Connect | Educate | Inspire | Secure

等级保护2.0解读及探索

等级保护2.0解读

等级保护基本情况

概念

对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

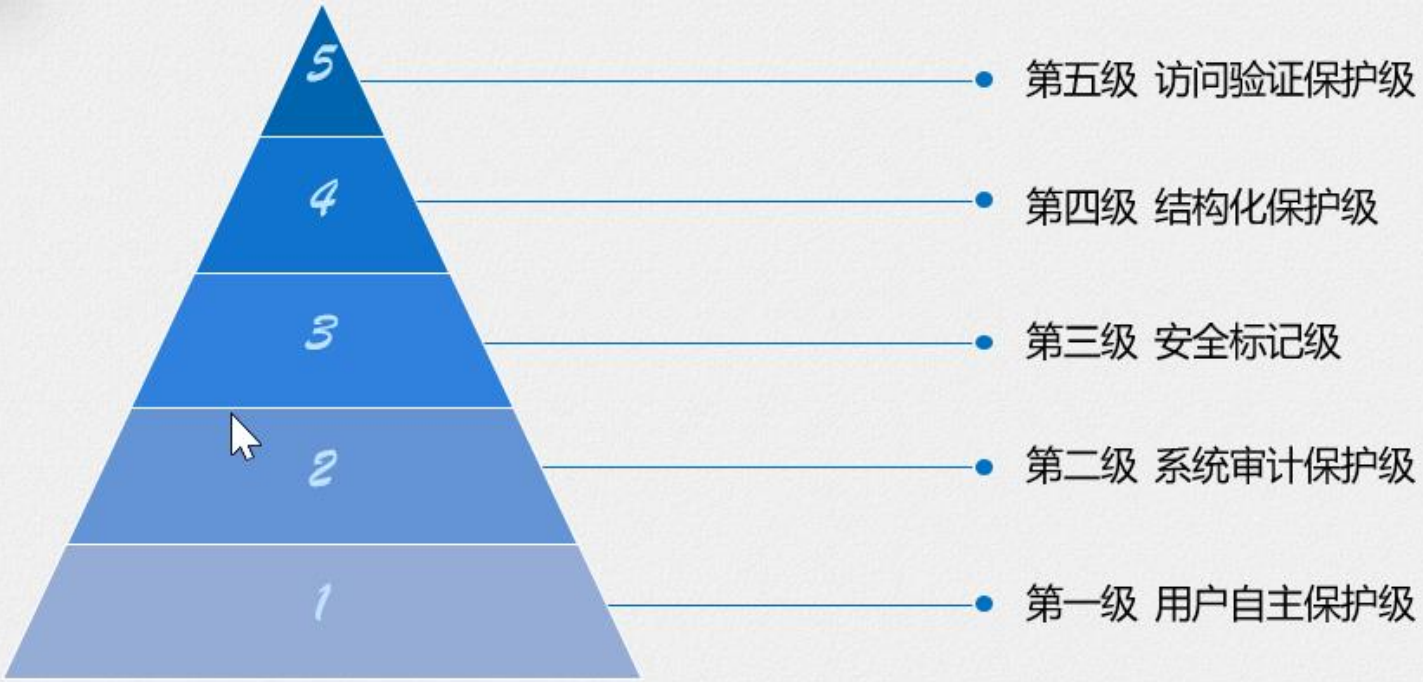
思想

对等级保护对象分等级、按标准进行建设整改、等级测评和监督管理

目标

突出重点，保障重要信息资源和重要信息系统的安全

等级保护基本情况



定级 ▶ 备案 ▶ 建设整改 ▶ 等级测评 ▶ 监督检查

等级保护基本情况

国家信息化领导小组关于加强信息安全保障工作的意见 （中办发【2003】27号）“抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”

01

02

2007年6月，公安部联合相关部门出台了《信息安全等级保护管理办法》（公通字【2007】43号），明确了信息安全等级保护制度的基本内容、流程及工作要求。

03

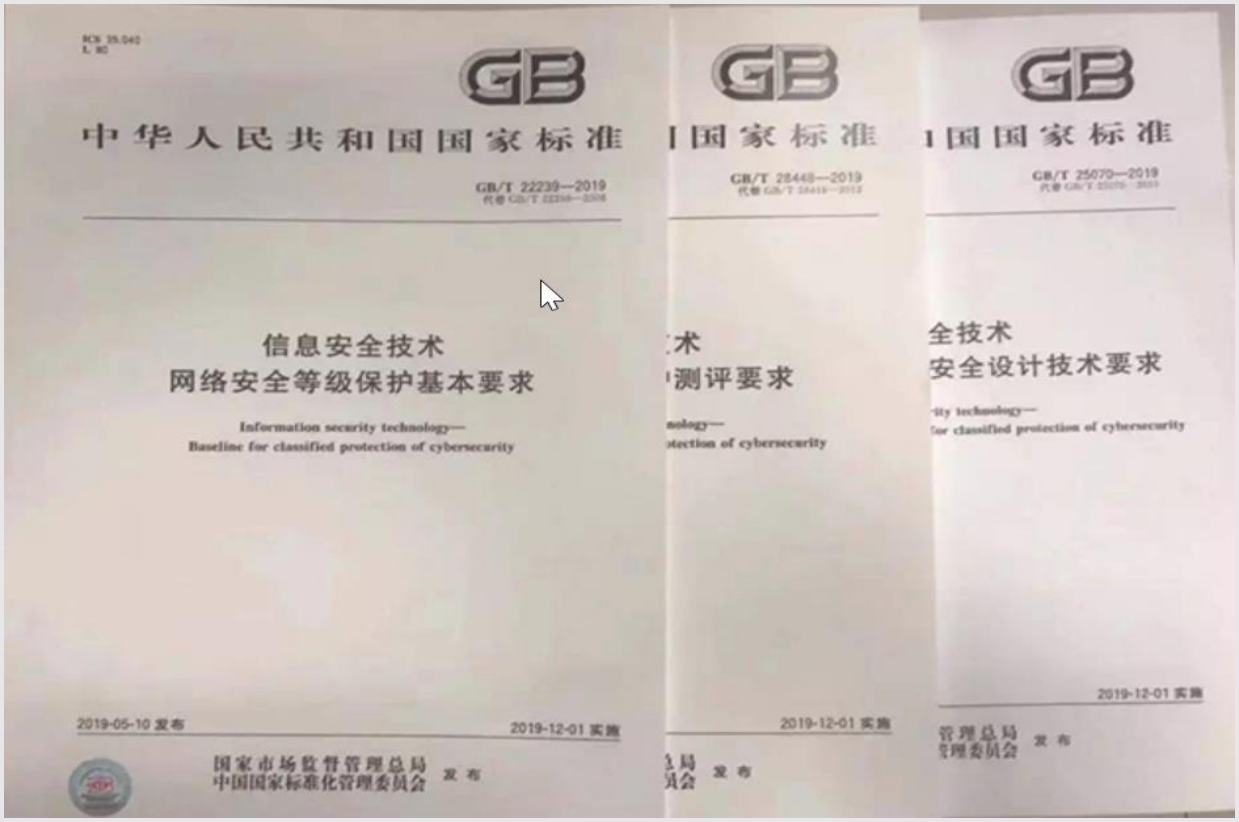
2008年《信息安全等级保护基本要求》及其他配套标准发布。

04

2017年《中华人民共和国网络安全法》发布，二十一条明确提出“国家实行网络安全等级保护制度”

等级保护基本情况

5月13日，国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，通报国家标准制定流程改革的有关情况，同时发布了一批重要国家标准。在网络安全领域，等保2.0相关的《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要求》三项国家标准终获正式发布，新标准将于2019年12月1日开始实施。



等级保护2.0的主要变化

口对应网络安全法

◆ 名称变化

信息系统安全等级保护改为网络安全等级保护，如《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》等；

◆ 新增个人信息保护要求

【个人信息保护】
应仅采集和保存业务必需的用户个人信息；
应禁止未授权访问和非法使用用户个人信息。

◆ 强调日志留存要求

【集中管控】应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

◆ 加强防恶意攻击入侵技术要求

【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网络攻击行为的分析

等级保护2.0的主要变化

口综合各方规范要求

◆ 商用密码

- 融合密码技术要求，如双因子认证、数据完整性保密性要求、通信传输等；
- 【安全方案设计】应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案 设计，设计内容应包含密码技术相关内容，并形成配套文件；
- 【产品采购和使用】应确保密码产品采购和使用符合国家密码主管部门的要求；
- 【测试验收】应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

等级保护2.0的主要变化

口综合各方规范要求

◆ 可信计算

- 【可信验证】可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可 信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

◆ 行业规范

- 【工控扩展】

  涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网；

  工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

  在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。

◆ 电子邮件专项

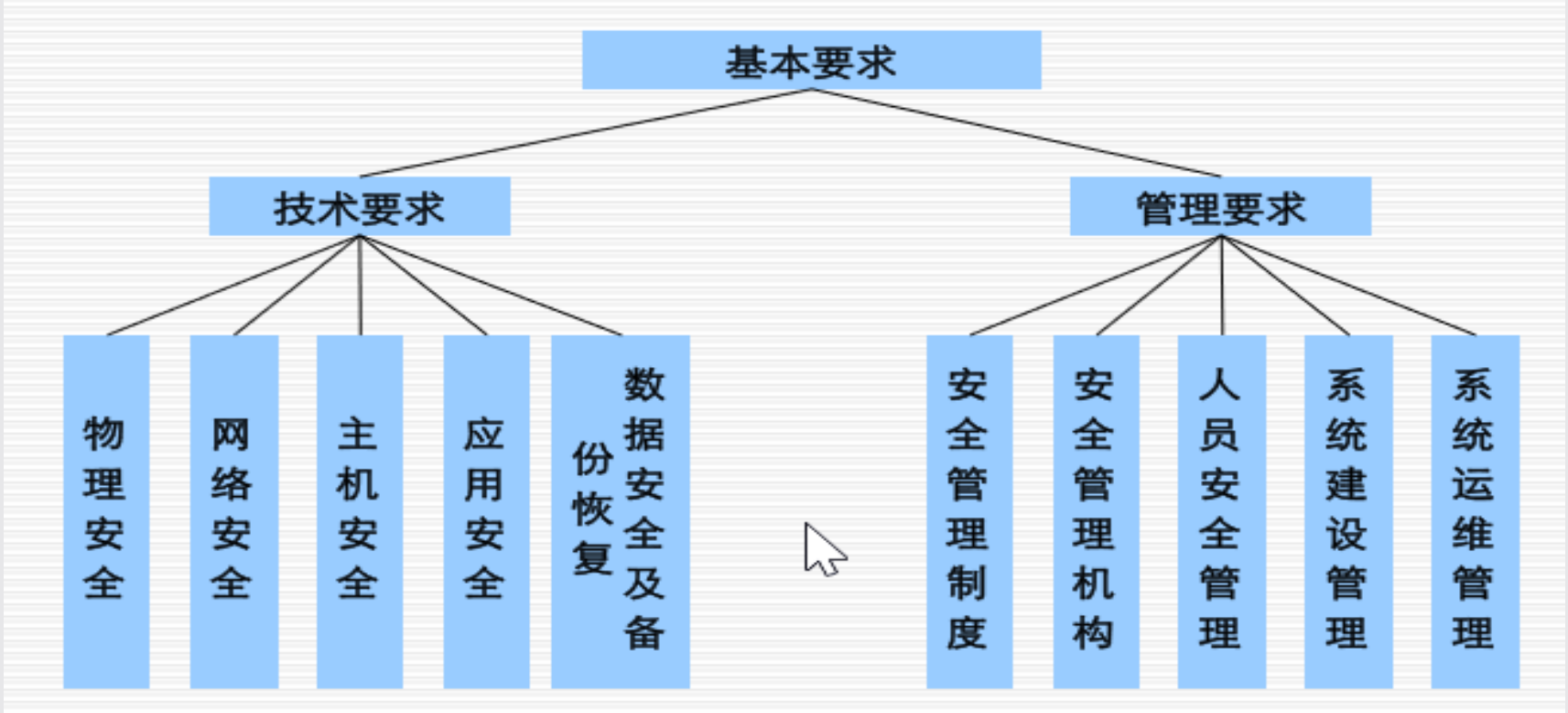
- 【恶意代码和垃圾邮件防范】

  应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机 制的升级和更新。

等级保护2.0的主要变化

口防护模型

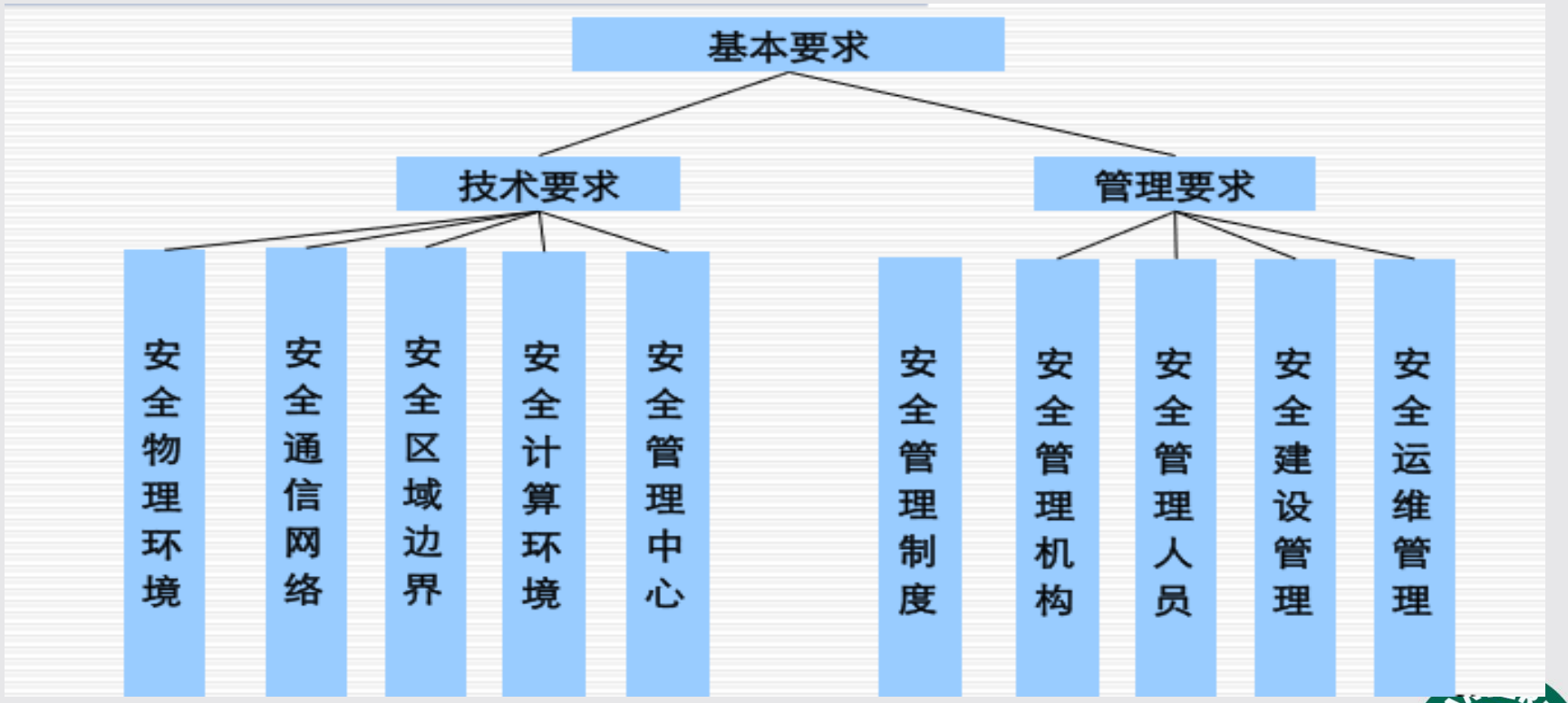
基本要求2008



等级保护2.0的主要变化

口防护模型

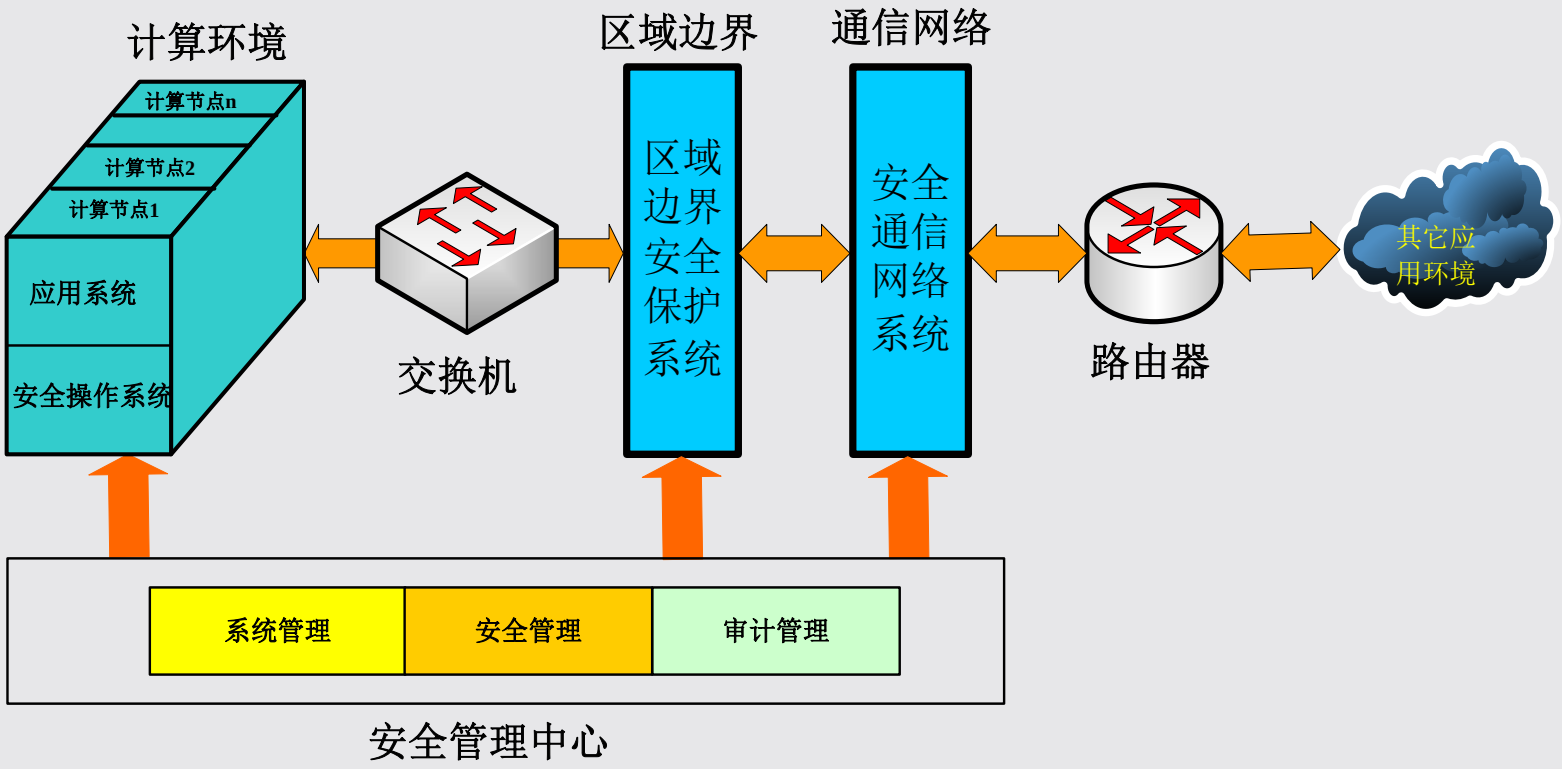
基本要求-2.0



等级保护2.0的主要变化

口防护模型

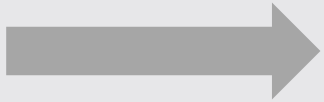
一个中心，三重防护



等级保护2.0的主要变化

口等级保护对象

信息系统



通用信息系统

移动应用互联技术系统

云计算平台/系统

物联网系统

工业控制系统

大数据应用/平台/资源

等级保护2.0的主要变化

云计算扩展要求	移动互联安全扩展要求	物联网安全扩展要求	工业控制系统安全扩展要求
• 云计算安全扩展要求，主要针对云计算的特点特殊保护要求。包含云计算平台自身安全防护要求和云计算平台上租户系统的安全防护能力要求。	• 移动互联安全扩展要求主要针对移动互联部分提出特殊安全要求，移动互联部分通常由移动终端、移动应用和无线网络三部分组成。	• 物联网系统通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。物联网安全扩展要求针对感知层部分提出特殊保护要求，网络传输层和处理应用层使用安全通用要求。	• 工业控制系统安全扩展要求主要针对现场控制层和现场设备层提出特殊安全要求，其他层次使用安全通用要求条款。

等级保护2.0的主要变化

口指标要求实效性优化

口 物理环境

- 取消原机房出入口专人值守要求，改为配备电子门禁系统；
- 弱化原防盗报警系统的要求，有专人值守的视频监控也可以；
- 取消原建立备用供电系统的要求。

口 区域边界

- 新增对无线网络的使用要求，要求通过受控的边界设备接入内部；
- 强调使用“白名单”方式设置访问控制规则；
- 新增对内部网络攻击行为的检测限制要求；
- 增加可信验证要求，要求计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

等级保护2.0的主要变化

□合规+有效是网络安全的主题

□ 网络安全必须依法合规

●网络安全法、密码法、以及相关具体条例将陆续出台；

●网络安全主管部门、行业主管部门监督检查力度不断加大。

□ 网络安全必须防护有效

●新技术、新应用背景业务发展必须依托网络安全的有效保障；

●必须能有效防范网络入侵、网络攻击等安全威胁；

●在面对如0day漏洞、APT攻击等新型网络攻击时需要确保安全风险可控；

网络安全问题分析

当前网络安全现状

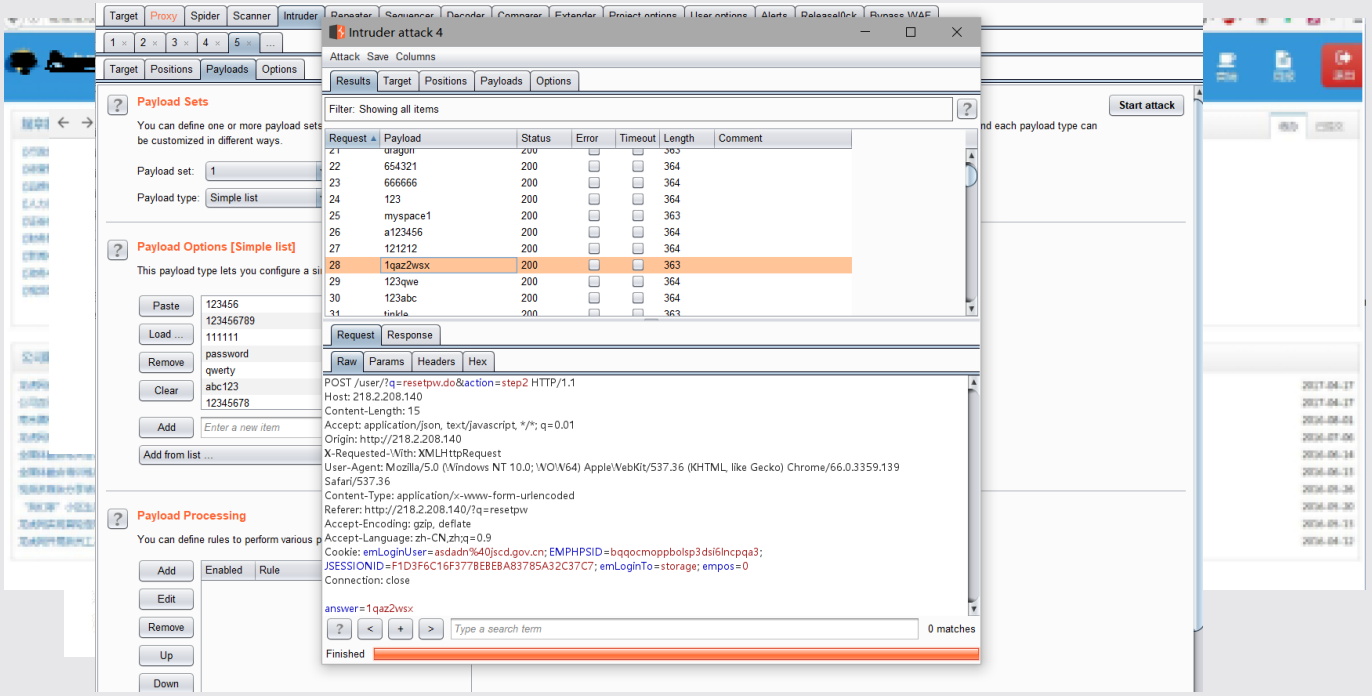
- 防火墙、入侵监测、病毒防范俗称“老三样”仍是主角
- 封堵查杀，疲于应付式地找漏洞补漏洞
- 总是在被入侵后才知道，缺乏对安全威胁的感知能力
- 尤其在“重点安全保障”的特殊时期，“封停并转”是实际应对主要措施
- 简单得出七分管理、三分技术的结论，网络安全工作一直处在被动的状态
- 部分安全厂商对网络入侵技术、网络攻防对抗的多样性、动态性了解不足，理论、方法以及实践跟踪式的居多
- 由于网络安全专业性强、涉及知识面广等原因，单位自身很难培养出专业的安全保障团队

网络安全之木桶理论

木桶理论也可称为短板效应，一只木桶能盛多少水，并不取决于最长的那块木板，而是取决于最短的那块木板。

在“木桶理论”指导下，网络安全工作必然是围绕漏洞的修修补补，应该说这种方式是最低效的，所以也很难改变安全防护的被动状态。

实例分析-弱口令



弱口令：弱口令是最经常被利用的安全漏洞，但其危害结果是显而易见，完全不设防。一般通过猜解和口令爆破即可造成控制设备、修改应用功能、上传恶意文件以及部署恶意程序等危害。

实例分析-弱口令

- **更改口令的长度、复杂度**

不易记忆，不便于日常操作；

大量撞库信息为口令爆破提供丰富的字典库，据统计重合率达70%以上；

- **通过密码工具生成更高复杂度的口令**

由于实在不便于记忆，实际一般出现又更改为便于记忆的口令；

密码管理工具一旦被破解，后果不可想象；

- **增加口令复杂度检测功能**

通过中间截获、键盘记录等手段恶意获取；

实例分析-struts漏洞

Struts2漏洞： Struts2漏洞被业内戏称为“万年漏洞王”，从2013年初始漏洞公布后，至今保持平均2个/年的漏洞曝光速率。每次只要漏洞一公布，马上掀起一波入侵高潮！

实例分析-struts漏洞

- 安装补丁、部署边界安全设备均是基于关键字的拦截

① <param name="excludeParams">dojo\..*</param>

② <param name="excludeParams">dojo\..*,^struts\..*</param>

③ <param name="excludeParams">dojo\..*,^struts\..*,^session\..*,^request\..*,^application\..*,^servlet(Request|Response)\..*,parameters\...*</param>

④ <param name="excludeParams">^dojo\..*,^struts\..*,^session\..*,^request\..*,^application\..*,^servlet(Request|Response)\..*,^parameters\..*,^action:.*,^method:.*</param>

木桶理论的局限性分析

□ 很难确定系统存在哪些短板

IT系统不能穷尽所有逻辑组合，必定存在逻辑不全的缺陷和漏洞；

有些漏洞很难发现，如ODAY漏洞、有些攻击特征很难被匹配，如CIA HIVE武器库、APT攻击；

□ 当前漏洞可能被利用或产生新的风险

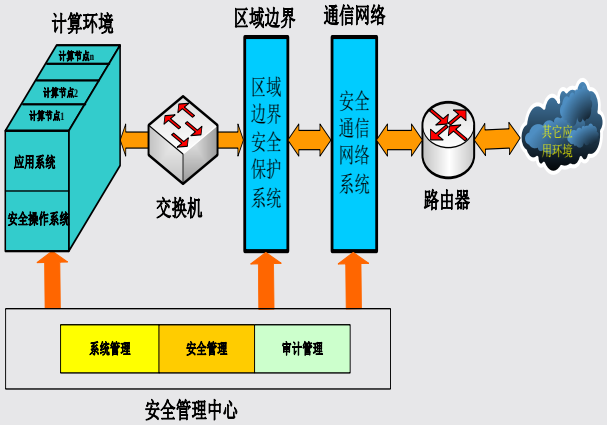
安全漏洞总是先于补丁出现，恶意攻击者可能已完成入侵活动；

有些漏洞的修补可能导致业务系统的异常，甚至产生更大的风险；

□ 很难主动、有效把控安全风险

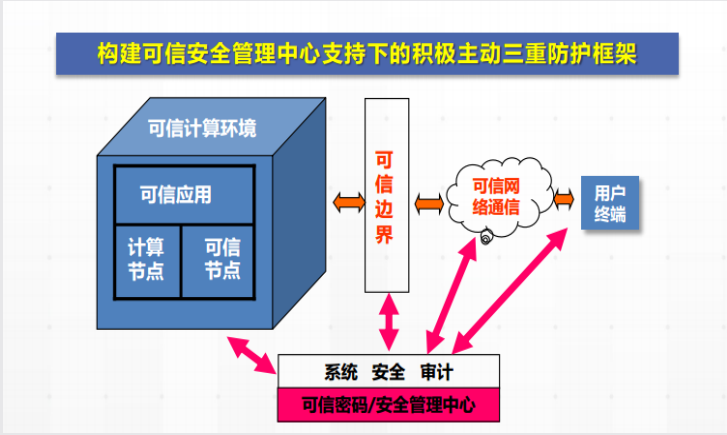
安全威胁作用于系统资产的脆弱性产生安全风险事件，由于漏洞的不确定性，以漏洞为核心开展安全工作相当于以未知条件求得解集的伪命题，必然无法把控重要安全风险。

网络安全防护的技术参考模型



基于先验知识的防御模型

- 基于先验的攻击特征的识别、匹配、防御等技术和模式均可归属此类；
- 工作上是围绕漏洞的发现、修补、防御等展开，本质上是基于木桶理论的防护模型；
- 通常具备业务无关性特点。



基于可信计算的防御模型

- 可信计算的核心概念：可信根和可信链，主要基于密码技术实现；
- 基本前提是认为在当前的技术框架下，人为设计的软件、硬件、网络、平台等存在缺陷和错误是一种常态，很难从根本上去避免。
- 在该前提下可信计算、拟态安全是区分与先验知识的安全模型。

基于先验知识的防御模型分析

条件不足

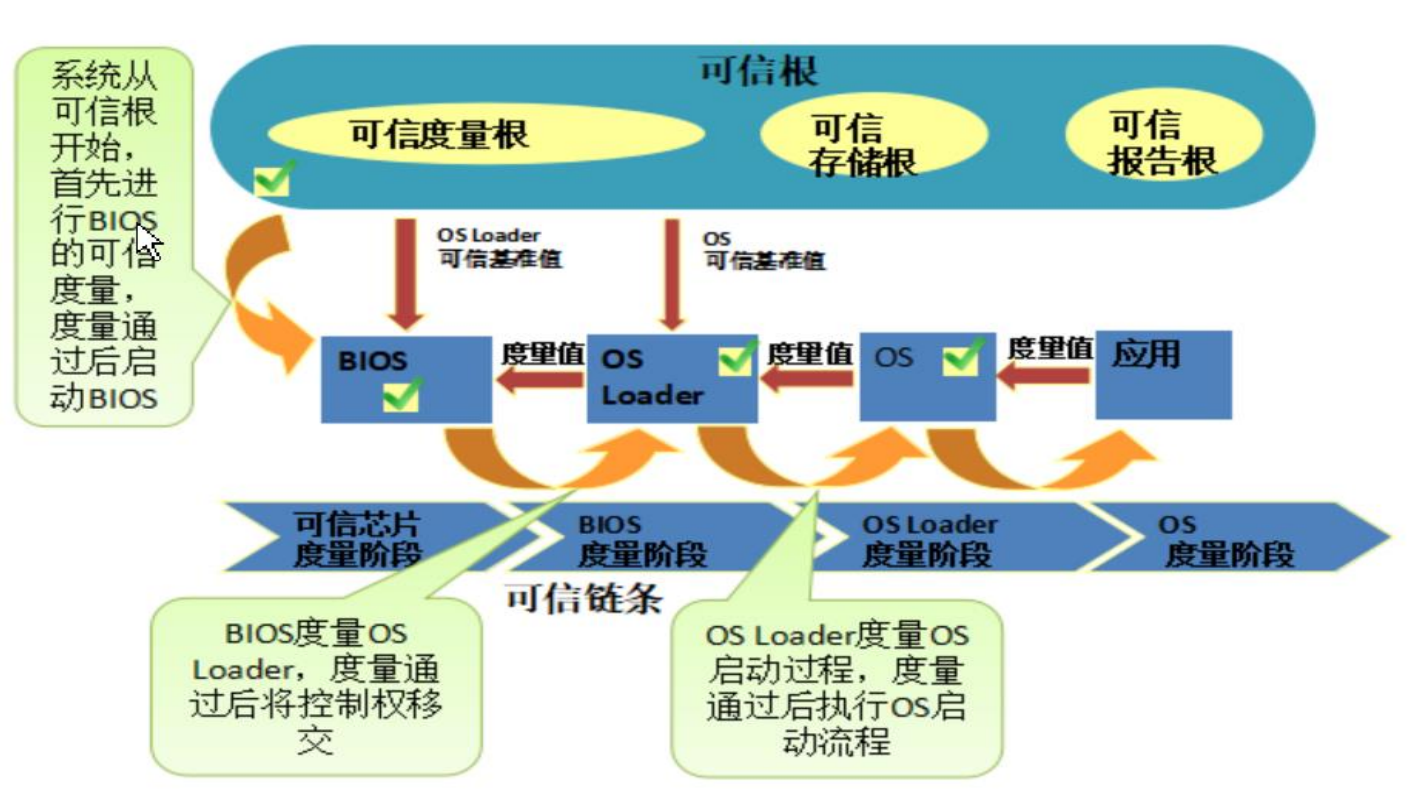
- 在当今的技术能力下，信息系统设计与实现中的漏洞是无法避免，采用国外怕后门，不采用先进性、成熟性无法保证；
- 系统后门的易安插性，产品的设计者可以透过产品的设计链、工具链、制造链、服务链等多种环节，有意地植入各种隐蔽的恶意后门；
- 在新的安全威胁方式面前，可能所有的防御手段都会过时。

效果不好

- 安全漏洞总是先于补丁出现，恶意攻击者可能已完成入侵活动；
- 在0day、APT、侧向攻击等新型网络攻击面前应对乏力；
- 由于业务无关特性，区域边界无法识别业务层面的逻辑漏洞。也无法实现风险事前事中事后的全过程管控；

CHARTERING (ISC)² CHAPTER

基于可信计算的防御模型分析



- 高度集中的可信根、集中签名机制的需要慎重，区块链的应用发展是很好的例子；
- 需要形成全产业链的长期系统工程，在技术研究、产品开发及推广应用有待时日。

回归风险管理看网络安全

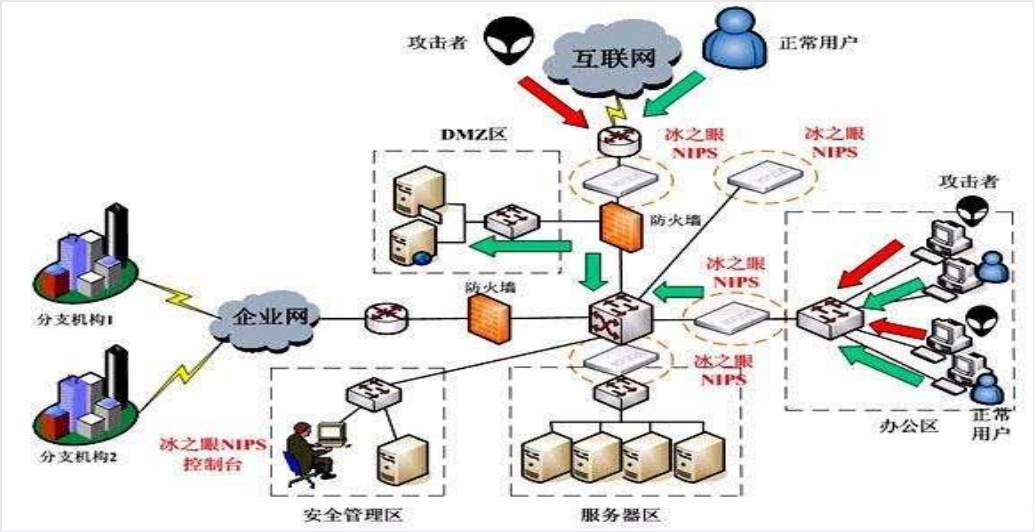
风险管理

- 风险管理是通过风险识别、风险控制等措施将风险可能造成的不良影响减至最低的管理过程。
- 风险管理的目标就是降低风险事件的发生概率和危害程度。

构建网络安全防护模型的探索

面向威胁场景实现主动防护

- 根据系统应用场景，最小化系统的受攻击面，确定可能存在的入侵途径；
- 针对不同入侵途径，通过威胁建模的方式分析和确定攻击类型和方式；
- 在威胁途径、威胁方式确定的情况下实施针对有效的防护措施。



构建网络安全防护模型的探索

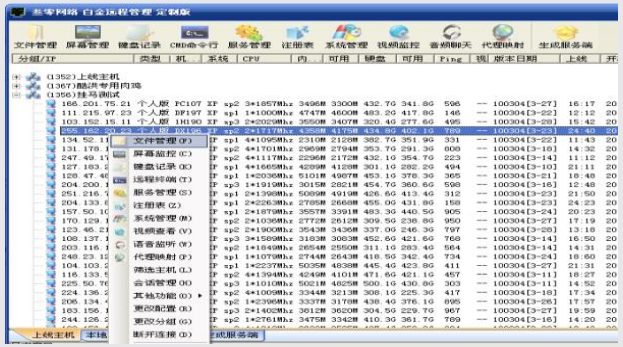
2、面向重要资源实现重点防护

- 通过系统业务特性的分析，识别系统的重要保护对象，如：敏感数据、系统服务、重要用户等；
- 保护对象确定后，分析对象的保护需求，如数据的机密性、完整性；服务的可用性、抗抵赖性；用户的真实性、可控性等。
- 采用相适应的密码技术满足对象的保护需求。

构建网络安全防护模型的探索

3、面向风险全过程提升防护能力

风险事件全过程管控



事前 全面、准确地风险识别、监测预警

事中 针对、有效地定位风险、控制处置

事后 快速、规范地处置风险、总结优化

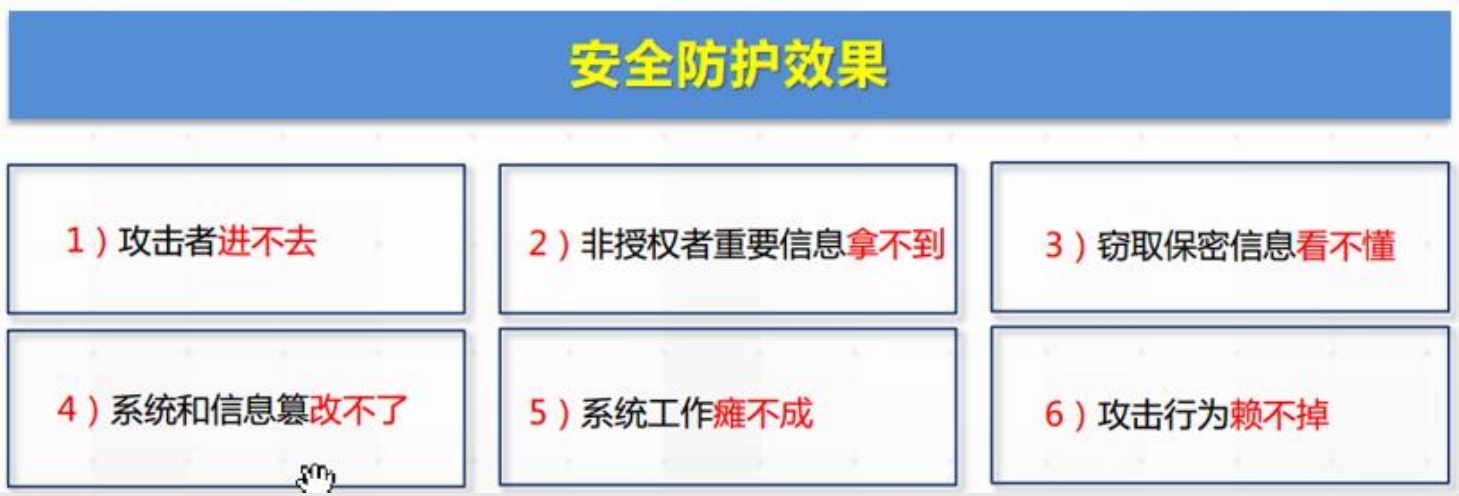
构建网络安全防护模型的探索

4、有机融合合规要求促进良性持续发展

依法合规是网络安全的基本原则

- 网络安全法要求；
- 等级保护中相关要求；
- 密码法安全要求
- 行业规范要求....

构建网络安全防护模型的探索



- 通过面向威胁场景主动防护实现主动、自适应的安全防护；
- 通过保护对象保护实现重要重要资源对攻击的自免疫；
- 传化面向漏洞为面向风险，从全过程风险管控角度提升防护能力；
- 有机融合实现依法合规的要求规避责任风险，形成良性可持续工作机制。

网络安全的探索与实践

专业网络安全服务体系的探索与实践

□ 面向业务创新安全风险的识别和分析方法

传统的安全风险理论指导下的安全服务由于重物理资产轻数字资产、重漏洞轻威胁等问题很难满足当前信息安全的迫切需求，所以需优化完善当前的安全风险管理的理论和方法，这也是体现安全服务价值的真正基础，是区别于其它安全产品、服务的核心。

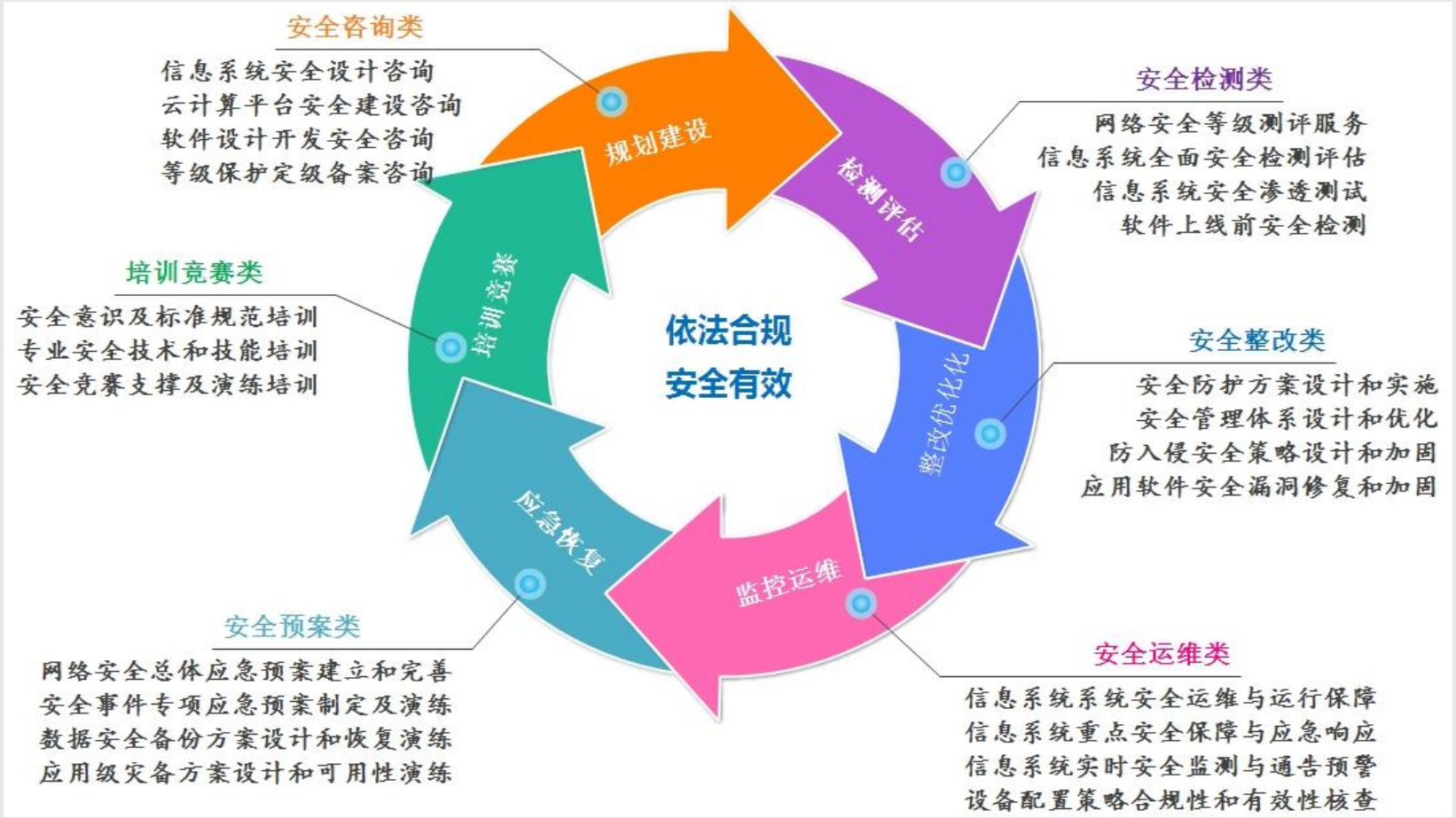
□ 面向工作构建了全生命周期的安全服务体系

单功能、专业化的安全服务或产品只能解决某一类问题，但网络安全问题是牵扯信息系统各个技术和管理层面的综合性问题，所以无法真正满足客户安全需求。加上一般政府企事业单位缺乏专业安全人才的培养环境，所以专业网络安全服务体系也是专业安全服务能力的交付。

□ 面向安全目标定义安全服务交付的质量标准

围绕用户安全目标，融合相关安全合规要求，从技术规范、支撑系统、过程控制以及结果展现统一规范服务的全过程，通过服务标准化、规格化工作确保用户的安全目标保质保量地达成，保证用户安全收益，体现安全服务价值。

江苏金盾专业网络安全服务产品体系



专业定制化安全检测评估服务

口 服务描述

依据创新构建的安全防护模型而建立的安全服务，通过威胁建模和业务特性分析建立适合于客户实际安全需求的检测评估指标，依托专业的服务支撑系统和成熟的实施过程控制方法确保检测验证的全面性和准确性，检测结果可直观反映出风险全过程管控中能力的不足，为客户整体掌握系统安全状况以及安全整改和安全措施的落实提供支撑和依据。

口 服务优势

- 创新了系统调研和安全防护需求的分析方法和手段；
- 建立适合于业务实际情况的风险管控能力的检测评估指标；
- 开发和集成专业的检测系统和工具支撑服务的实施；
- 为客户提供覆盖风险全过程的整改建议和合理的整改措施；
- 规格化了服务内容，可选择适合实际的多种规格的服务产品。

口 服务收益

- 有机融合合规要求，主动适应网络安全规范的调整和变化
- 有效防护网络攻击入侵，甚至包括0day漏洞、APT等新型网络攻击
- 将被动应付的安全工作状态转化到主动、自适应的工作状态；
- 全面发现和整体掌控系统防护能力的情况和安全态势，正确指导网络
- 安全的规划和整改建设工作。

专业网络安全渗透测试服务

口 服务定位

从面向威胁视角通过安全建模的方式分析系统实际存在的安全威胁场景，并对可能存在的威胁途径、威胁方式进行全覆盖式的测试验证，测试结果不但能明确反映出当前系统面临哪些方面的威胁、哪些威胁可被利用、哪些威胁可被抵御，而且对应安全风险事前、事中、事后全过程提出整改建议措施。解决了传统渗透测试的深度和广度不明确、整改建议碎片化、片面化等问题，真正为用户安全问题的妥善解决提供必要依据和技术支撑。

口 服务优势

- 依据实际安全威胁场景建立测试用例，确保安全测试的完备性；
- 区别传统渗透测试发现漏洞、利用漏洞、扩大入侵收益思路，从方法层面解决测试广度和测试深度的问题；
- 技术规范、工作规范、支撑系统的集成以及完善的实施风险的规避机制确保实施质量；
- 整改建议具备整体性和可操作性，改变对漏洞修修补补的被动工作状态；
- 规格化安全服务内容，可选择适合实际的多种规格的服务产品。

专业安全监测与保障服务

口 服务定位

江苏金盾安全监测与保障服务是集安全检测、安全加固、安全监测以及安全应急处置于一体的综合化安全服务产品，能够有效防止网站被篡改或仿冒、挂马或远程控制、用户敏感数据泄露等网络攻击入侵行为，通过实时安全监测第一时间定位和处置网站可能发生的异常事件，有效抑制安全事件的危害影响，尤其适用于重大活动期间网站系统的安全保障，切实提升单位网络安全的自主可控和安全保障能力。

口 服务优势

- 对可能存在的威胁途径、威胁方式进行全覆盖式的测试验证；
- 同时还包括入侵痕迹深度检测，排查系统可能存在的入侵后门；
- 对于存在高危漏洞的应用软件，可不需要通过更新源代码或增加安全设备实现安全漏洞的加固；
- 实时入侵监测全面发现和准确定位设定监测对象的各类异常行为，甚至包括新型木马病毒均能第一时间发现并预警，能够解决传统安全监测系统无法发现的入侵行为；
- 重大活动时期提供实时监测、分析、应急事件处置以及专人值守服务；
- 规格化安全服务内容，可选择适合实际的多种规格的服务产品。

谢 谢!