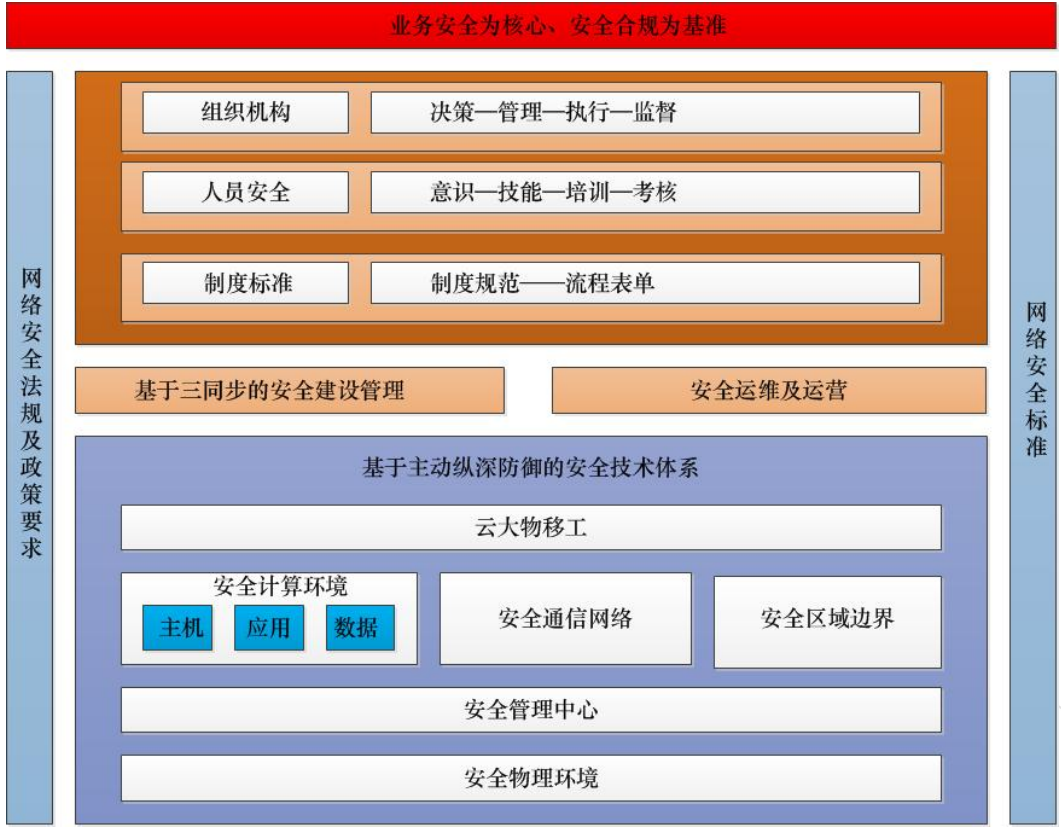


等保体系规划方法论

业务分析	等级确定	需求分析	策略机制设计	总体规划
了解系统特点 梳理业务流程	根据定级指南 确定保护等级	依据业务分析及保护等级确定安全防护需求	依据安全需求，采用“一个中心，多重防护”的框架设计策略及防护机制	根据策略设计，形成总体规划方案



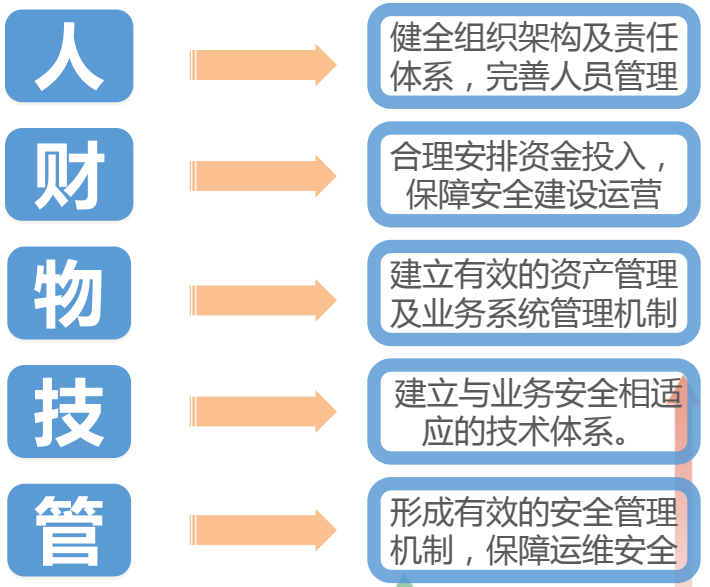
以业务安全为核心的企业防护体系



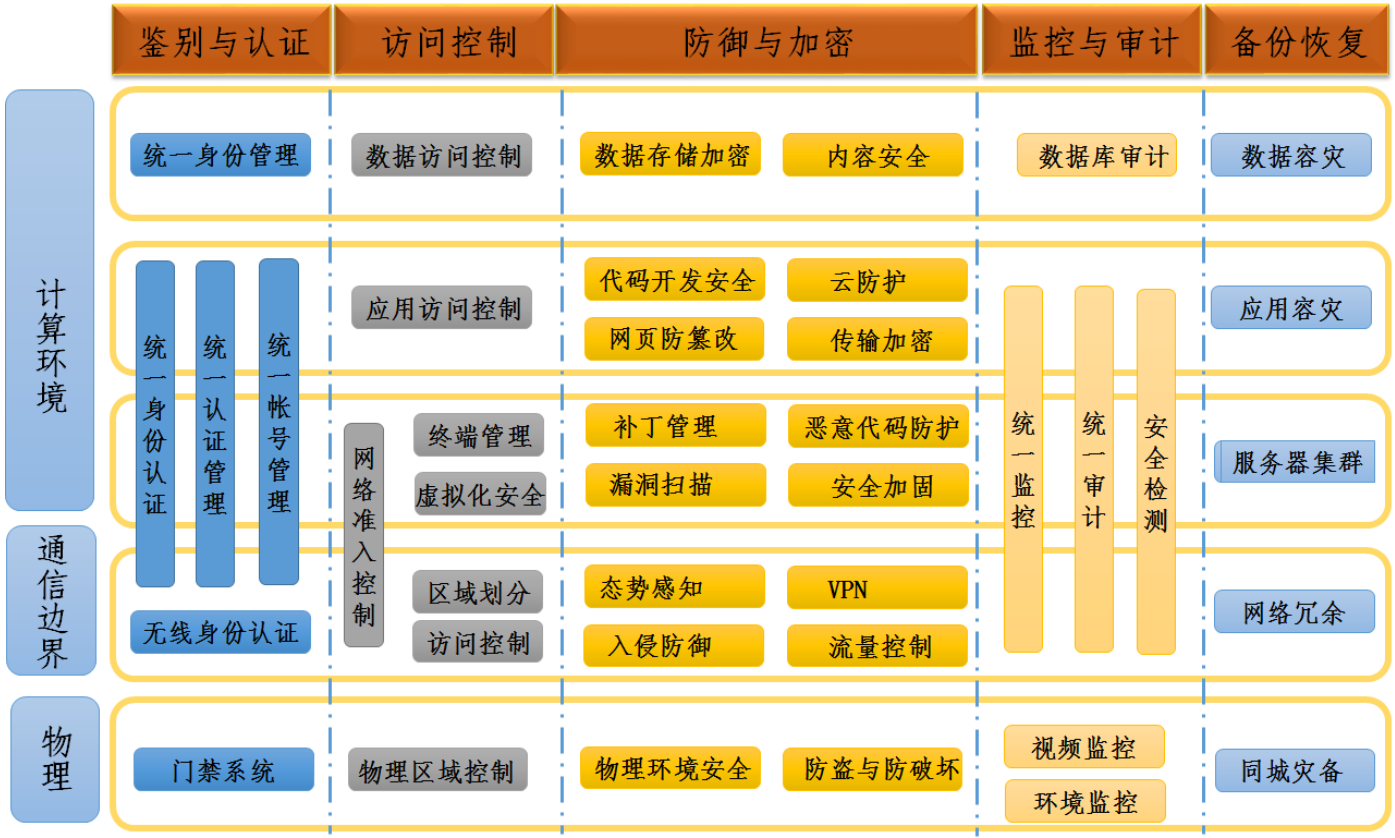
安全管理体系的目标

信息安全的全方位覆盖

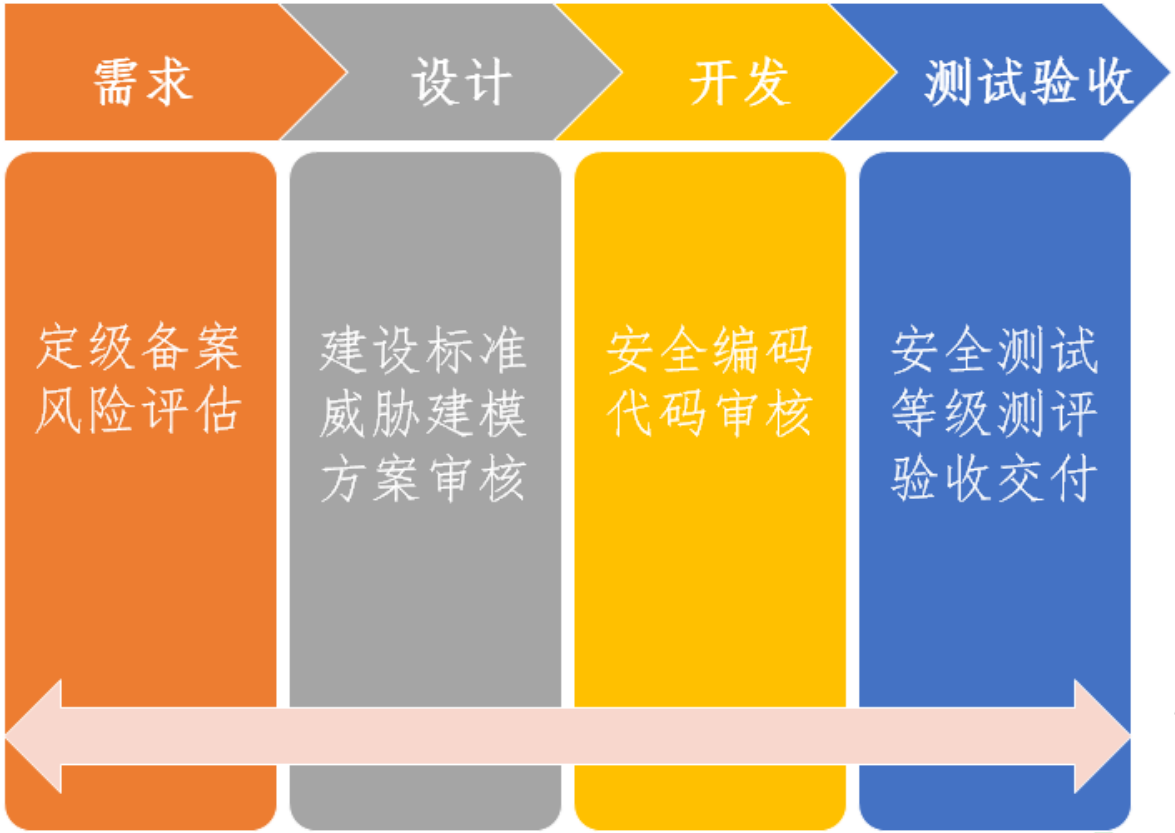
依靠体系的完善和常态化的管理，将信息安全工作落实到安全运维的方方面面



基于主动防御的安全技术体系



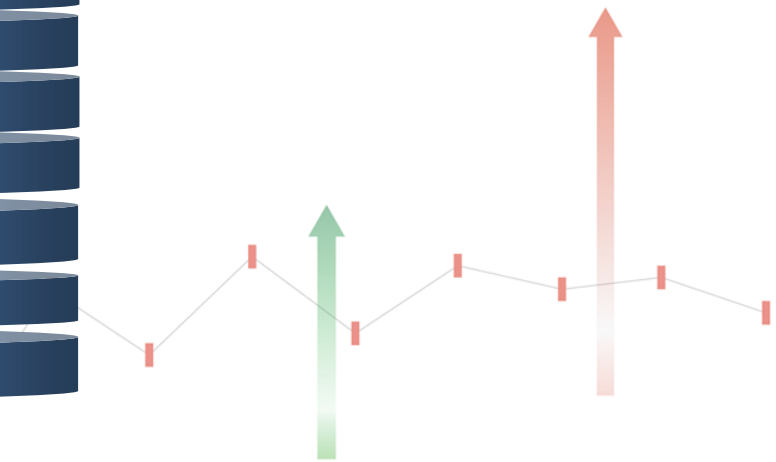
基于三同步的安全建设管理



安全运维运营

运维管理

- 环境管理
- 资产管理
- 介质管理
- 设备维护管理
- 漏洞风险管理
- 网络系统安全管理
- 安全管理中心管理
- 恶意代码防范管理
- 密码管理
- 变更管理
- 备份与恢复管理
- 安全事件处置
- 应急预案管理



安全运维运营


补丁管理
漏洞扫描
信息资产管理
安全基线
重大活动保障
渗透测试
策略管控
安全培训
安全检查
介质管理
日志分析
应急管理
配置管理
漏洞管理
外包运维管理

云计算环境的定级

云计算平台不承载高于其安全保护等级的业务应用系统

云平台责任划分

◆ **基础设施即服务（IaaS）**

云服务商：设施、硬件、资源抽象控制层安全等

云服务客户：应用平台、软件平台、虚拟化计算资源等

◆ **平台即服务（PaaS）**

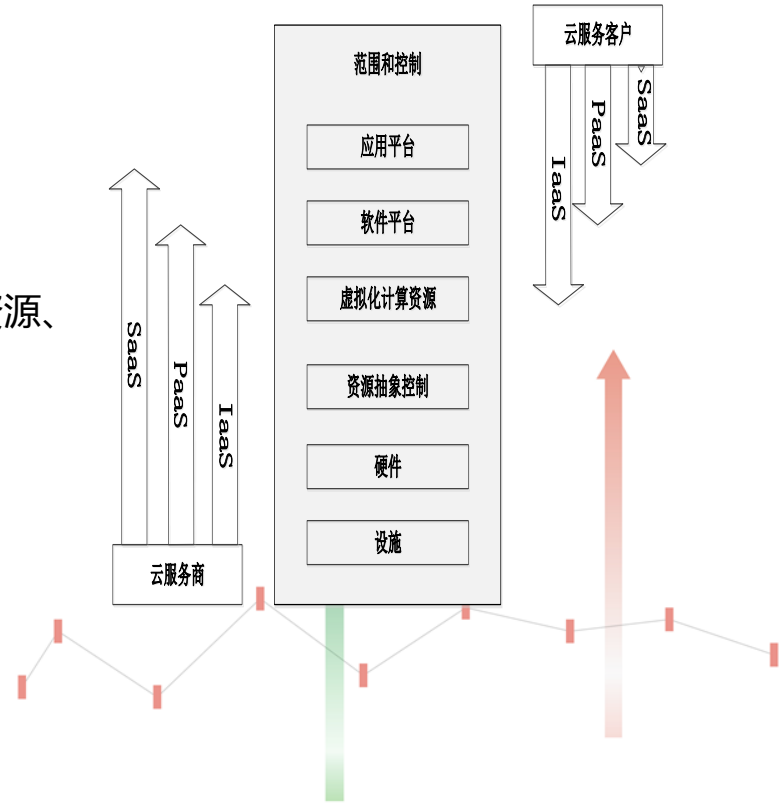
云服务商：设施、硬件、资源抽象控制层安全、虚拟化计算资源、软件平台等

云服务客户：应用平台等

◆ **软件即服务（SaaS）**

云服务商：全

云服务客户：部分应用安全责任、应用的安全使用等



云计算扩展要求

◆ 云计算安全扩展要求的主要思想

云计算平台**自身安全防护要求**

云计算平台**向其上租户系统**提供安全服务能力的要求

针对租户的安全要求

◆ 云计算安全扩展要求的选择

在对**云服务方的云计算平台**上进行等级测评时，应选择全部《安全测评通用要求》+《云计算安全测评扩展要求》 中适用于云计算平台的部分指标。

在对**云租户业务应用系统**进行等级测评时，应选择全部《安全测评通用要求》 和《云计算安全测评扩展要求》 中适用于云租户业务系统的部分指标。

云平台测评要求

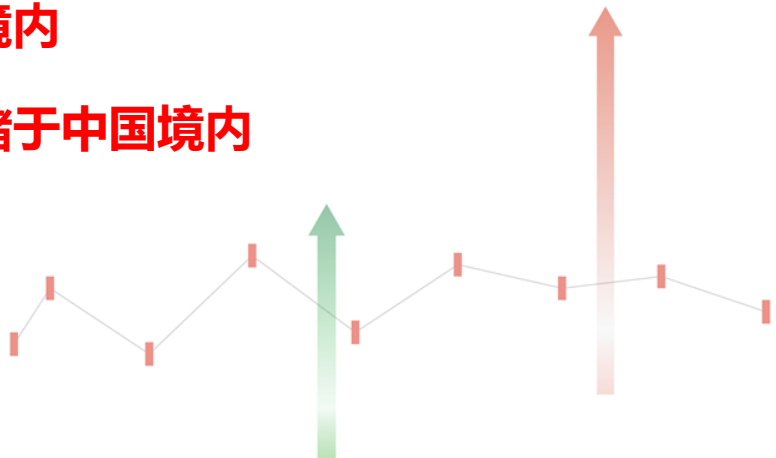
◆ **原则性要求：**

1、云计算平台**不承载高于其安全保护等级**的业务应用系统

2、云计算平台**基础设施必须位于中国境内**

3、云计算平台的**运维地点必须位于中国境内**

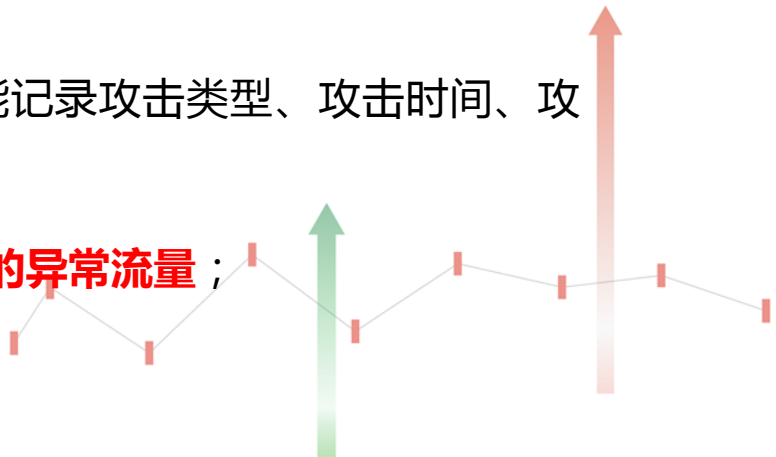
4、**云服务客户数据、用户个人信息等存储于中国境内**



云平台测评要求

云平台自身安全防护要求：

- 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
- 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
- 应能检测到**对虚拟网络节点的网络攻击行为**，并能记录攻击类型、攻击时间、攻击流量等；
- 应能检测到**虚拟机与宿主机、虚拟机与虚拟机之间的异常流量**；

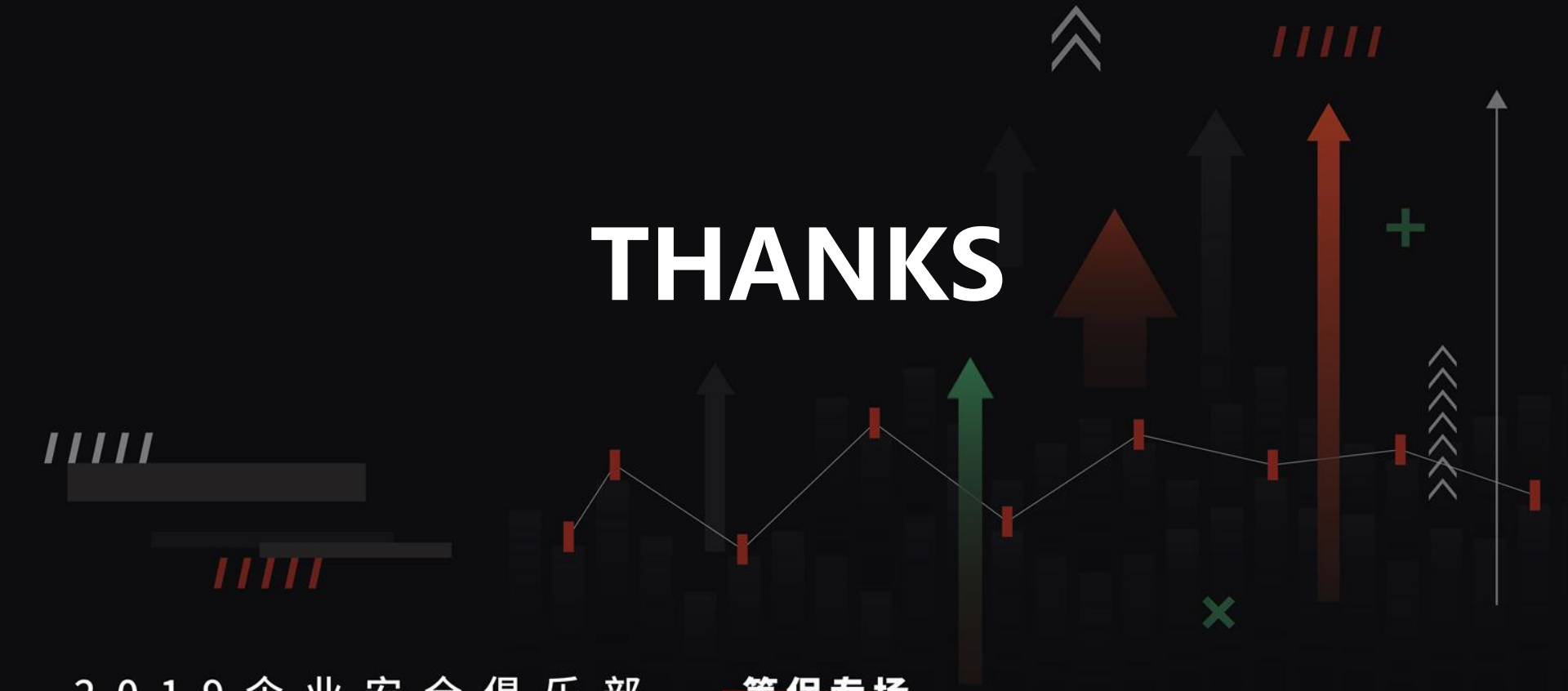


云平台测评要求

向租户提供安全服务的能力：

- 应实现不同云服务客户虚拟网络之间的隔离；
- 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
- 应具有**根据云服务客户业务需求自主设置安全策略的能力**，包括定义访问路径、选择安全组件、配置安全策略；
- 应根据云**服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计**；
- 应根据云服务商和云服务客户的职责划分，**实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测**。

FREEBUF | 企业安全 俱乐部



2019企业安全俱乐部 等保专场