“持续合规，安全有效”夯实金融科技安全防线

深信服科技

SANGFOR SECURITY
深信服智安全

企业级网络安全

2000
年成立

A股上市企业
股票代码300454

SANGFOR CLOUD
信服云

云计算+IT基础设施

50+

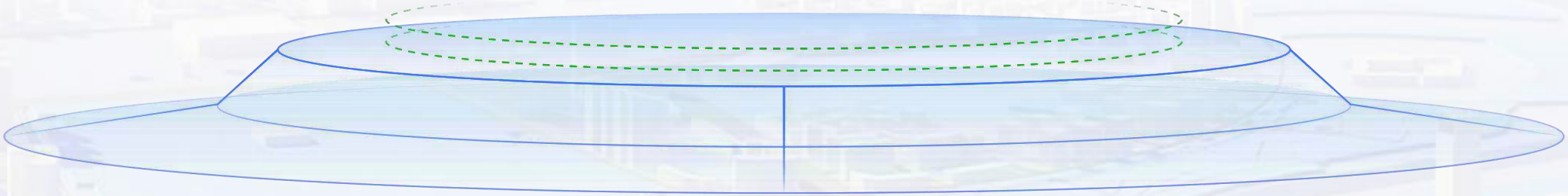
分支机构
分布在全球十余个国家和地区

SUNDRAY
信锐技术

数据通信+物联网

9000+

员工规模



20余年持续创新
发展迅速

坚持研发投入，持续自主创新

01

5 大研发中心

北京 / 深圳 / 长沙 / 成都 / 南京

02

20%+

营业收入投入研发

03

40% 研发人员

30% 硕博学历

人力资源部和社会保障部
博士后科研工作站

国家发展和改革委员会
国地联合工程实验室

国家网络应急技术处理协调中心
网络安全应急服务支撑单位

国家企业技术中心

广东省云安全关键技术企业
重点实验室

中国网络安全龙头厂商

23年安全基因
领先定义安全理念&多款安全产品

国内首创安全垂直领域大模型--安全GPT
创新推出“平台+组件+服务”的安全建设新范式
国内率先率先落地SaaS XDR
率先实现SASE、MSS在国内的落地
国内率先发布下一代防火墙、云安全资源池
定义了上网行为管理产品品类
全球率先推出IPSec/SSL二合一VPN网关

引领行业，深度参编安全国标&行标

长期以来深信服充分发挥自身技术势能，深入参与信息安全标准的研究工作，现累计参与制定国家标准、行业标准、团体标准等30项，持续为行业的健康、有序发展贡献力量

多款主流安全产品市占率第一

- VPN、全网行为管理连续十余年在中国市占率TOP 1
- 下一代防火墙、终端安全管理系统分别位列中国市占率前三

攻防实战，荣誉团队

在多个国家级/省级实战攻防演练中屡获殊荣：
- 2019-2023期间，在国家级攻防演练中均位列前十，
- 2020-2023期间，共获19个省级攻防演习冠军

大力投入安全产业人才培养

特别设立深信服产业教育中心、安服学苑，依托20余年的安全实践经验、研究成果和专业能力，为国家和社会持续输送高质量安全产业人才

迅猛发展的创新型云计算厂商

快速成长

桌面云　分布式存储

超融合　托管云

2012年开启虚拟化技术自研
十年间 推出多款云产品

超融合

成为中国市场占有率
TOP3

托管云

数据中心节点 100+
用户规模 1000+

理念&技术创新，产品比肩国际一流

- 创新推出“线上线下一朵云”的先进理念，让用户上云无须取舍
- 创新实现云内建安全能力，实现业务上线即安全
- 创新推出IOM智能运维分析平台
- 将网络虚拟化和安全虚拟化创新融入超融合架构
- 破除小文件存储性能难题，创新自研凤凰高性能文件系统

超融合
性能稳定性大幅提升

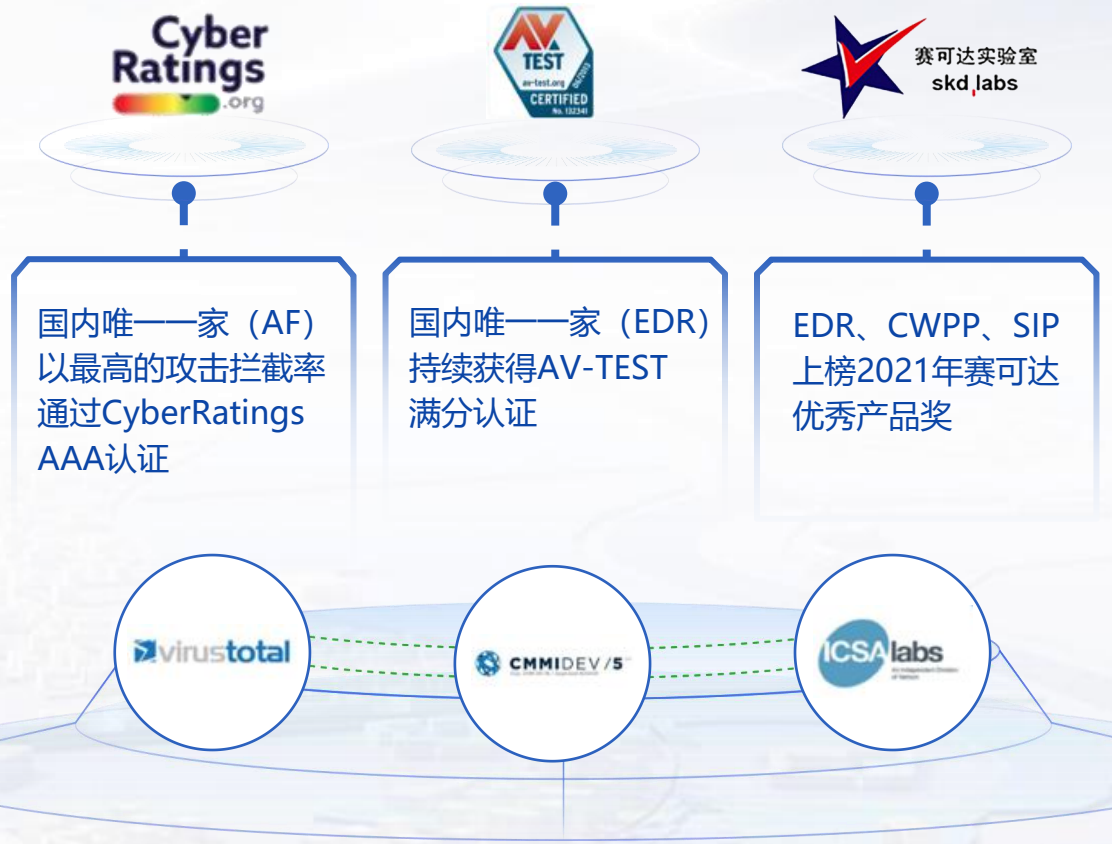
桌面云
使用体验不断升级

AD
性能可靠性大幅领先

EDS
文件性能稳步提高

广受国际权威认可

国际最高水平技术认证



AI First，以人工智能领创产业

模型技术储备早

深信服从2016年开始持续投入AI，在安全和云的不同场景都有成熟模型

数据情报积累强

深信服具有全国部署数量最多的安全组件及大量云计算基础设施，基于优质数据训练出更精准的AI模型

能力全面的大型人才队伍

具备较多的算法人才、安全人才、调优算力人才，尤其是拥有既懂AI又懂安全和云计算的人才

DIRECTORY

目录

我国已经基本形成网络安全法+等保+关保+密评+数据安全评估+安全可控等为基础的网络空间政策框架

政策法规陆续出台，顶层制度安全保障

《网络安全法》

2016年11月《网络安全法》正式发布，其中明确要求“保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”

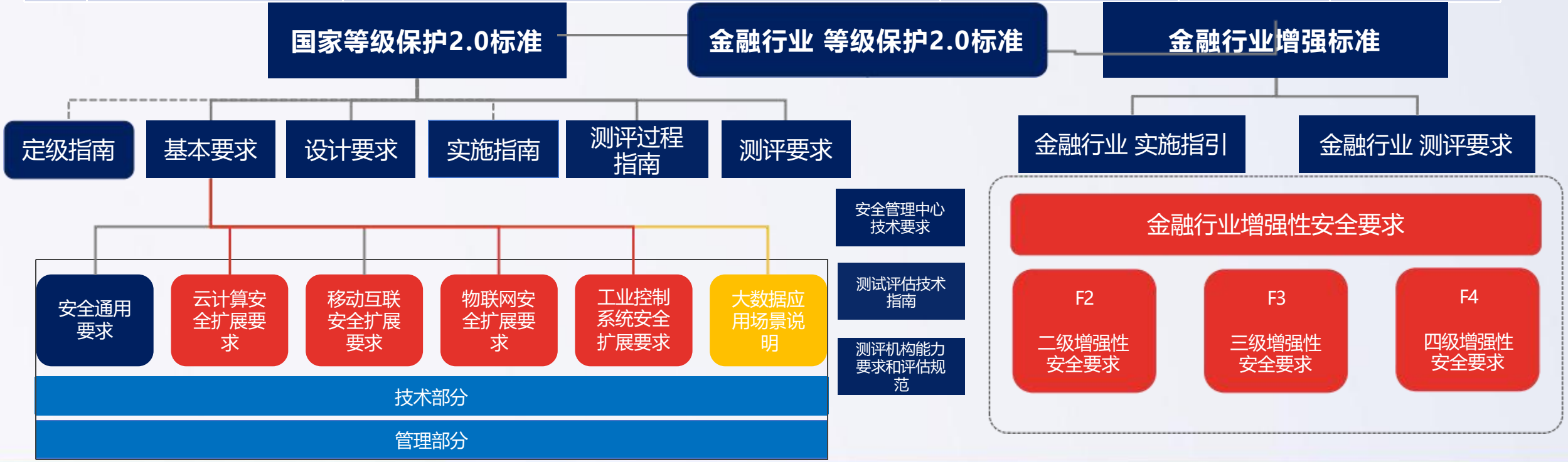
《国家网络空间安全战略》

2016年12月，国家互联网信息办公室发布《国家网络空间安全战略》，提出9大战略任务，其中将“保护关键信息基础设施”明确列为重要战略任务之一

安全合规的重要变化1：等级保护2.0新标准的增强性加固

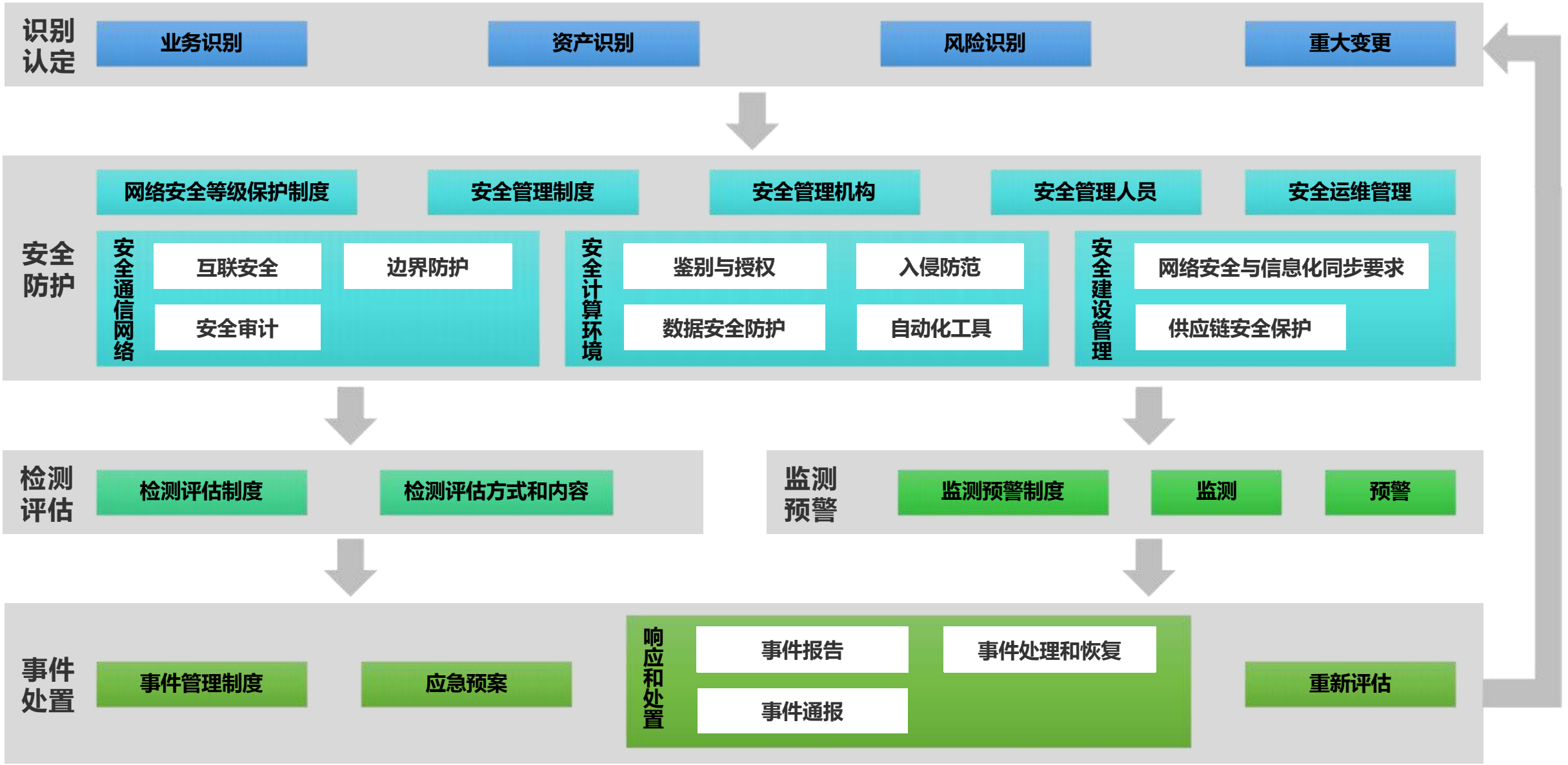
等保

序	标准号	标准名称	标准性质	状态	发布日期
1	JR/T 0071.1—2020	金融行业网络安全等级保护实施指引 第1部分：基础和术语	推荐性行业标准	现行	2020-11-11
2	JR/T 0071.2—2020	金融行业网络安全等级保护实施指引 第2部分：基本要求	推荐性行业标准	现行	2020-11-11
3	JR/T 0071.3—2020	金融行业网络安全等级保护实施指引 第3部分：岗位能力要求和评价指引	推荐性行业标准	现行	2020-11-11
4	JR/T 0071.4—2020	金融行业网络安全等级保护实施指引 第4部分：培训指引	推荐性行业标准	现行	2020-11-11
5	JR/T 0071.5—2020	金融行业网络安全等级保护实施指引 第5部分：审计要求	推荐性行业标准	现行	2020-11-11
6	JR/T 0071.6—2020	金融行业网络安全等级保护实施指引 第6部分：审计指引	推荐性行业标准	现行	2020-11-11
7	JR/T 0072—2020	金融行业网络安全等级保护测评指南	推荐性行业标准	现行	2020-11-11



安全合规的重要变化2：《关键信息基础设施安全保护》推进落实

关保



安全合规的重要变化3：商用密码应用与安全性评估

密评

没有网络安全

就没有国家安全

在重要领域、重点人群乃至全社会**普及密码知识和政策**，在金融和重要领域**推进密码应用**，是落实习近平总书记网络强国战略思想、构建安全可控信息技术体系的一项重要举措。没有网络安全就没有国家安全，密码作为网络安全的**核心技术**，是保护国家安全和根本利益的**战略性资**源。了解密码知识、熟悉密码政策、推进密码应用，是新时期对党政干部的一项新要求。要树立以总体国家安全观为统领、以密码为基础支撑的网络安全观，在相关工作中全面推进密码应用，切实维护国家安全、促进经济发展、保护人民群众利益。

——摘自栗战书同志2017年3月在密码应用工作会议上的讲话

习近平总书记多次对密码工作作出重要指示

法律

《中华人民共和国密码法》

《中华人民共和国电子签名法》

法规

《商用密码管理条例》（修订草案征求意见稿）

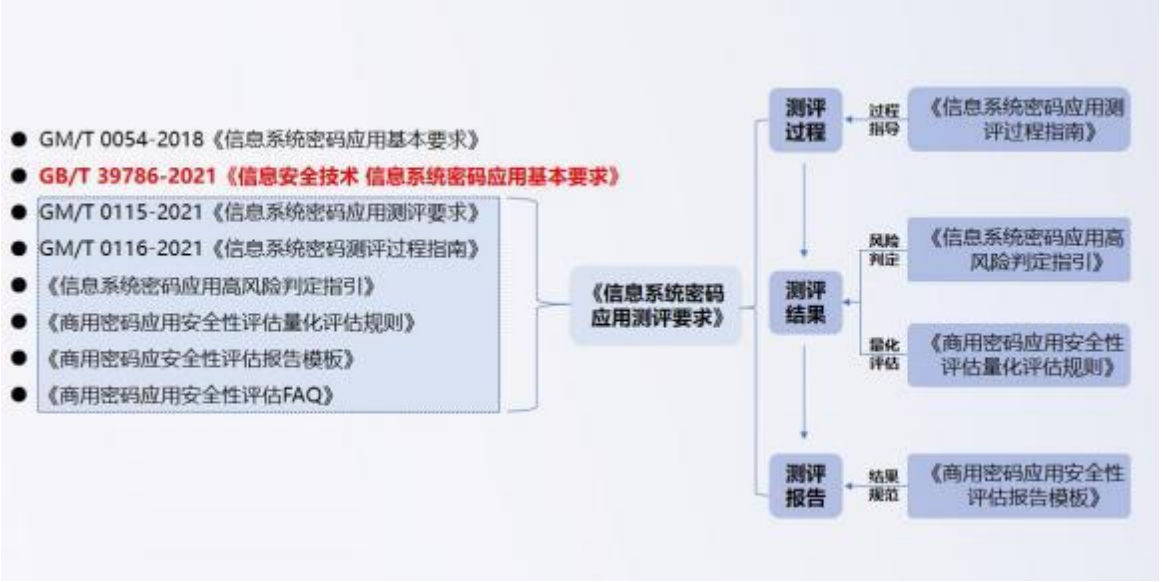
《网络安全等级保护条例》（征求意见稿）

规章

《信息安全等级保护商用密码管理办法》（国密局发〔2007〕11号）

《〈信息安全等级保护商用密码管理办法〉实施意见》（国密局发〔2009〕 10号）

《商用密码应用安全性评估管理办法（试行）》（国密局〔2017〕138号文）



安全合规的重要变化4：数据安全和个人信息保护

数据安全评估

伴随数据安全领域**法律法规**、**合规政策**的陆续颁布，**监管机制逐步完善**，数据安全事件的影响已经不局限于**经济损失**、**声誉损害**，

还可能面临**巨额罚款**和**刑事责任**。

- 刑法修正案
- 国家安全法
- 网络安全法
- 数据安全法
- 个人信息保护法（草案）

全国人大

- 民法典
- 保守国家秘密法
- 密码法
- 电子商务法
- 关于加强网络信息保护的决定

巨额罚款

刑事责任

工信部

- 通信网络安全防护管理办法
- 电信和互联网用户个人信息保护规定

国务院

- 科学数据管理办法
- 商用密码管理条例
- 数据安全管理条例（计划）
- 关键信息基础设施安全保护条例（计划）

经济损失

声誉损害

网信办

- 数据安全管理办法（征求意见稿）
- 个人信息出境安全评估办法（征求意见稿）
- 儿童个人信息网络保护规定

公安部

- 信息安全等级保护管理办法
- 网络安全等级保护条例（征求意见稿）

……

监管机制逐步完善

2012年11月 银发235号《关于开展联合整治**非法买卖银行卡信息**专项行动的通知》

2016年9月 银监办发2号《中国银监会办公厅关于加强网络信息安全与**客户信息保护**有关事项的通知》

2017年 银保监会《银行业保险机构**数据治理**指引》

2018年5月 GB/T 36618-2018信息安全技术 **金融信息服务**安全规范

2018年9月 中国人民银行《**个人金融信息**保护技术规范JR/T 0171—2020》

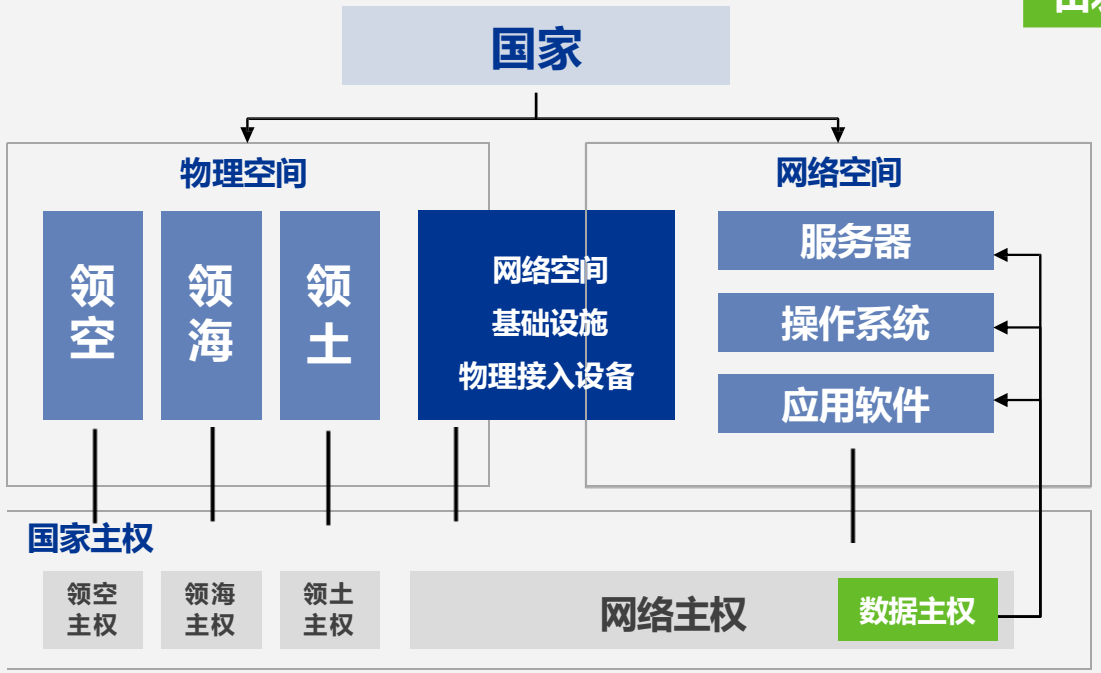
2020年2月 中国人民银行《金融数据安全 **数据安全分级指南**JRT 0197-2020 》

2020年9月 **多方安全计算**金融应用技术规范

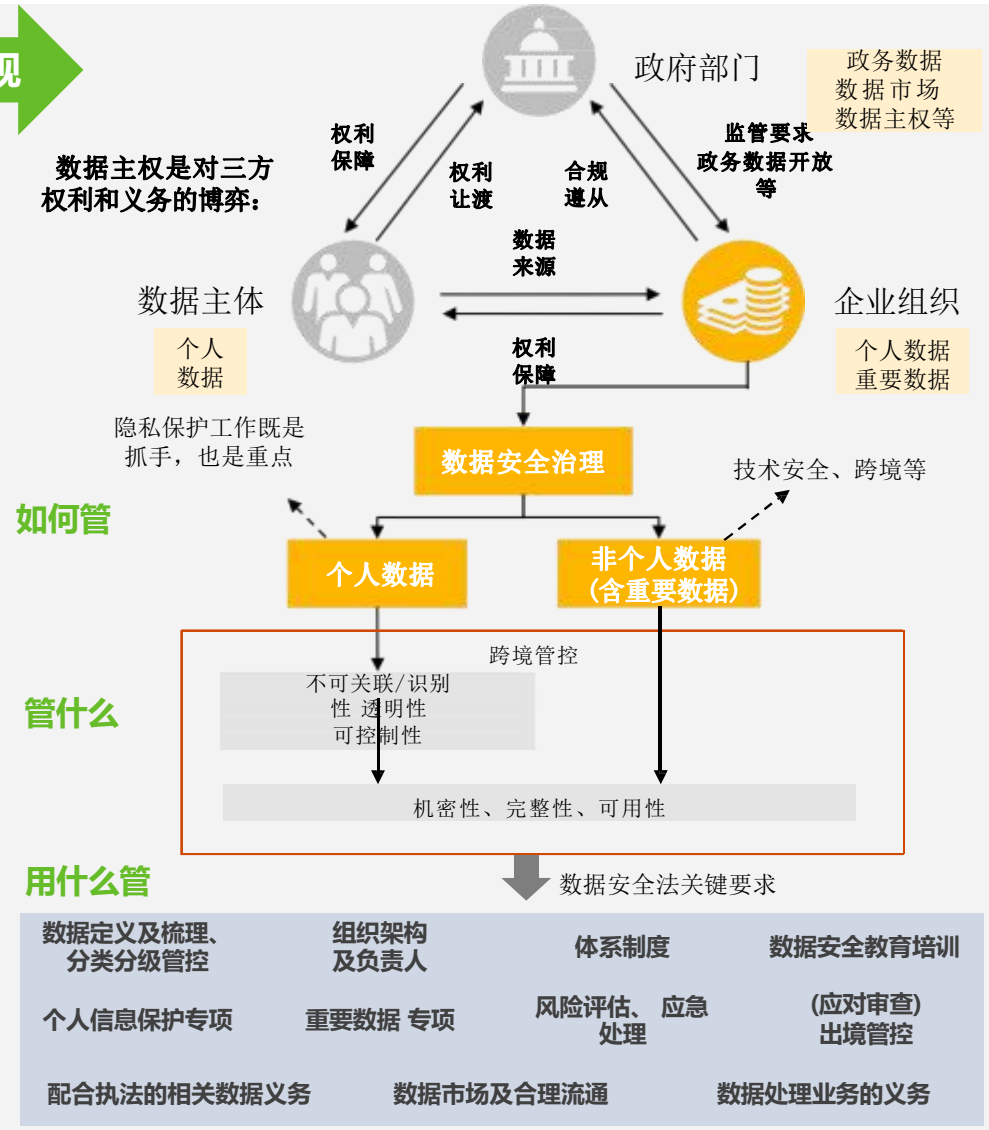
2020年11月 中国人民银行《金融数据安全 **数据生命周期**安全规范 JRT 0223-2021》

2021年4月

由数据主权与数据安全、隐私保护的关系，理解数据安全法的管控框架及企业合规框架



由宏观至微观



- **网络主权**，是国家主权在网络空间的延伸和应用；包括对地理边界内网络空间基础设施/物理接 入设备的管辖权。

- **数据主权**，是网络主权的组成部分，在各国司法实践中，**主要指对网络空间数据的司法管辖权**， 但在判定管辖权归属的问题上，仍然存在属人和属地的差异。数据主权，具有多种具体的表现 形式，在不同的规制手段和措施中，均可以体现数据主权原则

安全合规的重要变化5：攻防演练行动-以攻促防，提升防御能力

合法合规

法律、法规不断完善，要求越来越严

《中华人民共和国网络安全法》自2017年6月1日起施行。

《网络安全等级保护条例》于2019年12月1日开始施行。

《关键信息基础设施安全保护条例》自2021年9月1日起施行。

《中华人民共和国数据安全法》于2021年9月1日起施行。

《中华人民共和国个人信息保护法》于2021年11月1日起施行。

《关于修改<中华人民共和国网络安全法>的决定（征求意见稿）》于2022年9月12日发布，在法律责任部分加大了**惩罚力度**。

监督管理

安全监测检查趋常态化

公安常态化的安全监测通报、不定期抽查

主管单位常态化的监测预警

网信、CNCERT、通管局常态化监测预警

实战重保

实战演练牵引，重大事项保障

全国性攻防实战演练规模不断扩大

重大会议、节日期间安全保障

合规遵循和实战效果双轮驱动

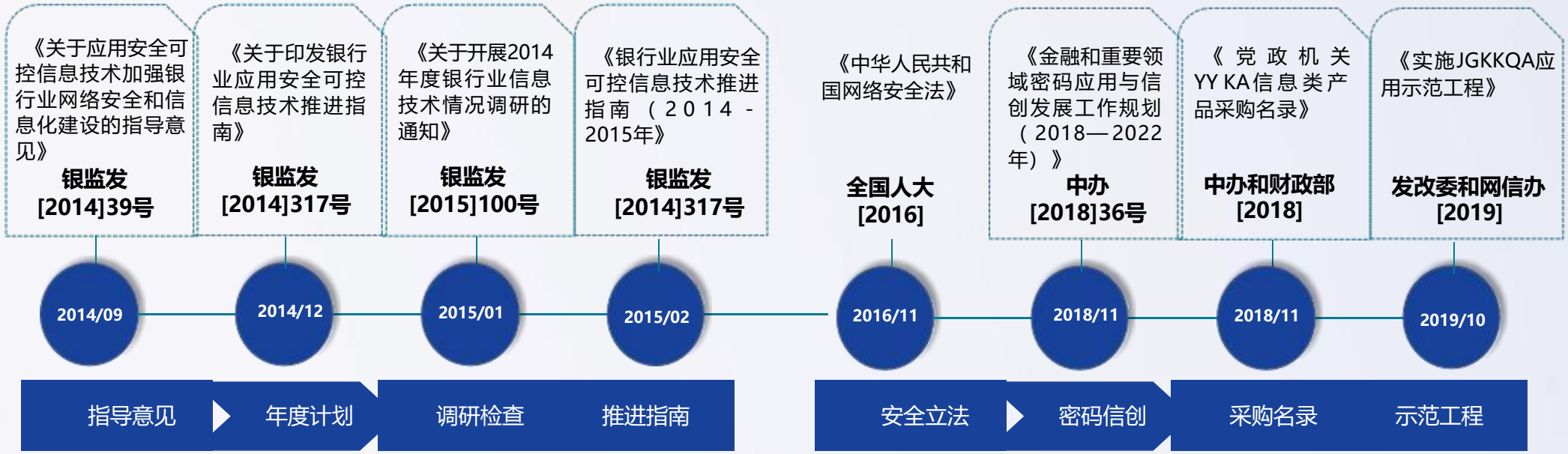
高规格以攻促防，全面提升防御能力

- 真攻真防，最大程度接近国与国的真实网络攻击，对标“网络风暴演习”
- 覆盖所有行业、重要单位、重要系统
- 尽可能发现重大网络安全问题、提高网络安全重视程度和投入效果
- 提升防守能力，真正解决问题、提升我国网络安全整体能力

安全合规的重要变化6：金融信创面临政策合规挑战

信创/安全自主可控

建立银行业信息技术资产分类目录和安全可控指标管理体系



- 信息技术资产分类由类别代码、名称、说明等要素构成
- 分为两个层次，共计10大类68小类
- 银监会对每类资产设定了不同的自主可控要求

银行业金融机构应渐进式地实现应用安全可控，具体工作要求如下:

- **先关注新增应用，后着眼已有应用**
  安全可控指标的应用任务主要关注于“新增安全可控设备”逐年不低于15%比例增加的年度可控指标要求
- **先考虑成熟产品，后考虑自主信创**
  安全可控技术相对成熟的网络设备、存储、中低端服务器优先级较高，而对于操作系统、大/小型机和数据库等领域，银行业需着重于探索尝试的研究任务
  未来银行业信息架构上需逐步减少对高端服务器的依赖，如使用开源的X86应用集群替代高端服务器。

- **安全合规的重要变化7：金融科技应用带来新的安全风险，针对新安全风险的监管在增强，行业形成了一系列新的安全标准、规范的制修订**

序号	已发布标准、规范		序号	制定中标准、规范	
1	《移动金融客户端应用软件安全管理规范》（JR/T0092-2019）、《证券期货业移动互联网应用程序安全规范》（JR/T 0192-2020）	**移动金融APP备案及安全**	10	**《金融行业商用密码应用基本要求》《金融信息系统加密服务的技术能力评价模型》**《基于分散密钥的数字证书认证技术规范》《移动证书应用技术规范》	**国密、密钥分散和协同签名技术，手机盾、手机云证书**
2	网上银行系统信息安全通用规范》（JR/T 0068—2020）	**网银安全要求更新（IPV6、云安全、主动防御、国密…）**	11	《数字函证金融应用安全规范》、《金融领域电子单证技术应用规范》（可信安全体系：七部委发文推进会计师事务所函证数字化）	**可信安全体系**
3	《金融分布式账本技术安全规范》（JR/T 0184—2020）	**区块链安全**	12	《多方安全计算金融应用技术规范》	**多方安全计算、隐私保护**
4	《个人金融信息保护技术规范(JR/T 0171-2020)》	**数据安全和个人信息保护**	13	<条码支付安全技术规范》、《人脸识别线下支付安全应用技术规范》：《聚合支付安全技术规范》、《支付信息保护技术规范》	**支付安全**
5	证券期货业软件测试指南 软件安全测试》（JR/T 0191-2020）	**软件开发安全**	14	《分布式数据库技术金融应用规范 灾难恢复要求 》《分布式数据库技术金融应用规范 安全技术要求》	**分布式数据库应用安全技术**
6	商业银行应用程序接口安全管理规范》（JR/T 0185—2020）	**API安全**	15	《金融信息系统WEB应用服务安全测试通用规范》《金融行业信息系统网络安全众测实施指南》《银行互联网渗透测试指南》	**WEB扫描、众测、渗透测试**
7	金融业网络安全态势感知与信息共享平台	**态势感知监管平台**	16	《金融数据安全 数据安全分级指南》、《金融数据安全 数据生命周期安全规范》	**数据安全**
8	**《商用密码产品生产和保障能力建设规范》等13项密码金融行业标准**	**密码、国密**	17	《云计算技术金融应用检测规范 安全技术》、《云计算技术金融应用检测规范 技术架构》、《云计算技术金融应用检测规范 容灾》	**云安全**
9	**《金融行业网络安全等级保护实施指引》2020版（11月11日人行发布）**	**等级保护**	18	《金融科技创新应用测试规范》《金融科技创新安全通用规范》..	**金融科技创新安全**
19	金融网络安全 网络安全运营中心建设指南 金融网络安全 信息基础设施网络安全防御技术框架建设指南	**安全运营和纵深防御**	20	《金融网络安全_网络安全能力成熟度模型》	**能力成熟度**

DIRECTORY

目录

金融行业安全趋势

一是互联网经济犯罪活动居高

- 网络攻击和网络犯罪现象日益突出，相比前几年愈发呈现出**攻击工具趋于专业化、目的趋于商业化、行为趋于组织化、手段趋于多样化**的特点
- 此类威胁的特点在于利益驱使高、受害主体广、攻击方式多、社会危害大

二是金融面临的高级威胁不断加剧

- 黑客攻击手段不断升级，新兴APT攻击威胁层出不穷，恶意木马病毒持续泛滥，零日漏洞的精准突袭
- 网络安全的主要威胁已经从黑客攻击模式转化成为犯罪分子规模化敛财模式，呈现出明显的**规模化、产业化、精准化**趋势

三是基础设施、通用软件安全不可控

- 基础设施并不完全可靠，也不是完全可控，近几年频发的通用软件漏洞导致全球服务器、网络设备、Web应用遭受影响就是典型的案例
- 银行业自身IT资产庞大，高危漏洞修复工作量巨大，面临的风险敞口加大

四是移动设备和支付安全问题凸显

- 银行业在互联网上的安全防御能力并没跟上互联网的发展
- 随着移动支付方式的普及，我们24小时都暴露在互联网攻击之下，安全威胁在不断升高

五是泄露窃密性攻击步入“高发期”

- 网站系统安全漏洞，以及内外部勾结买卖客户信息的事件不断发生。
- 银行除了要防范攻击外，更需防范数据的丢失及有组织的窃取，这关系到银行的声誉和品牌形象

六是新业务、新技术带来的潜在风险

- 通过互联互通、大数据、跨界融合发展，银行业可在方方面面与各行业合作，但其所带来的数据流转与交换，使银行业面临更多业务与技术的挑战
- 云计算、大数据、物联网、智能设备、生物识别等成为网络攻击潜在的安全隐患，物理边界模糊，安全风险持续升级

金融科技发展带来的安全风险形势

- 金融科技的快速发展促进了金融创新，深刻改变着金融服务模式和金融概念。同时新技术的综合运用也带来新的风险及挑战，需要积极应对，主动防控。

1.通用基础组件漏洞数量持续增长

2.新技术应用引发新类型风险

3.金融生态圈涉及交易参与方多、环节多，暴露面大，防护链条长，防护面广

4.新业务创新引入风险，线上线下融合，风险容易被传导

5.数据泄露与数据滥用风险日益突出

23年网络安全风险态势

1、 供应链攻击

根据欧盟网络安全局（ENISA）的调查研究，供应链攻击呈现出以下趋势：

✓ 66%攻击事件的攻击目标是供应商代码，20%攻击事件的攻击目标是数据，14%攻击事件的攻击目标是内部流程。

✓供应商并不清楚攻击是如何发生的：

✓超过50%的供应链攻击归因于知名网络犯罪组织，包括APT29、Thallium APT、UNC2546和Lazarus APT等

2、 数据安全威胁

根据Verizon的调查数据显示，数据安全威胁呈现出以下趋势：

✓85%的数据泄露都与人为因素有关,泄露最多的数据是凭证(60%)和个人数据(50%)

✓ 网络钓鱼仍然是数据泄露的主要原因（36%），其次是使用被盗凭证(25%)和勒索软件(10%)。经济动机仍然是攻击的主要动因，其次是间谍活动，通常涉及盗窃知识产权或其他机密信息

3、 云环境威胁

基于云的服务在计算机网络运营(CNO)过程中越来越多地被攻击者利用：

✓云漏洞利用增多：攻击者倾向于利用服务器软件中已知的RCE漏洞

✓利用配置错误的镜像容器：攻击者会定期利用配置不当的Docker容器。

✓恶意软件托管和命令与控制（C2）：网络犯罪和有针对性的入侵攻击者大多是利用合法的云服务来传播恶意软件

4、 勒索软件攻击

通过钓鱼邮件和暴力破解远程桌面协议(RDP)服务进行攻击是两种最常见的攻击向量：

✓勒索软件组织针对基础设施发起攻击：知名的勒索软件攻击事件包括Colonial Pipeline、JBS Foods、New Cooperative攻击事件

✓ RDP和钓鱼依旧是最常见的攻击方式

✓勒索软件即服务（RaaS）商业模式发展壮大

✓招募企业内鬼：更复杂的勒索软件攻击即将出现的趋势是积极招募员工在勒索软件活动期间提供协助。

5、 漏洞利用

漏洞一直是网络攻防的焦点所在：

✓ 2021 年发布了 20,136 个常见漏洞和披露(CVE)。这标志着连续五年发现了创纪录的漏洞数量

✓ 2022年将是0day漏洞创纪录的年份

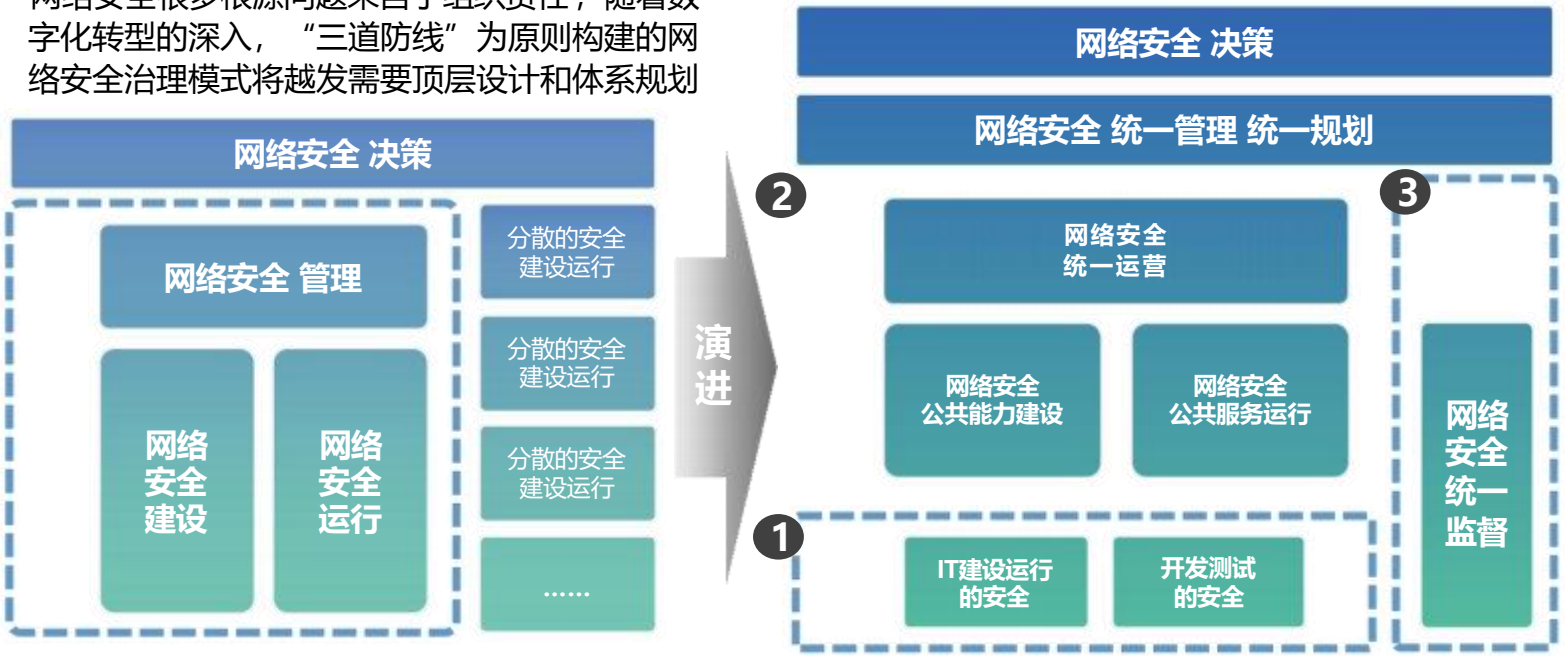
- 上半年众多Fortinet供应商（包括为关键基础设施部门提供软件的供应商）的产品中共发现了72个0day漏洞
- 22年出现最多的漏洞当属Apache Log4j。如果不加以修复，攻击者可以闯入系统、窃取密码和登录名、提取数据并使用恶意软件感染网络。
- 端点漏洞成为焦点：这些远程设备特别容易受到攻击。犯罪分子经常试图将端点设备用作访问公司网络和窃取数据、利用现有软件漏洞或劫持信息的入口点
- 物联网OT漏洞：2022年5月，FortiGuard实验室发现并报告了西门子产品的24个0day漏洞；此外，OT:ICEFALL今年早些时候发布的56个漏洞影响了10家不同供应商的OT设备
- 勒索病毒漏洞利用：如攻击者采用**VMware** ESXi 服务器 2021 年的远程代码执行漏洞 CVE-2021-21974 获得交互式访问，借以**部署新的** ESXiArgs **勒索软件**

DIRECTORY

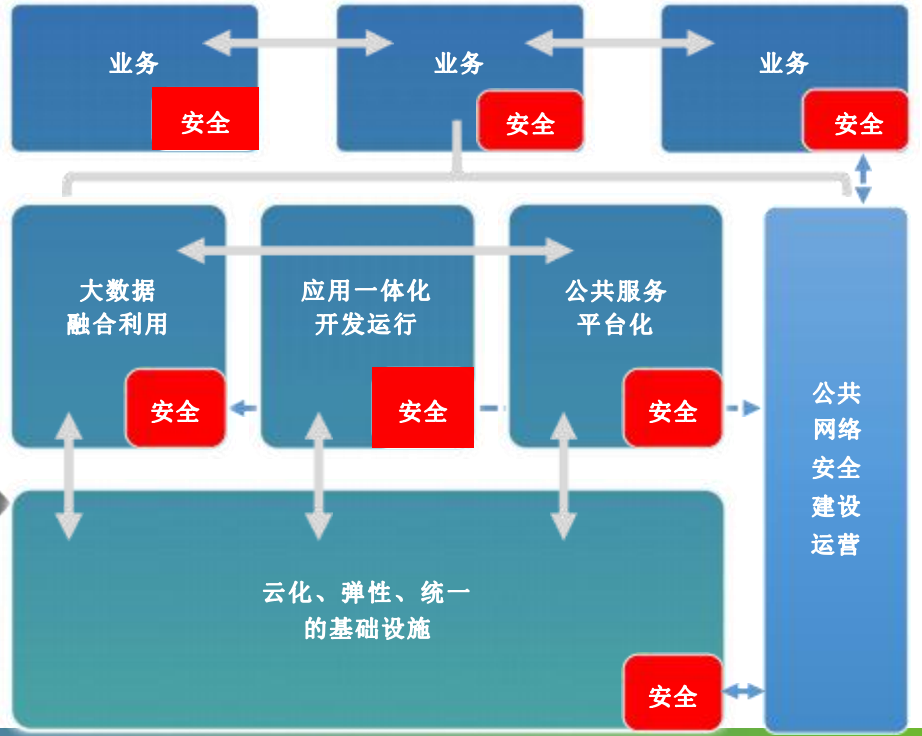
目录

数字化转型下网络安全治理模式演进

网络安全很多根源问题来自于组织责任，随着数字化转型的深入，“三道防线”为原则构建的网络安全治理模式将越发需要顶层设计和体系规划



数字化转型打破独立的业务烟囱，通过大数据融合利用、应用一体化开发运行、公共服务平台化、基础设施云化实现业务的融合发展，而安全将从外挂模式，融入数字化分工，并持续推动公共网络安全能力建设运营。



网络和信息安全整体建设思路

网络安全数字化转型重点任务

驱动力

三法一条例
行业及上级部门
合规要求

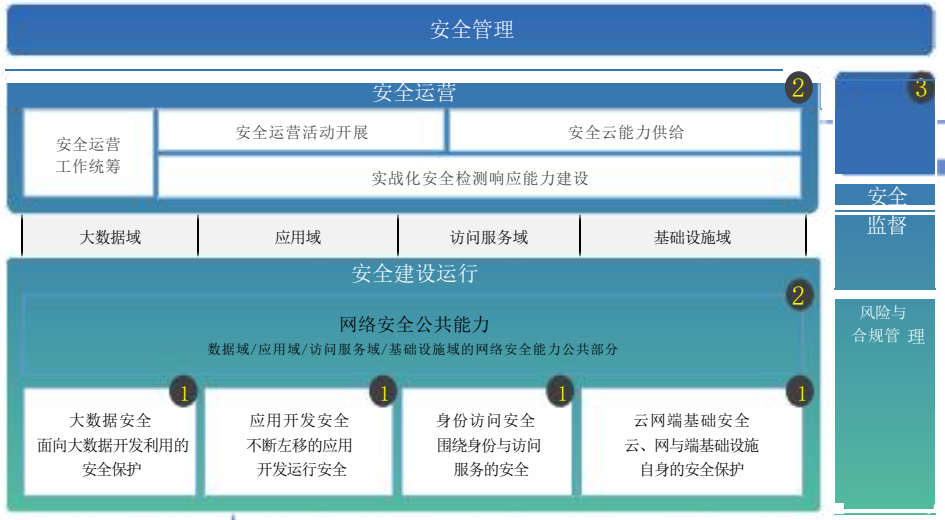
以风险优先级
实战化对抗
为需求导向

业务及数字化场景、
对象的新增、变更
为需求指引

行业总体现状，行业平均水平，网络安全的行业竞争力

安全架构/组织架构

安全总体框架



安全组织架构

管理&监督部门
1. 业务部门
2. IT 管理部门
3. 数据管理部门
4. 安全管理部门
5. 风险合规部门
……

数字化建设单元
1. 云网端基础设施0 U
   • 终端/网络建设运行
   • 云IaaS 建设运行 …
2. 应用建设与开发测试0 U
   • 云PaaS 建设运行
   • 应用开发与测试. …
3. 网络安全建设运行0 U
3. IT 平台建设运行0 U
   • 身份与访问平台
   • 公共IT 服务平台 …
4. 大数据资源管理0 U
   • 大数据平台建设运行
   • 数据资源管理与治理 …
5. 业务IT 建设运行0 U

1+N 数字化安全建设分工：
「1」网络公共安全建设与运营
「N」云网端基础设施自身安全、应用开发测试安全、IT平台（身份与访问管理）安全、大数据安全管理、业务安全 …

主要任务

管理监督相关任务
(任务主体、协同部门)

安全运营平台建设任务
(任务主体、协同部门)

安全运营活动开展任务
(任务主体、协同部门)

安全组件建设运行任务
(任务主体、协同部门)

基于“纵深防御”的安全体系建设

网络安全核心指导思想

预测

- 自动评估在网系统风险
- 分级展现总分行信息系统、设备风险
- 基于数据“抓主要风险”

防御

- 边界访问控制、在网设备全量发现、安全事件管理
- 设备安全属性自动提取、设备安全配置
- 安全域变更实时感知
- 边界设置及策略核查

回溯

- 准确、全面、实时攻击事件原始线索收集能力
- 精准安全事件关联分析告警，触发应急响应流程
- 快速、有效的事件分析及处置

监测

- 安全域流量检测、设备配置漏洞核查
- 软件代码漏洞扫描
- 业务策略设置漏洞监测
- 业务逻辑漏洞分析

一个安全体系

要把信息安全工作提升到企业发展的战略性高度，健全信息安全管理体系，加强信息安全技术防护，提升关键信息基础设施的安全保障水平，确保风险可控

三道安全防线

遵从银行业信息科技风险三道防线要求，从网络层、系统层、业务层、数据层四个层面，建立纵深防御体系，有效防范各类系统破坏、业务滥用、信息盗窃等恶意攻击

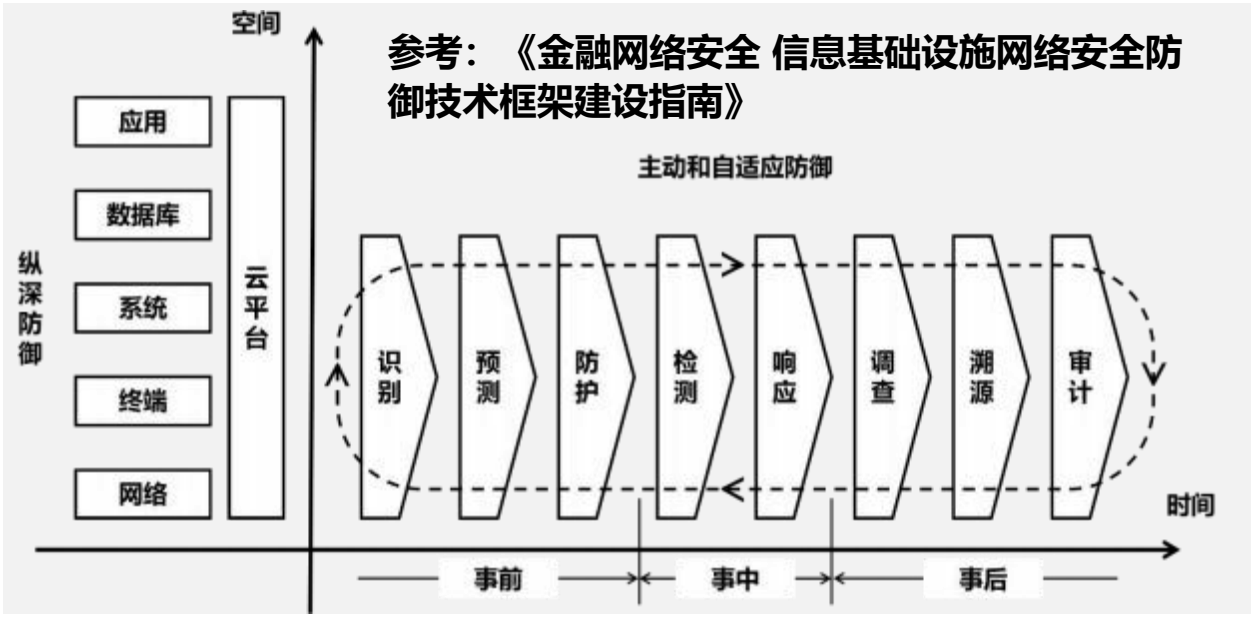
四个有效防护能力

- 有效的事前预测能力
- 有效的深度监测能力
- 有效的安全防御能力
- 有效的回溯响应能力

六个统一安全服务

- 统一的安全策略服务
- 统一的数据安全服务
- 统一的身份认证服务
- 统一的应用安全服务
- 统一的基础安全服务
- 统一的安全监测服务

技术路径：传统“纵深防御”的防御框架向立体化、 自适应、 主动防御升级



参考：《金融网络安全 信息基础设施网络安全防御技术框架建设指南》

- **现状：** 当前**金融机构的安全体系**主要从**空间维度，** 根据自身的网络空间环境， 从**网络、 终端、 系统、 数据库、 应用**等不同的信息技术领域进行防御技术规划和设计。 通过**层次性的防护**， 合理利用各种技术的特点， 从而**达到多方式、 多层次、 多重技术功能互补的效**果。 以**满足防护的均衡性、 抗易损性要求， 防止出现一处防御措施失效后，全线被突破**的局面。
- **未来：** 空间和时间两个维度的立体化网络安全防御， 在” 时间维度 “增强主动和自适应防御。
  - ✓ **主动防御**要求有机组合技术、 管理和人员， 尽可能缩短威胁检测时间， 尽可能延长威胁遏制时间。
  - ✓ **自适应防御**要求防御过程是一个持续循环的过程， 通过**威胁动态分析， 自动适应不断变化的网络和威胁环境， 并不断优化自身的安全防御机制**

附： 金融网络安全 信息基础设施网络安全防御技术框架建设指南（征求意见稿）

网络安全防御技术是指金融机构信息科技部门在信息系统运行阶段， 为防范、监控和处置网络安全威胁， 配套部署的技术设施。

金融机构网络安全防御技术框架宜遵循以下原则：

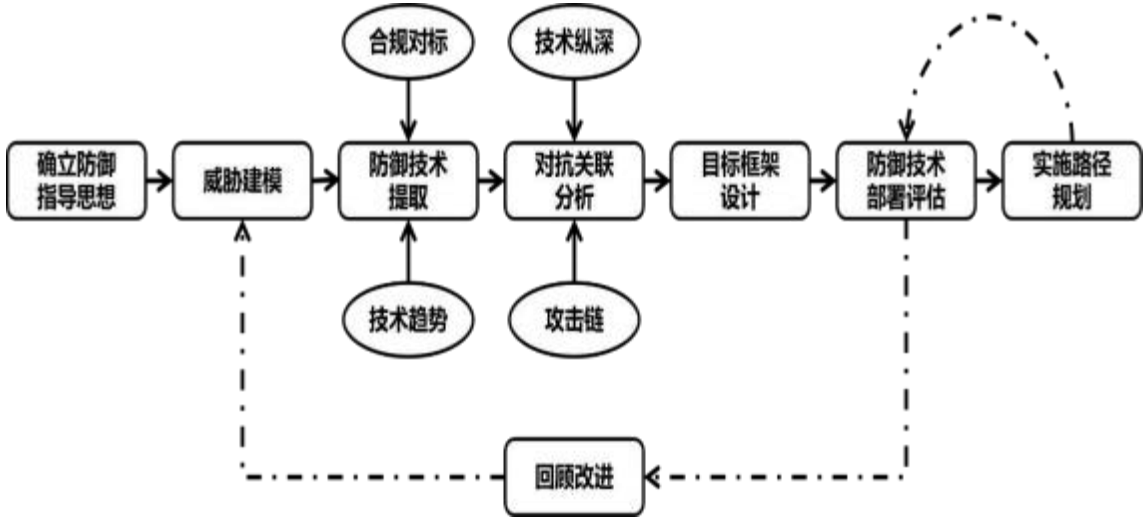
a) 合规原则， 框架建设继承了金融行业强监管的网络安全管理思想， 需要充分满足国家法律法规、行业监管要求。全球化运营的金融机构， 还需要考虑所在国家和地区的法律与监管要求。

b) 对抗原则， 框架建设需要瞄准网络攻防对抗， 充分利用网络空间纵深进行布防， 尽可能使用有效的技术手段， 及时发现和遏制网络攻击。

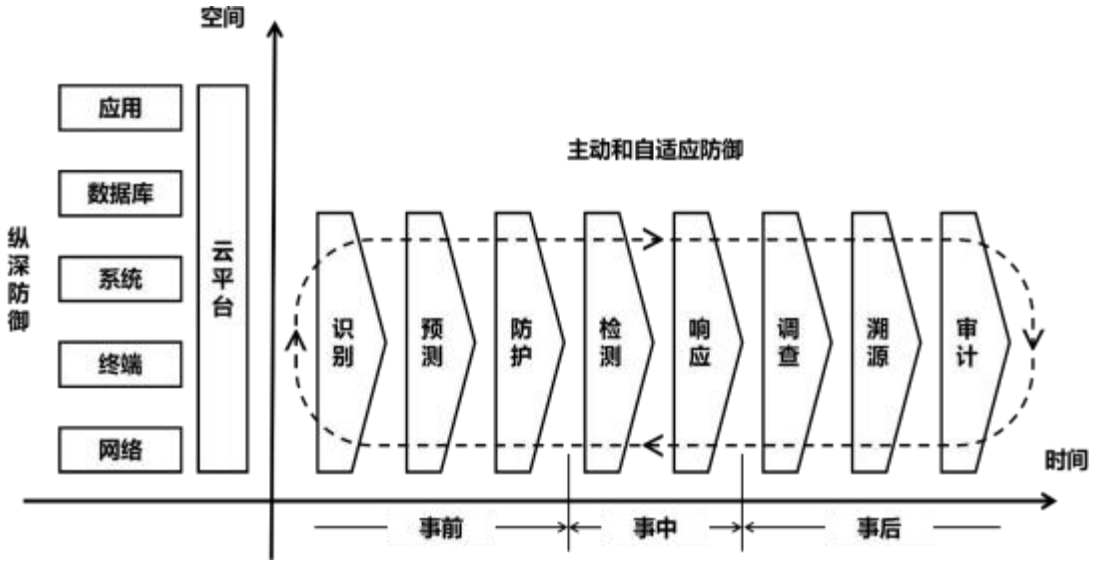
c) 同步原则， 金融机构信息系统投产运行时， 配套网络安全防御技术宜同步部署启用。

d) 持续改进， 金融机构网络安全防御技术框架建设宜遵循持续改进的原则， 不断提升网络安全防御能力。

框架演进



防御指导思想



网络安全防御技术框架建设分为确立防御指导思想、威胁建模、防御技术提取、对抗关联分析、 目标框架设计、防御技术部署评估、实施路径规划、 回顾改进八个演进步骤， 按照网络、终端、系统、应用、数据库、邮件、即时通讯、云平台8个技术领域来进行部署。通过层次性的防护， 合理利用各种技术的特点， 达到多方式、多层次、多重技术功能互补的效果。

金融网络安全防御技术框架的未来蓝图

基础能力 | 增强能力

主动和自适应防御

审计：日志审计 | 用户行为审计 | 安全例外

威胁：SIEM | SOAR:安全自动化编排 | 调查取证 | 威胁溯源 | 威胁狩猎

网络

- 网络隔离
- 网络访问控制
- 非法外联检测
- 文件和数据流转
- 无线准入和安全
- 非法AP检测和压制
- 无线网络
- DDOS
- DNS安全
- 旁路阻断
- IDS/IPS
- 流量威胁检测
- 安全检测沙箱
- 网络DLP
- 网络传输加密
- 网络基础日志

终端

PC终端
- 恶意代码防护
- 软件白面单
- 补丁管理
- 终端DLP
- 移动介质DLP
- 终端威胁检测和响应
- 终端附件控制
- 终端环境感知

移动终端
- 恶意代码防护
- 移动终端DLP
- 防提权
- 远程擦除
- 电子围栏
- 应用运行安全沙箱

IOT终端
- 安全审计日志

数据库

- 数据加密
- 数据脱敏
- 数据有效删除
- 数据库防火墙
- 数据库审计日志

系统

- 系统访问控制
- 恶意代码防护
- 补丁管理
- 软件白名单
- HIDS/HIPS
- 系统日志审计

IM

- 即时通信DLP
- IM通讯审计

邮件

- 反垃圾邮件
- 邮件DLP
- 邮件威胁检测
- 邮件审计日志

应用

- WAF RASP
- WEB传输加密
- 防篡改
- API威胁检测
- 应用安全日志
- 集权应用审计日志

云平台

云管
- 云管平台审计日志

虚拟网络
- 东西向安全
- 东西向流量威胁检测

虚拟网络隔离
- 访问控制
- 租户隔离
- 微隔离

容器
- 防逃逸
- 镜像检测
- 审计日志
- 镜像库审计日志

虚拟机
- 防逃逸
- 微隔离
- 镜像检测
- 管理系统审计日志
- 系统镜像库审计日志

纵深防御

准入：VPN | 无线网络准入 | 上网代理 | 堡垒机 | 终端准入 | API网关 | 应用隐藏网关 | 密网 | 准入

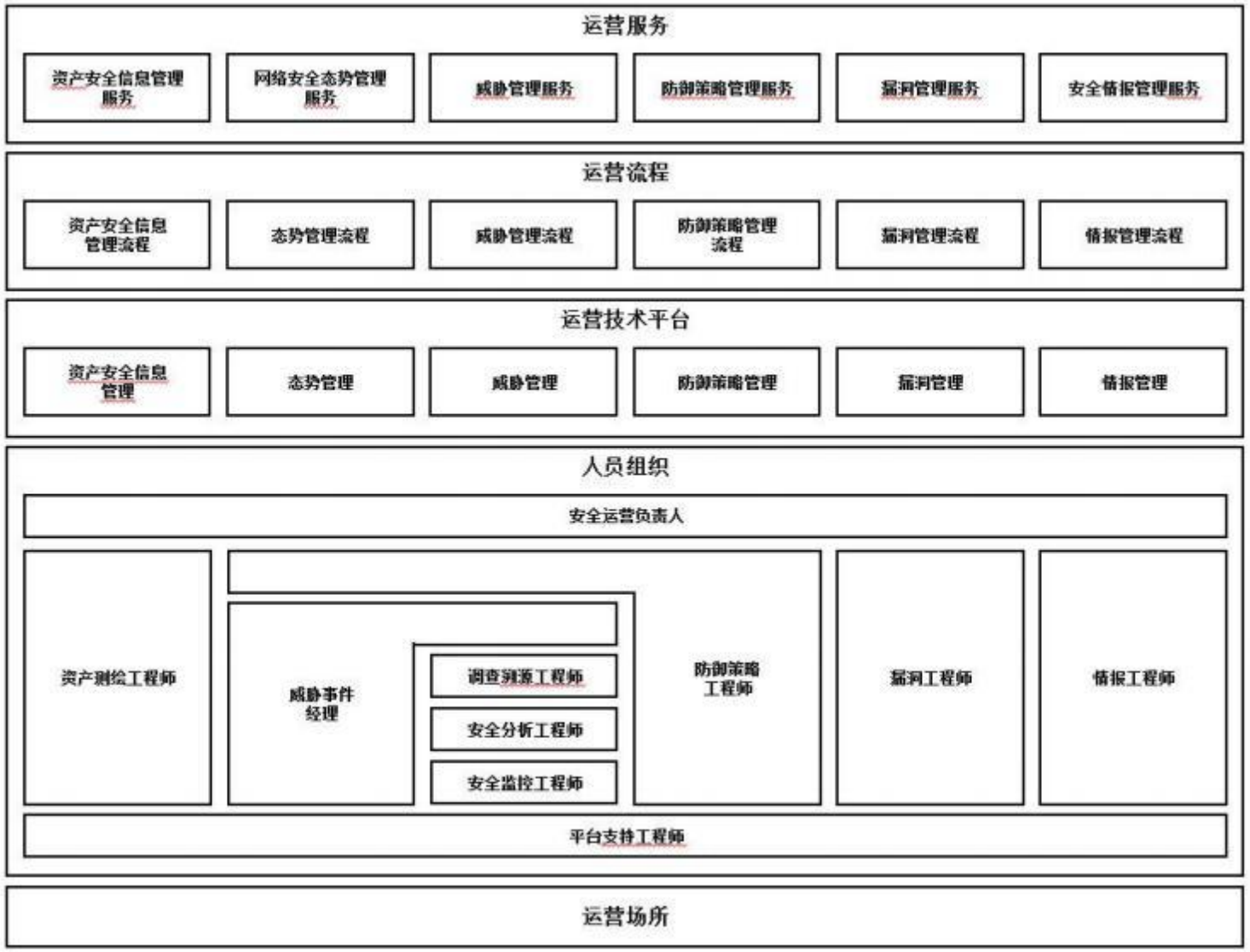
身份：身份认证和权限管理 | 多因素认证 | 持续信任评估 | 动态访问控制

情报：基础信息情报 | 漏洞情报 | 威胁情报 | 信息泄露情报 | 黑客画像情报

漏洞：配置缺陷检测 | 系统漏洞检测 | 应用漏洞检测 | 自动渗透测试 | 云管平台配置缺陷检测 | 防御有效性检测

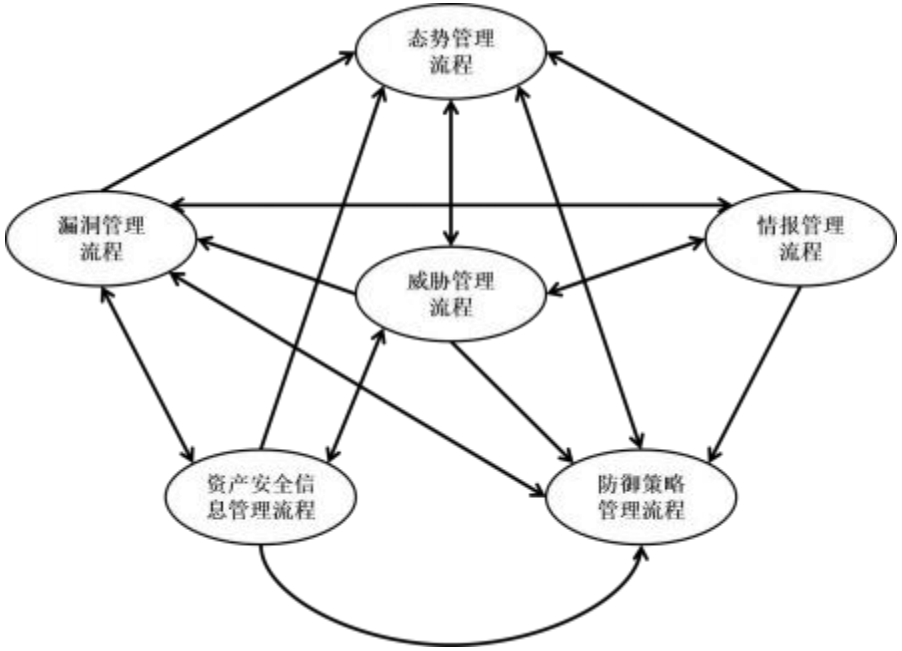
资产：主机资产发现 | 软件组件发现 | API资产发现 | 互联网服务发现 | 公众网络空间资产发现 | 非法资产发现

附： 金融网络安全 网络安全运营中心建设指南（征求意见稿）



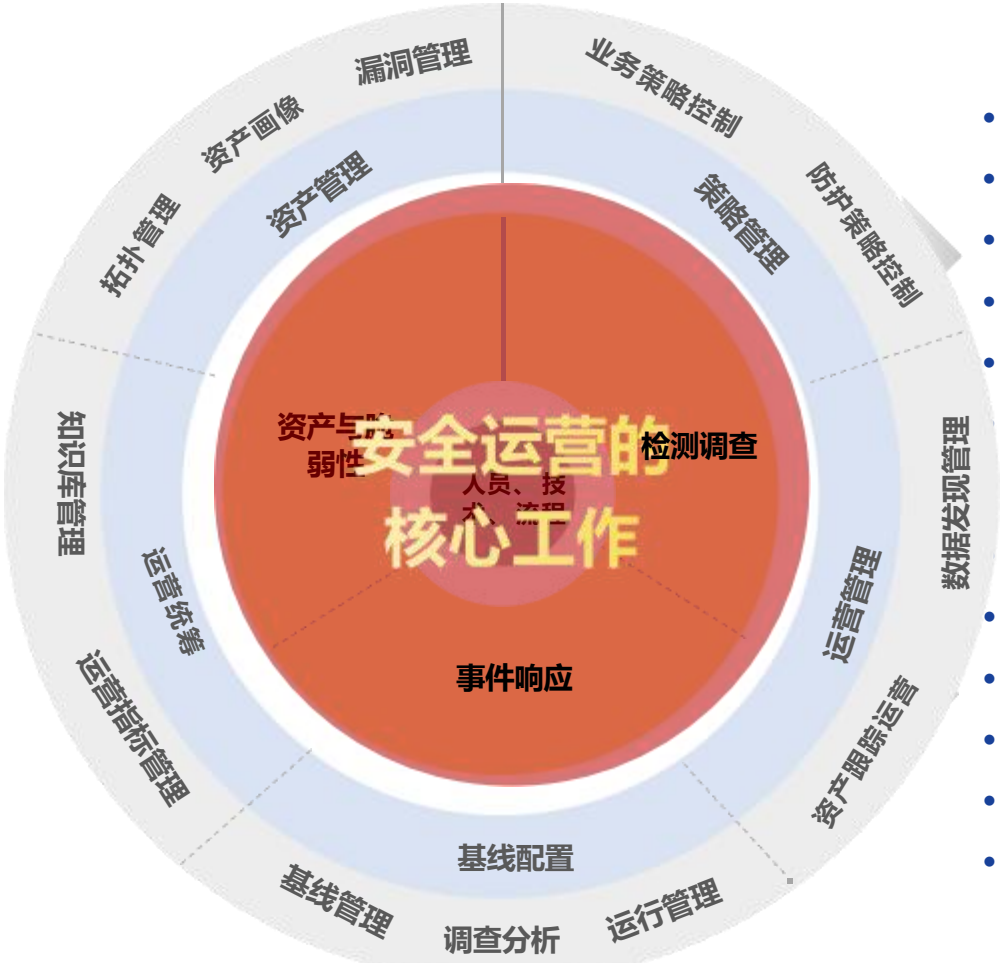
金融行业网络安全运营中心运营能力分为基础和增强运营能力两大类。基础运营能力的种类包括：威胁管理能力、漏洞管理能力。增强运营能力的种类包括：资产安全信息管理能力、安全情报管理能力、网络安全态势管理能力、防御策略管理能力。

金融行业网络安全运营中心需要具备基础运营能力。根据IT技术设施规模和投入计划，金融机构可对增强运营能力种类进行适当裁剪。



安全运营建设思路：安全运营应当以效果为核心

思路



手段

- 数据融合编织
- 海量噪声消减
- 情景检测
- 威胁定性
- 故事线还原
- 智能研判

- 资产与脆弱性碎片化管理
- 资产定位到人
- 热点威胁影响面排查
- SOAR
- 流程工单
- 线上/线下服务

效果

强化检测与调查能力，实现威胁可视可溯

持续获取有效的一手遥测数据，利用丰富且详细的上下文信息进行情景检测，还原故事线，自动调查举证，实现少而精准的检测效果

通过资产融合与攻击面分析，实现资产的可视可控，优先加固关键攻击入口点，提升预防效率

强化碎片化资产的融合，构建安全运营基座，提升热点威胁影响面排查效率，持续降低安全风险

加强事件响应能力，使事件处置更高效

基于SOAR构建多层次、精细化、场景化的响应能力，打破安全孤岛，破解数字化时代下的安全运营难题

人员组织与流程服务优化，推进安全运营持续有效落地

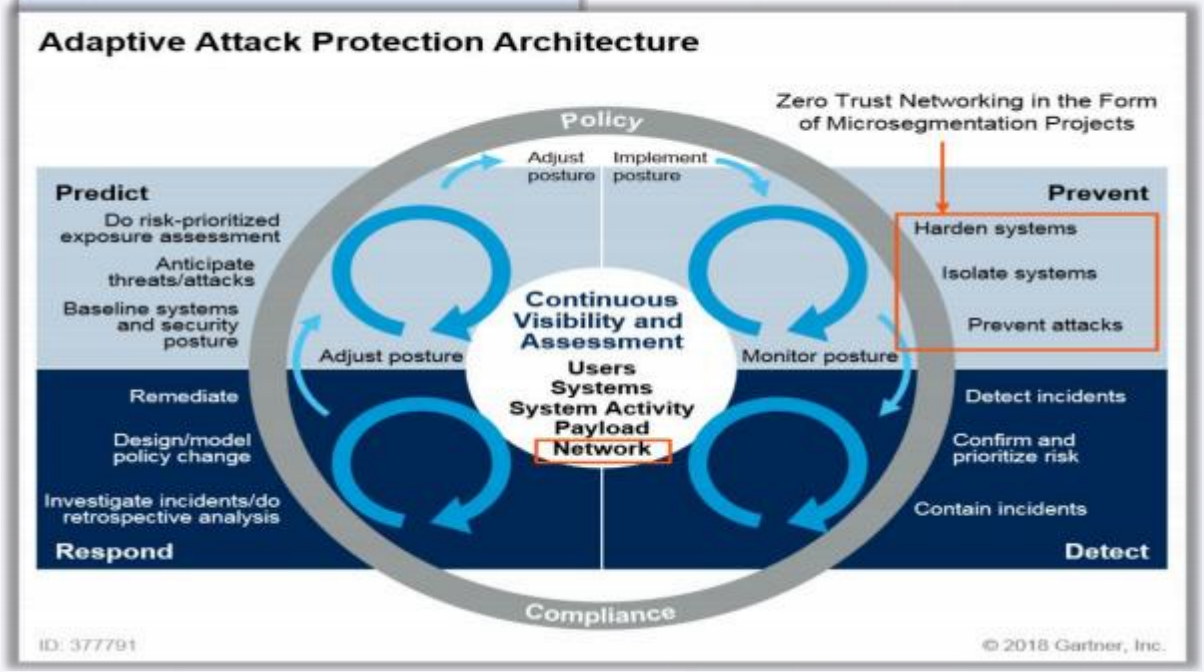
整合"人员、流程、工具"体现安全工作价值，提升安全效果与安全效率

安全运营工作涵盖范围很广，功能设计比较灵活，但最终**效果**的达成取决于内核能力的建设质量 —— 即**实战化的威胁对抗能力**，安全运营应当以效果为核心、以闭环为目的，聚焦检测能力提升，实现精准高效的效果。

安全架构演进Gartner CARTA——持续自适应风险信任评估

自适应攻击保护安全架构

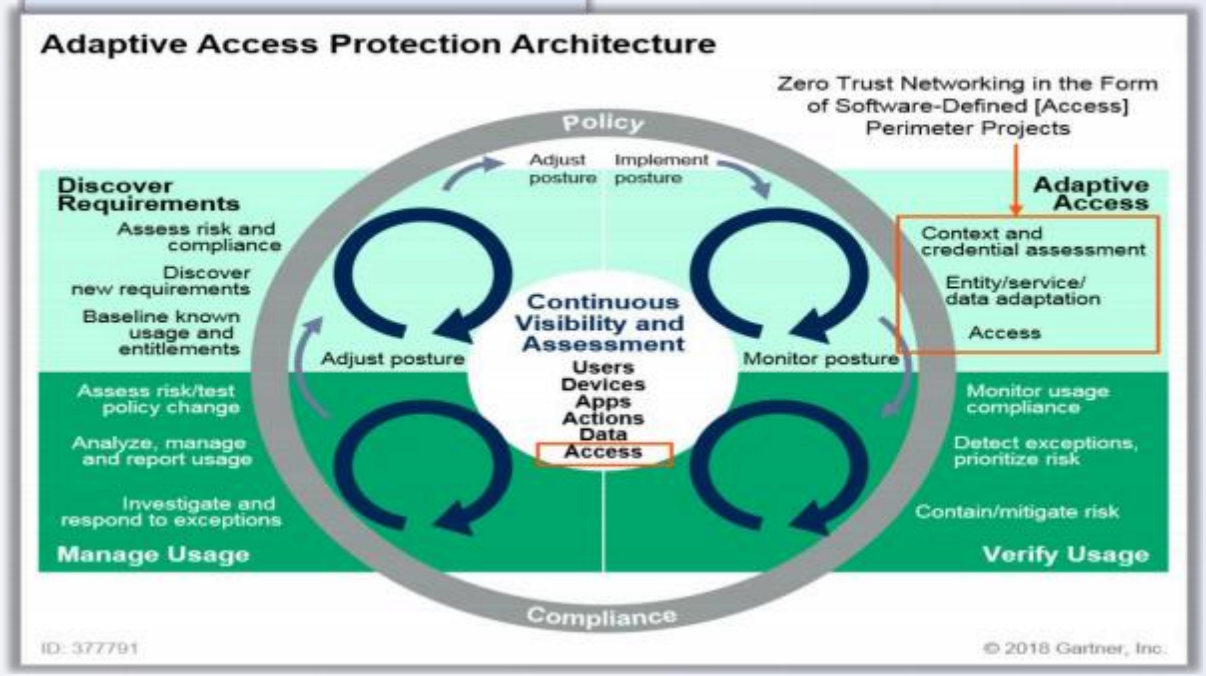
以微分段形式的零信任网络



使用**默认拒绝、零信任初始状态**进行自适应攻击保护

自适应接入保护安全架构

以软件定义访问形式的零信任网络

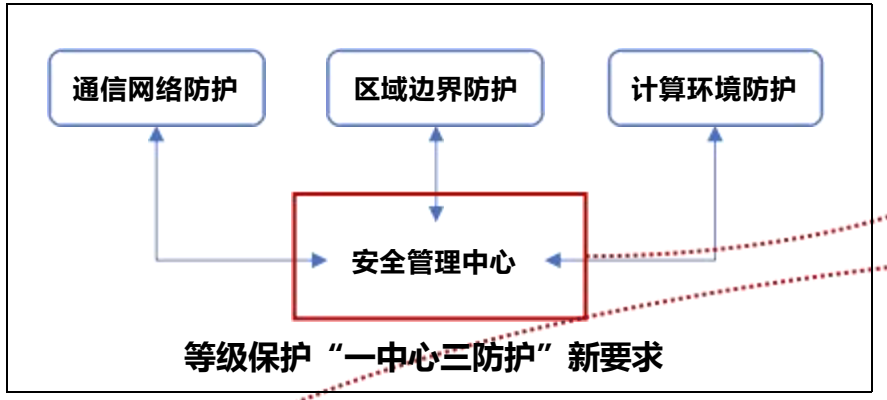


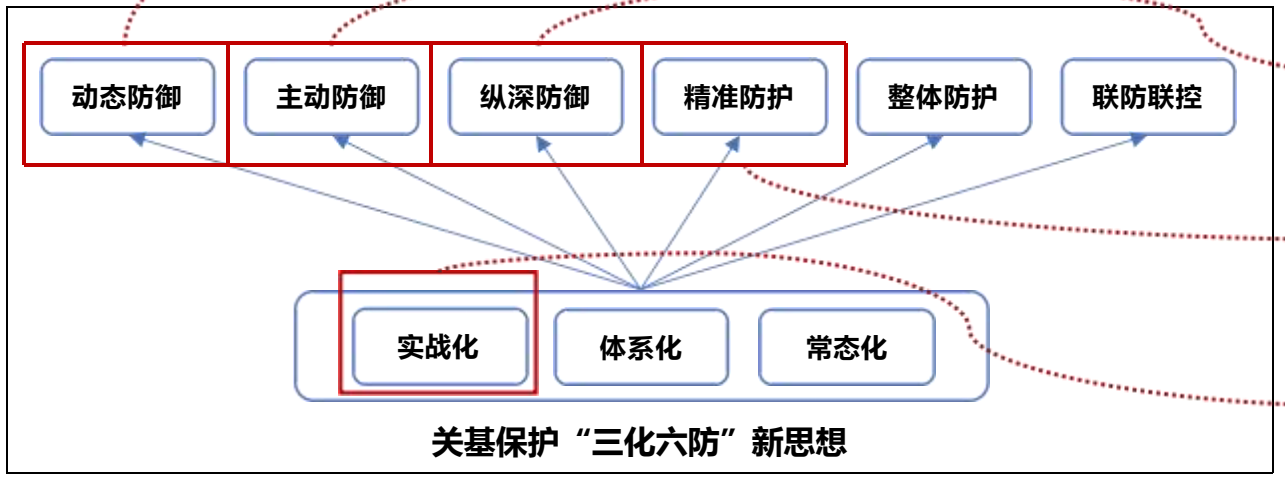
使用**默认拒绝、零信任初始状态**进行自适应访问保护

- 聚焦信任和风险，进行持续闭环的控制——持续自适应风险信任评估（CARTA， Continuous Adaptive Risk and Trust Assessment)
- 零信任是初始状态，需要基于持续的风险评估，进行动态、精益的信任控制

零信任与等保、关基保护的关系

在网络安全等级保护和关键信息基础设施保护的转型期，需要以新思想、新方法和新举措进一步深入推进等保和关保的实践，零信任作为国内外公认的新一代安全范式，为网络安全建设提供了有益的指引。





- 零信任架构建立统一的访问控制决策点，汇总、研判安全风险信息，发挥了安全管理中心的作用。
- 零信任架构建立信任评估机制，持续监测和评估访问异常与风险，实时调整访问授权实现动态防御。
- 零信任架构建立了威胁情报、行为分析等多元信息渠道，可以实现主动的访问权限升降级能力。
- 零信任架构追求用户、设备、网络、应用、数据全访问链条的安全，通过微隔离提供纵深防御。
- 零信任架构以数据资源为保护核心，以访问路径为控制手段，提升了安全防御的精准性。
- 零信任安全架构以消除不必要的隐式信任为原则，假设已被入侵，立足于有效对抗APT攻击。

安全架构演进以合规为抓手，保护数据处理活动，成为治理数据安全工作的必经之路

1 总体数据基础层面

数据定义及梳理、分类分级管控

《数据安全法》第3、 6、 21条

2 管理职能及职责层面

组织架构及负责人

第27条

3 合规义务层面

规范数据处理活动（收集、存储、使用、加工、传输、提供、公开等），保障数据安全

第1、 2、 4、 8、 13、 21、 28、 29条

3.1 基本合规义务层面

数据安全制度体系

第27条

数据安全教育培训

第27条

3.2 重点合规义务层面

个人信息保护专项

第7、 8、 28、 29、 32条

重要数据专项

第29、 30、 32条

风险评估与监测、 应急处理与告知上报

第22、 23、 30条

(应对审查)数据出境管控

第24、 25、 31、 35条

4 对外数据合作层面

配合执法的相关数据义务

第35条

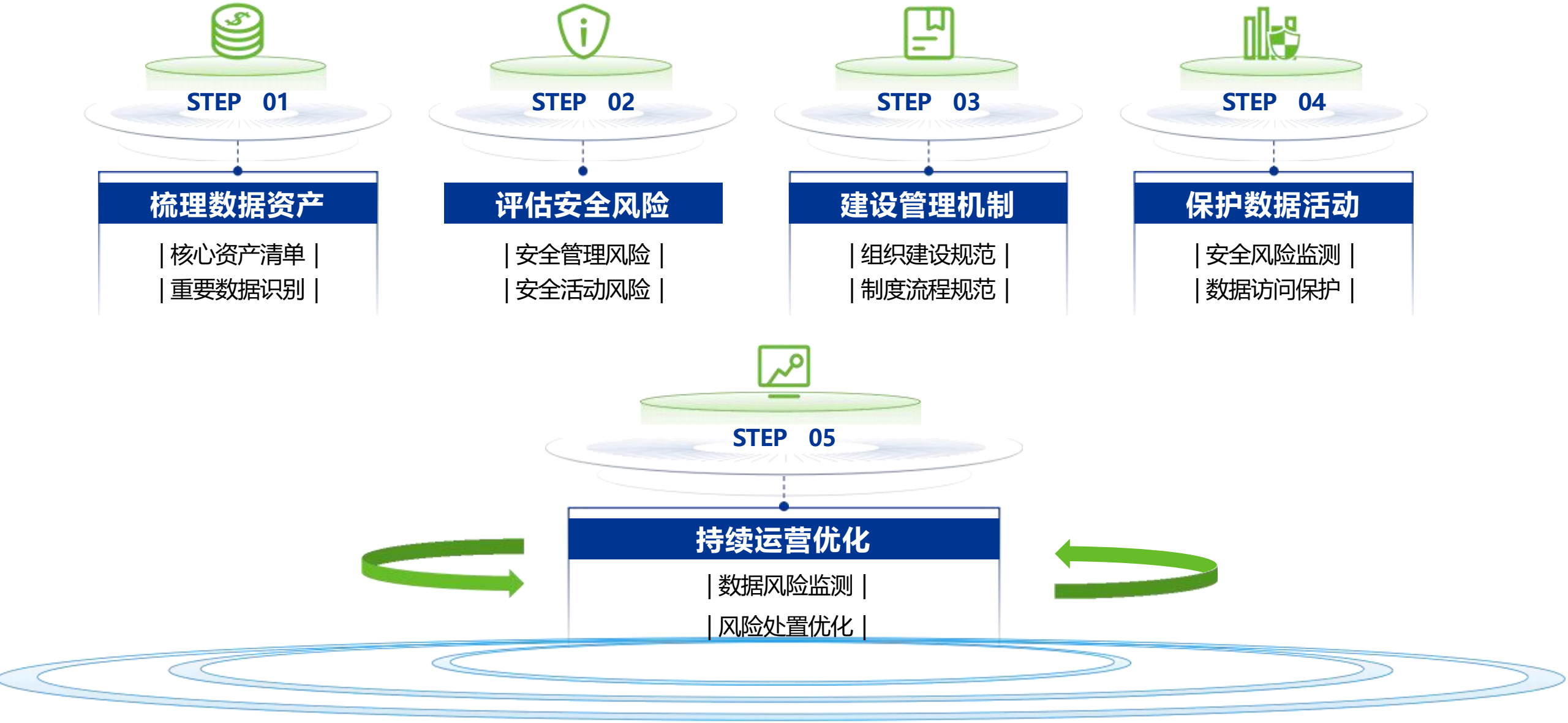
涉及(外协)数据处理工作的义务

第8、 33、 34、 40条

数据市场及合理流通

第11、 13-20条

构建“数据处理活动”的全流程安全防御机制



安全架构演进从业务安全的角度看开发安全建设

应用问题修复困难大

安全总是落后于业务，出现安全问题后，修复问题成本巨大，安全要为业务让步，埋下隐患。

应用迭代快，安全跟不上

云原生及DevOps的快速应用，数字应用的快速发展，现有安全举措难以匹配业务进行有效防护。

无法作用于应用内部

传统的安全是作用于网络、终端、存储等对象的“外挂式”安全，无法有效解决应用内部问题。

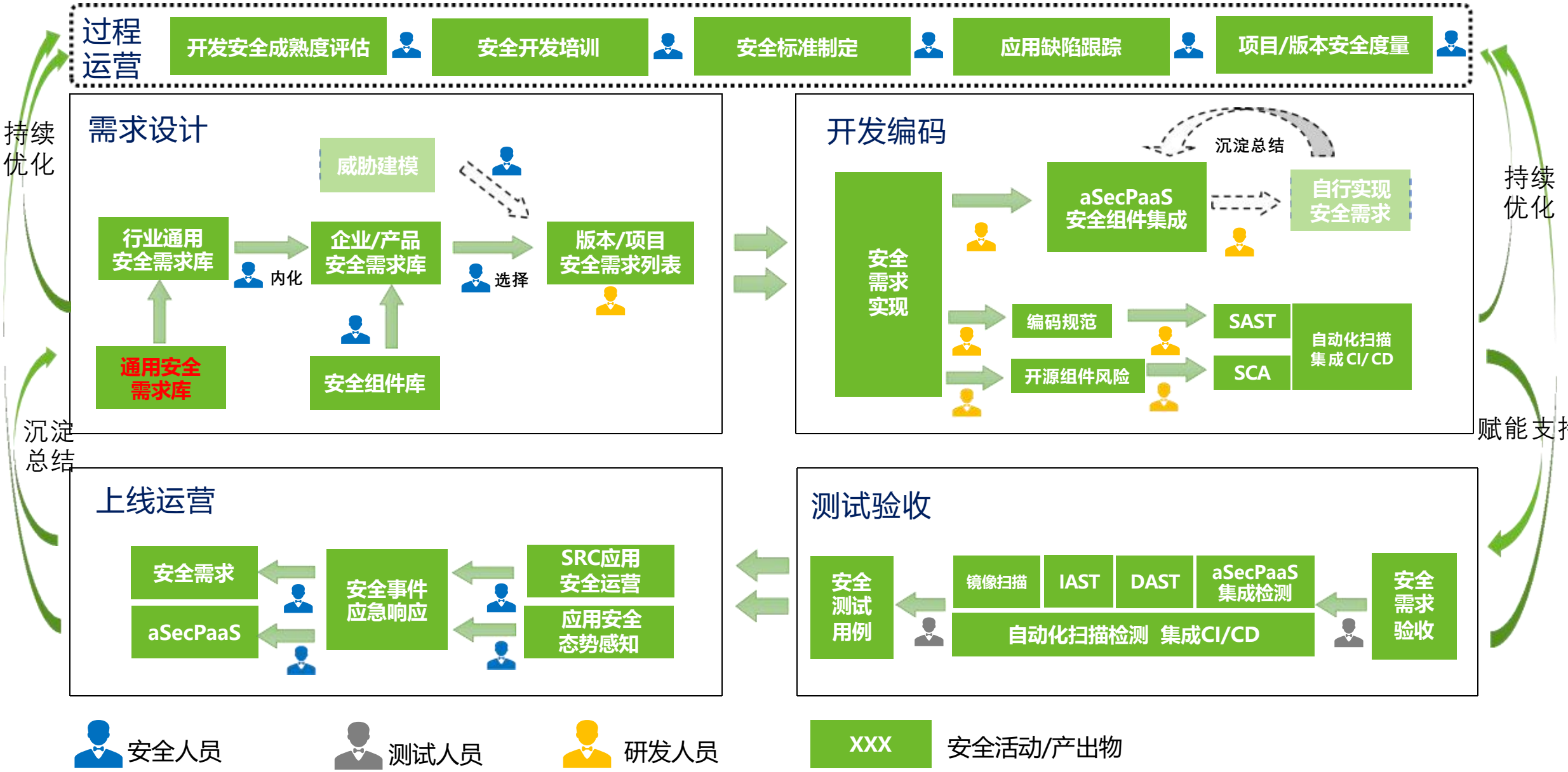
安全需要前置

安全需要左移

安全需要内生

在应用开发阶段解决应用安全风险是最有效、低成本的安全建设方式

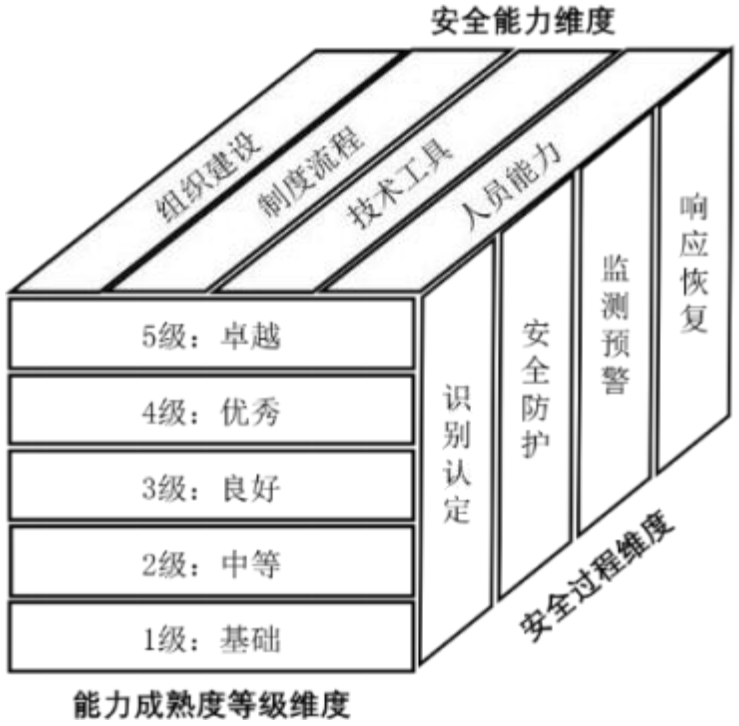
开发安全建设实践流程


过程运营
开发安全成熟度评估
安全开发培训
安全标准制定
应用缺陷跟踪
项目/版本安全度量
持续优化
需求设计
威胁建模
行业通用安全需求库
内化
企业/产品安全需求库
选择
版本/项目安全需求列表
通用安全需求库
安全组件库
开发编码
沉淀总结
安全需求实现
aSecPaaS安全组件集成
自行实现安全需求
编码规范
SAST
自动化扫描集成CI/CD
开源组件风险
SCA
持续优化
沉淀总结
赋能支持
上线运营
安全需求
aSecPaaS
安全事件应急响应
SRC应用安全运营
应用安全态势感知
测试验收
安全测试用例
镜像扫描
IAST
DAST
aSecPaaS集成检测
自动化扫描检测 集成CI/CD
安全需求验收
安全人员
测试人员
研发人员
XXX
安全活动/产出物

参考资料：**《金融网络安全_网络安全能力成熟度模型》征求意见稿**（人行）

如何量化评估安全水平，推进金融机构的网络安全能力提升？——《金融网络安全_网络安全能力成熟度模型》

规范金融机构网络安全能力评估的方法，指导金融机构提升网络安全防护水平，完善网络安全体系建设，目前行业制定中**《金融网络安全_网络安全能力成熟度模型》**



能力成熟度等级	能力成熟度等级特征
等级1：基础（L1）	金融机构在满足国家及行业法律法规要求的基础上，对于关键节点及重要环境仅通过实施有限的安全防护措施，做到应对已知风险的基础防护，但安全防护体系化不足，难以应对复杂问题。在发生重要业务运营中断事件后，能够快速恢复。
等级2：中等（L2）	金融机构初步形成网络安全防护架构，检测和防护手段能做到因地制宜，开展规范化的安全防护工作，能够有效处置大部分业务的运营中断事件。
等级3：良好（L3）	金融机构已具备较为完善的安全防护体系架构，并建立健全配套的组织架构、制度流程、技术工具和安全人员能力支撑，具备风险的自动化检测和纵深防御能力，能够有效处置绝大部分业务的运营中断事件。
等级4：优秀（L4）	金融机构主动实施网络安全风险检测与分析，自动化的工作全面替代手工执行，侧重攻击方法学习和威胁情报收集，通过渗透测试、攻防演练、特征分析等以攻促防，积极参与国家与行业间安全风险防范联防联控。
等级5：卓越（L5）	金融机构持续对网络安全防护能力现状进行分析评估，及时消除安全防护体系存在的问题和不足，持续提升网络安全能力，具备极限环境下的响应与恢复能力。

a）组织建设（Organization）：金融机构内网络安全组织的设立、职责分配和沟通协作；
b）制度流程（Process）：金融机构内网络安全领域的制度和流程执行；
c）技术工具（Technology）：通过技术手段和产品工具落实安全要求或自动化实现安全工作；
d）人员能力（Ability）：金融机构内执行网络安全工作的人员的安全意识及相关专业能力。

a）识别认定：了解并管理支持关键业务的资源，以及相关的网络安全风险；
b）安全防护：制订并实施适当的防护措施，保证业务连续性，防范网络安全风险；
c）监测预警：持续开展网络安全风险及事件监测，实施风险预警与通报；
d）响应恢复：制订网络安全事件响应与应急预案，控制并处置网络安全事件，恢复功能与服务，持续提升安全事件应急处置能力。

参考资料：《金融网络安全_网络安全能力成熟度模型》征求意见稿（人行）

基于FCS-CMM架构的金融网络安全CD体系（IPDR架构）提供了金融安全建设的完整框架和能力矩阵

金融网络安全能力域

识别认定（I）	安全防护（P）	监测预警（D）	响应恢复（R）
• CD01 业务识别 • CD02 资产管理 • CD03 安全策略 • CD04 风险管理	• CD05 物理安全 • CD06 网络通讯安全 • CD07 服务器安全 • CD08 终端安全 • CD09 应用安全 • CD10 数据安全 • CD11 安全开发 • CD12 安全运维 • CD13 人员安全 • CD14 攻防实战	• CD15 安全监控 • CD16 态势感知 • CD17 分析预警	• CD18 安全应急 • CD19 响应改进

	组织建设	制度流程	技术工具	人员能力	小计
L1：基础	9	42	20	1	72
L2：中等	16	43	50	8	117
L3：良好	10	44	79	5	138
L4：优秀	5	16	63	2	86
L5：基础	3	13	38	3	57
总计	43	158	150	19	470

基于安全过程建立，包括4个安全过程、19个CD（安全域）、105个CSD（能力项）、470个**建设点/评估项**

a)识别认定过程的CD（CD01-04）包括：业务识别、资产管理、风险管理、安全策略4个CD及下属18个CSD；

b)安全防护过程的CD（CD05-14）包括：物理安全、网络安全、服务器安全、终端安全、应用安全、数据安全、安全开发、安全运维、人员安全、攻防演练10个CD及下属65个CSD；

c)监测预警过程的CD（CD15-17）包括：安全监控、态势感知、分析预警3个CD及下属14个CSD；

响应恢复过程的CD（CD18-19）包括：安全应急、响应改进2个CD及下属8个CSD

金融网络安全能力成熟度等级评价.xlsx

DIRECTORY

目录

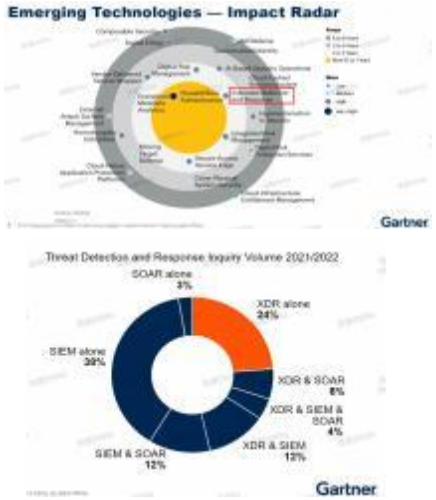
1、业界安全运营的技术发展趋势

安全运营已从基于SIEMI技术解决合规与归档问题的阶段，过渡到基于技术强化威胁监测与响应的阶我。

Gartner

资料来源： 在2022年Gartner发布的

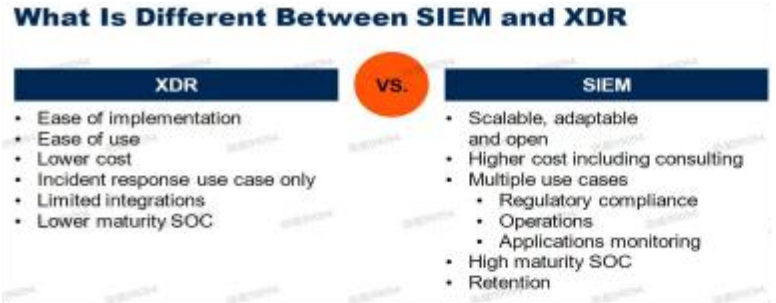
《 Hype Cycle for Security Operations, 2022》



资料来源：Gartner:positioning your solutions in the world of XDR

基于Gartner的统计结果，**XDR已成为过去两年在威胁检测与响应领域最炙手可热的技术。**此外，根据《Gartner 2022年预测整合式安全平台将是未来的发展趋势》中的分析情况，到**2027**年，**50%**的中端市场安全买家将**利用XDR推动工作空间安全技术的整合**，如端点、云和身份。

Gartner



- **传统安全运营中心（SOC）的主要实现方式**是**SIEM**。
- 传统安全运营中心聚焦解决合规性和报告任务，但**基于SIEM的威胁管理很难成功**，对**分析场景**没有深刻的认知，数据的价值无法发挥，**缺乏真正多源关联分析的能力**，过于依靠人员能力。
- 而**XDR**具备**聚合**分析**流量**和**端点一手数据**的能力，以及微剧本半自动化响应事件，结合 MDR 的及时支撑，可以作为 SOC 方案的底座，是**当前 SOC 现代化改造的重要组成部分**。
- Gartner认为基于**XDR**技术的新一代安全运营方案的**升级**可有效解决安全运营**核心**问题，也是**必然趋势**

核心能力

资产与脆弱性

定位到人

资产唯一标识对应到身份

数据来源：准入、AD、资产系统/ CMDB、人工维系/录入

脆弱性展示

脆弱性及基础信息

数据来源：各类安全产品、漏扫产品

定位业务

资产所属业务/所属责任人

数据来源：资产系统/ CMDB、人工维系/录入

脆弱性优先级排序

脆弱性排序计算因子：

对应资产重要性，资产对外暴露属性，攻击者触达难易程度，是否存在利用方式，是否有内外部攻击成功过；

数据来源：
资产台账、主机探针/主机安全、流量探针、内外部情报、各方产品脆弱性信息

资产清点

端口、应用、web资产、框架、中间件、系统、账号、进程……

数据来源：主机探针/主机安全、流量探针、资产系统/CMDB、人工补录

检测、调查

组件检测

基于组件能力检测出的安全日志，此部分检测效果依托于组件检测引擎
数据来源：端点、网侧检测组件的安全检测日志

原始日志检测

攻击者行为痕迹信息：进程、注册表、命令执行、文件执行、wmi、可以启动项、原始流量访问跟踪、内存行为异常、账号异常行为等原始遥测数据
数据来源：端点数据、网络探针原始数据采集、第三方可开放原始审计数据

少量精准事件聚合

还原出攻击链

端+网攻击上下文信息

数据来源：端+网探针采集、第三方开放遥测数据

告警举证聚合

告警信息/安全日志

数据来源：多方安全设备告警

威胁定性

降低运营成本

数据来源：聚合后的告警和攻击事件

E+N复合分析

IOA、IOC

man-in-the-AI

关联分析

全网威胁调查

事件、告警+攻击者行为痕迹信息

数据来源："多方告警数据"+"端点数据遥测、网络探针原始数据采集、第三方可开放遥测数据、原始审计数据"

响应

事件触发+情报匹配

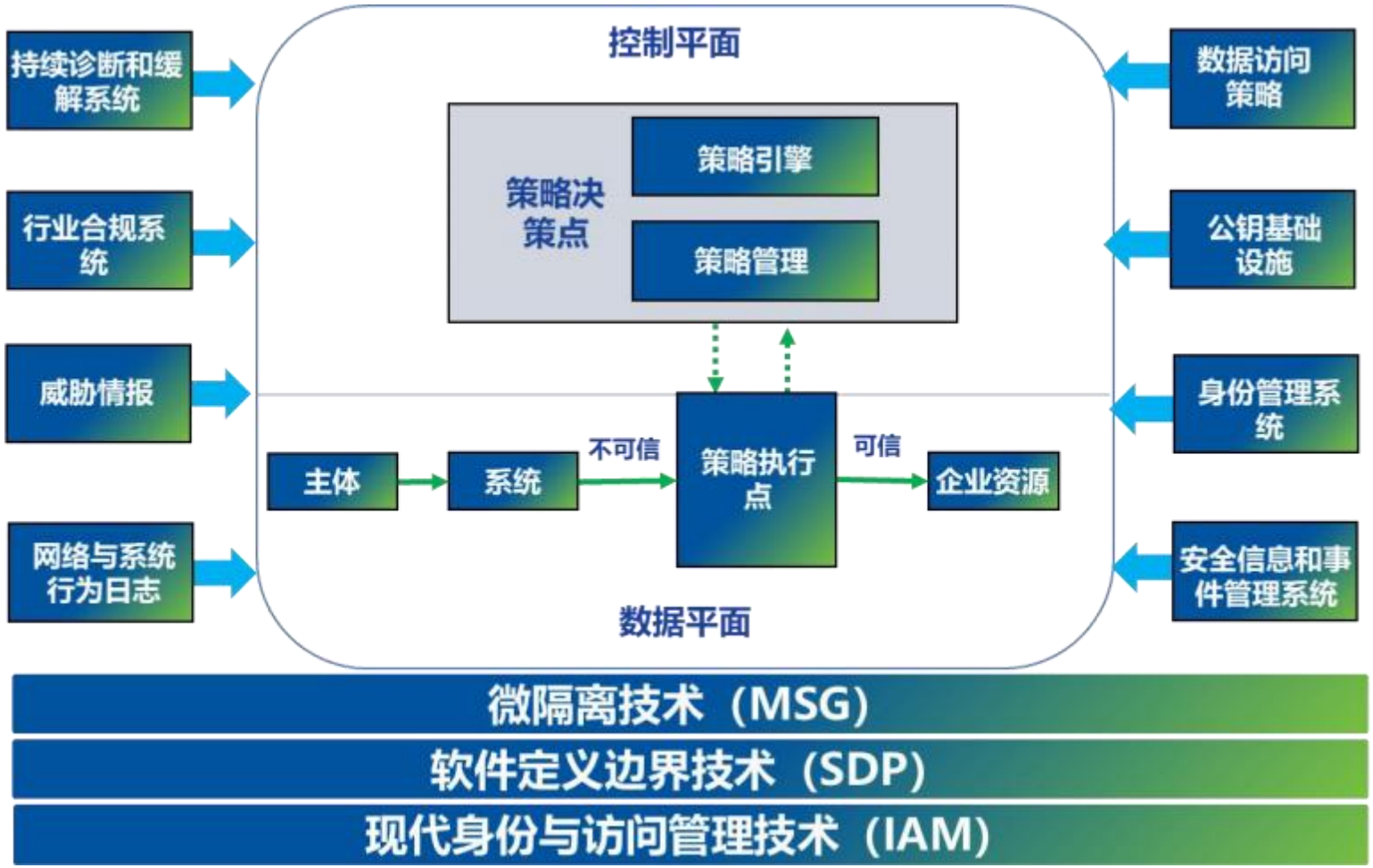
响应对象：
攻击威胁实体：IP、端口、文件、DNS、进程、主机、用户

响应优先级：
攻击者情报：IP、端口、DNS、攻击画像、所属组织（辅助研判）

响应分级：
1、自动化处置
2、SOAR
3、人工研判

2、零信任架构和关键技术

零信任架构核心组件由控制平面和数据平面构成（支撑系统称为控制平面，其他部分称为数据平面），数据平面由控制平面指挥和配置。同时，多个数据源提供输入和策略规则，供策略引擎在做出访问决策时使用



软件定义安全（SDP）

通过“控制器+代理网关”的形式定义边界，融合动态权限控制和多源信任评估，属于南北向流量控制。

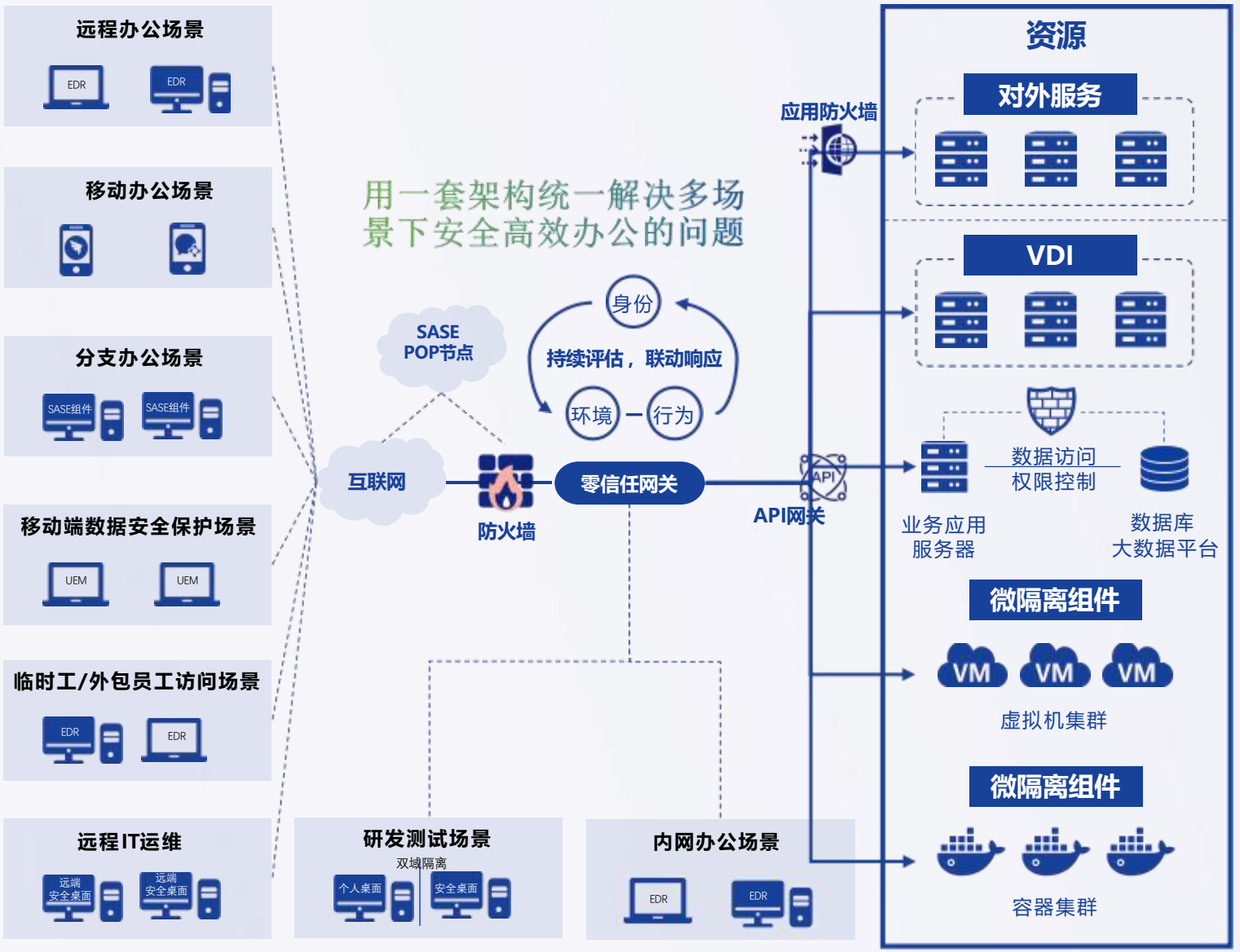
微隔离（MSG）

通过微隔离的形式控制东西向流量，结合终端管控和安全检查能力强化信任评估和管控能力。

增强型身份治理（IAM）

通过精细化的身份识别和权限设置实现基于身份认证的访问控制。

零信任应用场景



远程办公场景：

所有远程接入访问均需经过身份验证及可信确认，再经过零信任网关加密转发，极大减少内部系统被非授权访问的行为。

移动办公场景：

通过零信任系统， 为H5应用构建安全接入平台，实现更安全、体验更好、适应性更强的移动办公安全接入方案。

分支办公场景：

通过SASE技术，实现分支办公场景的安全接入以及统一安全运维管理，达成安全与效率的平衡。

内网办公场景：

以流量身份化、动态访问控制等关键技术，为企业内网访问重塑内网安全边界，减少内部资产被非授权访问的行为。

移动终端数据保护场景：

为用户构建 “双域空间”办公平台，实现业务系统的安全边界清晰化，以及数据落地后的安全保护，防止数据泄密。

IT运维、 研发测试场景：

通过桌面云的方式，实现办公和上网隔离，既满足日常办公需求，又能防止研发测试等敏感数据外泄。

除上述场景外，还有一些场景，如数据中心服务间访问、数据共享、第三方接入等，将也会在零信任架构的保护范围之内。

零信任安全访问建设路径

1 架构建设及零信任远程访问

2 架构优化及零信任内网访问

3 零信任服务访问

零信任基础架构及零信任远程访问建设

- 建设零信任访问网关，覆盖**远程接入用户的B/S、C/S应用、移动应用的访问**；
- 建设**零信任控制中心**，包含信任分析引擎，汇总分析评估用户访问的风险，实现信任判定；策略控制服务建设，管理零信任访问网关，实现动态的认证策略调整和权限控制能力；
- 部署**零信任客户端代理**，覆盖远程接入的终端，实现对终端的安全状态感知和信任评估

零信任架构的优化及零信任内网访问建设

- 建设**零信任访问网关**，覆盖**内网(IV区）终端用户**的应用访问，部署零信任客户端代理，实现对内网终端安全状态感知和信任评估
- 结合内网终端的使用特点，针对性建设**信任分析模型**和零信任访问控制策略
- 零信任控制中心统一纳管网省的**上网行为管理**，实现统一的安全策略及零信任的上网管控
- 优化远程访问的动态访问控制策略、终端检测策略等，优化多源风险的**综合信任分析模型**，考虑不同用户类型、终端类型、应用类型等因素，实现安全与效率的平衡

零信任服务访问建设

- 建设**零信任API网关**，覆盖应用之间API接口的场景
- 实现零信任控制中心对API网关的**统一管理和控制**
- 采集API访问数据，创建API访问的**信任模型**，实现服务访问的持续监测、动态访问控制

3、数据安全-API安全在金融行业面临挑战汇总

业务架构云化、微服务化

随着金融业务的微服务化、无服务化、边缘计算、应用交付SaaS化趋势下，**API承载了应用各组件间高密度高价值数据流动**，成为数据交互最重要的传输方式之一

数据中台的建设与发展

金融数据中台的建设打破了“数据孤岛”，通过平台化建设形成了一套高效可靠的数据资产化体系和依赖数据金融疗服务能力，**API成为数字服务化过程中重要的数据传输通道**

数据共享开放日益普遍

金融数据在流动过程中产生价值，为高质量金融服务，高质量患者体验，提高金融水平做出贡献，数据共享开放将变得越来越普遍，**API成为数据共享开放的主要形式之一**

API安全面临的挑战

API资产难看清

- 接口数据总量
- 涉敏API发现
- API脆弱性
- 流转访问可视

接口风险难监测

- 权限有无风险
- 接口有无风险
- 访问有无风险
- 行为有无风险

防护措施难有效

- 缺少访问控制
- 缺少数据发现
- 缺少属性条件
- 规范落地困难

泄密事件难溯源

- 什么数据泄密
- 什么人员泄密
- 什么时间泄密
- 查泄密上下文

API数据防泄漏方案建设思路

资产管理

- API接口自动识别梳理
- API接口细粒度画像
- API敏感数据资产梳理
- 应用资产梳理
- 账号资产梳理

数据防护

- API数据动态脱敏
- API接口水印
- API攻击防护
- 应用攻击防护

响应处置

- API接口访问日志审计
- API数据泄露溯源
- API数据安全风险联动处置

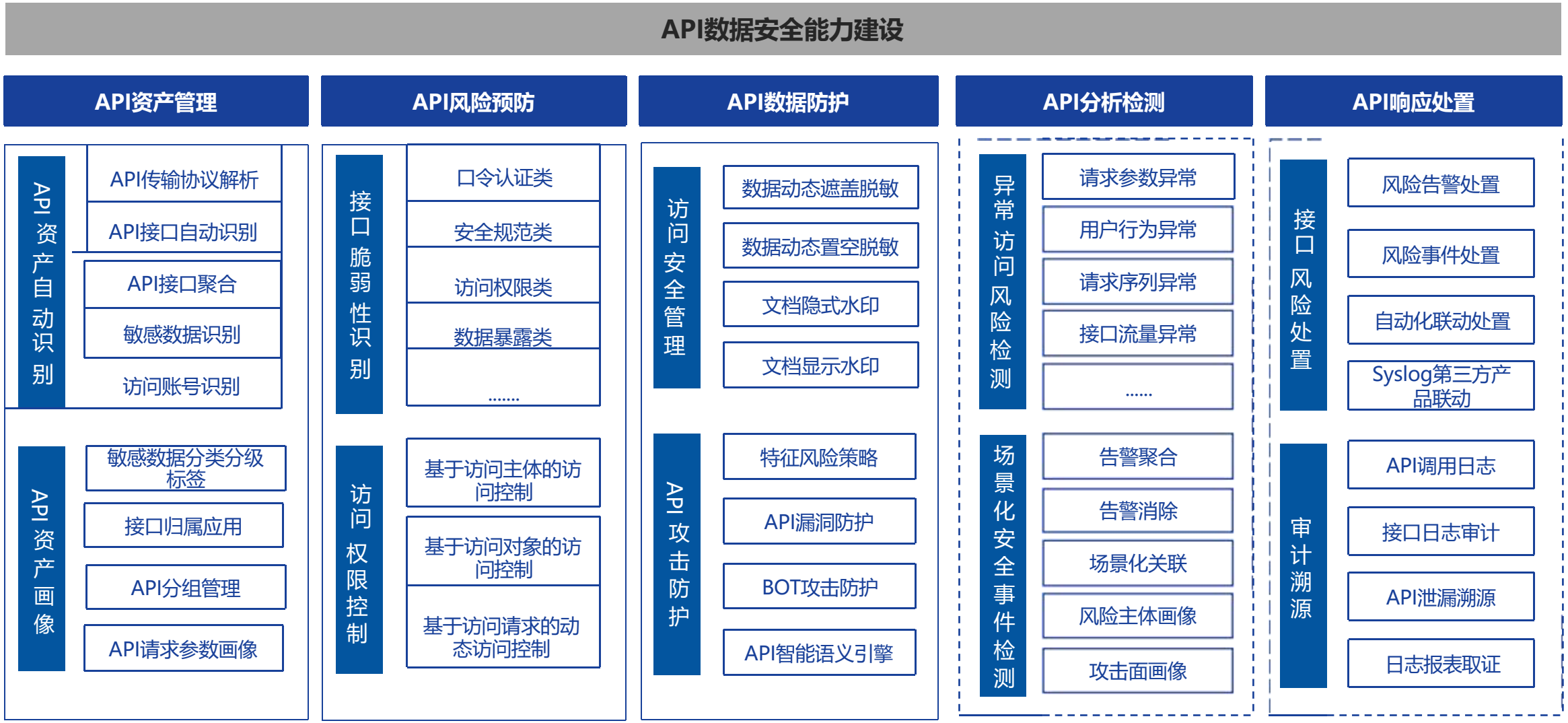
风险预防

- API攻击面管理，识别接口脆弱性隐患，提前进行风险闭环
- 通过API访问权限控制收缩暴露面，提前预防数据泄漏风险

分析检测

- 基于策略的数据安全风险检测
- 基于UEBA的数据安全风险检测
- 基于数据安全泄露场景的数据泄露风险事件检测

API数据安全建设能力架构图



4、数据保护：数字化工作空间建设方案

构筑数字化工作空间的全链条信任环境

标星*部分为可选组件

Workspace形态：一站式工作台

数据保护：分级数据防泄密

✓ 数据不落地（VDI）

通过虚拟桌面云办公时，数据存储在远端服务器集群，本地无数据落地；并通过双向拷贝管控，保障数据可控传递

✓ 数据落地加密（UEM）

未通过虚拟桌面云办公，可在本地部署数据虚拟沙箱，实现办公桌面的数据自动落地加密，并通过剪切板隔离技术，实现办公桌面与个人桌面单双向的拷贝隔离

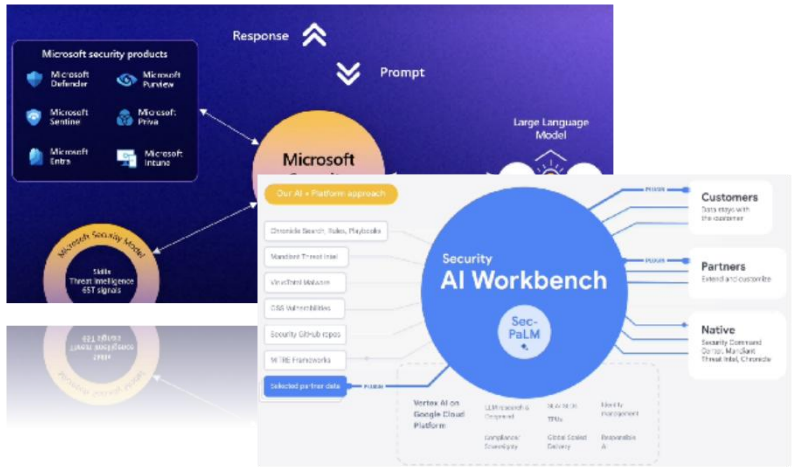
✓ 网络隔离确保合规

安全桌面内不允许访问未授信地址，个人桌面不允许访问内网业务系统，避免个人应用通过网络获取企业数据

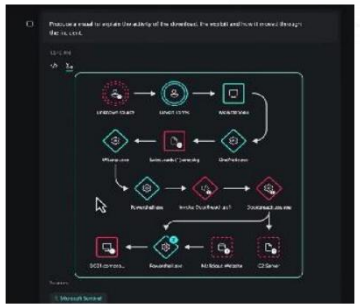
✓ 多重手段防止泄密

安全桌面可开启剪切板隔离、数据导入导出控制，防截屏等多种数据管控手段，同时可开启屏幕水印，对屏拍等行为进行震慑、审计和溯源。

5、23年，大语言模型成为网络安全的热点方向



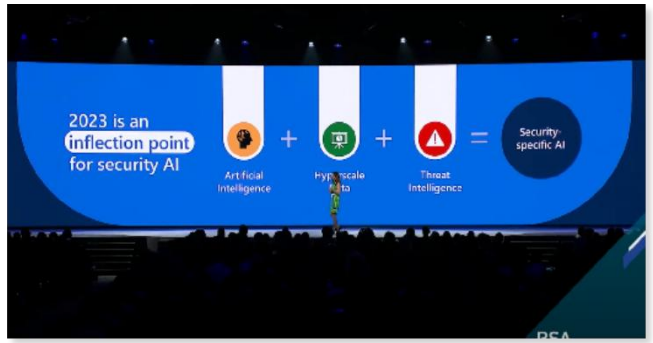
安全事件调查



安全知识解答

微软 Security Copilot / 谷歌 Sec-PaLM

- 安全事件解读与分析
- 优先级排序与深度分析
- 网络安全知识助手
- 安全能力强化学习
- 内部安全态势评估总结、创建汇报文档



- 2023年RSAC，**60多家安全厂商发布AI驱动战略或产品**
- RSA首席执行官：**AI将成为网络安全的基础**
- 微软联合副总裁：**2023年是AI安全的拐点**

RSAConference

Gartner

Hype Cycle for Security Operations, 2023

Organizations will benefit from generative cybersecurity AI as it can improve efficiency and shorten response times to cybersecurity risks and threats

……

Cybersecurity technology providers can exploit generative cybersecurity AI to improve existing workflows, be a proxy of existing analytics, generate security configuration or realistic attack data.

组织将受益于生成式网络安全人工智能，因为它可以**提高效率并缩短对网络安全风险和威胁的响应时间**

.....

网络安全供应商可以利用生成式网络安全人工智能来改进现有的工作流程，开展安全分析，生成安全配置或真实的攻击数据。很快，**自动化值守能力将出现，可以自主基于高级指引运行，而不需要频繁提示对话**

基于思维链和上下文学习的自主值守、研判、处置

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

思维链能力 CoT

- 类似于逻辑推理能力，可以从现象看到原理，可以将问题分步骤拆解并解决
- 神奇咒语： **Let's think step by step**
- 此能力在OpenAI投喂了代码作为训练数据后大幅增强

上下文学习ICL

- 通过少量样本Few-shot、一个样本One-shot甚至零样本Zero-shot的情况下，通过简单提示，模型就能通过类比输出新任务的结果
- 非常像人类，可以通过之前的知识积累解答没有学习过的问题

安全GPT构建全景

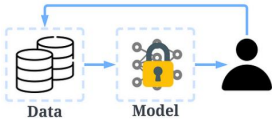
数据准备（通用+安全）

- 设备日志
- 业务流量
- 告警事件
- 安全百科
- 电子书籍
- 期刊论文
- 网页爬取
- 新闻数据
- 行业数据
- 其他语料

数据清洗

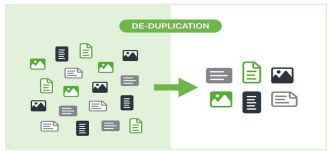
- 特殊字符
- 格式编码
- 繁简转换
- 分段分句
- 违禁词过滤
- 语种筛选

低质量文本过滤



高质量文本	低质量文本
漏洞编号：cnvd 危害等级：中 影响产品：xxx	免责声明：xxx 谢邀专家：xxx 关注+点赞收藏

文本去重去噪



增量预训练

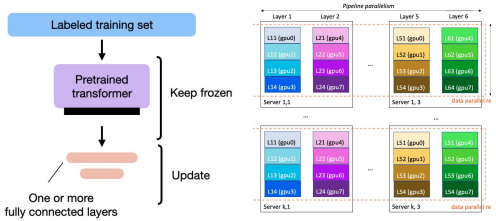
[通用数据：世界知识]

唐代之所以能广泛吸取西域民族、北方民族及佛教的文化，正因为它拥有一个秦汉以来建立的强大的中华文化传统。

[安全数据：行业知识]

横向攻击是在一个已被入侵的网络环境中，攻击者试图扩展他们的攻击面，将入侵范围从初始受害主机扩展到其他网络节点。

数据配比和增量预训练



SecurityGPT 预训练基座

指令微调

通用指令

- 真实多轮对话指令
- COT推理任务指令
- 复杂任务指令
- 人类价值观对齐

安全指令

- 漏洞解释指令
- 恶意家族介绍指令
- 安全术语指令
- 安全百科指令
- 身份信息指令
- 情报趋势解读指令
- 指代词消解指令

- 安全问答
- 上下文理解
- 产品数据联动
- 合规检查

部署推理

SecurityGPT 大模型

- 安全问答
- 上下文理解
- 产品联动
- 合规检查

泛化 迁移

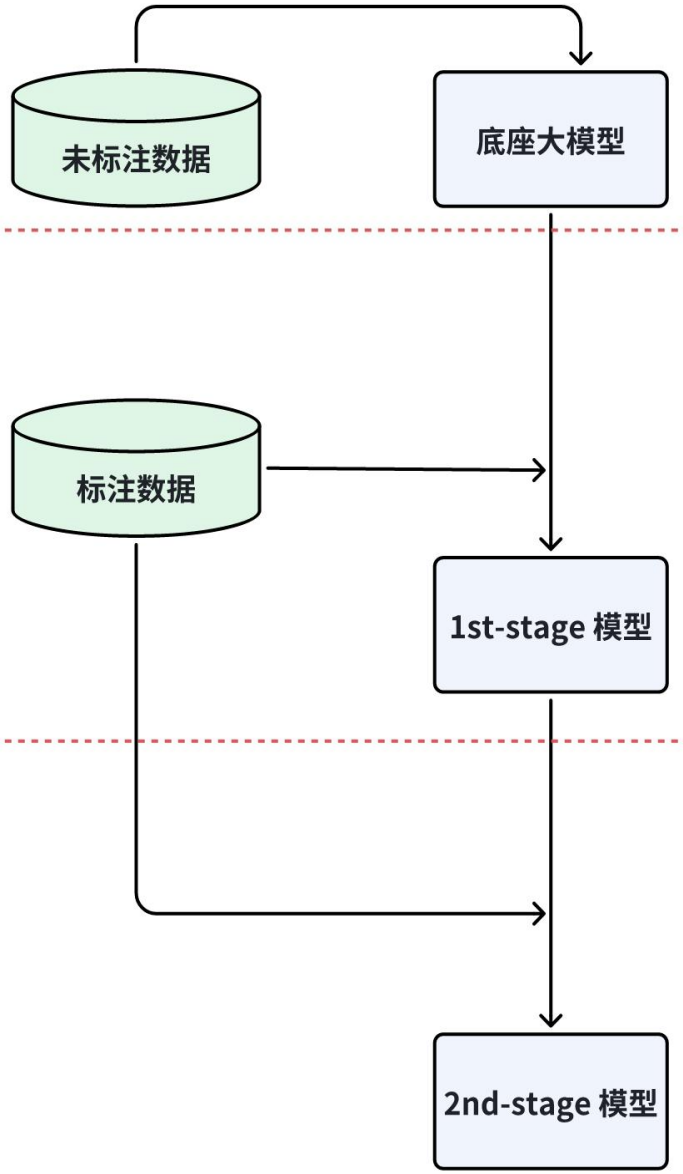
安全领域相关任务

- 自然语言对话
- 流量研判
- 事件解析
- 日志关联
- 建议生成
- 其他生成式能力

行业领跑 保持跟进 行业领跑

- **500+** A100/A800 底层算力支持，4090支撑推理，逐步适配/切换昇腾体系
- 百亿参数MoE架构，2500亿预训练Token，800万微调指令。
- 中英双语，上下文长度**16k**，使用Byte-Pair Encoding 作为分词方法，并使用了**Flash-Attention**、**混合精度**等为训练和推理提速。

检测大模型提升检测能力：MoE架构

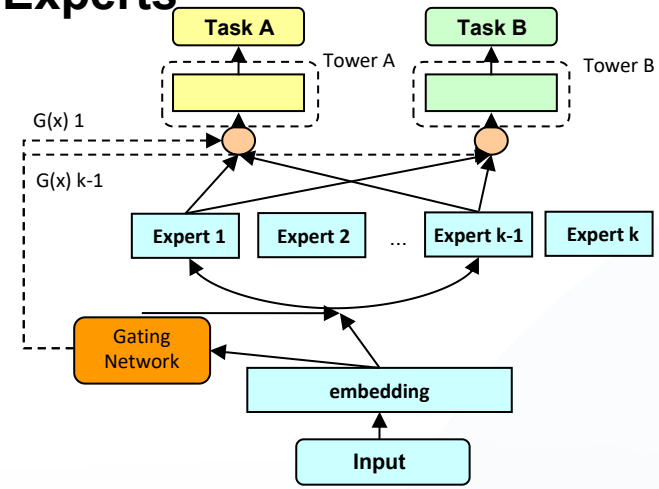


预训练

通过对大规模垂直语料无监督训练，提升模型底座对安全理解能力

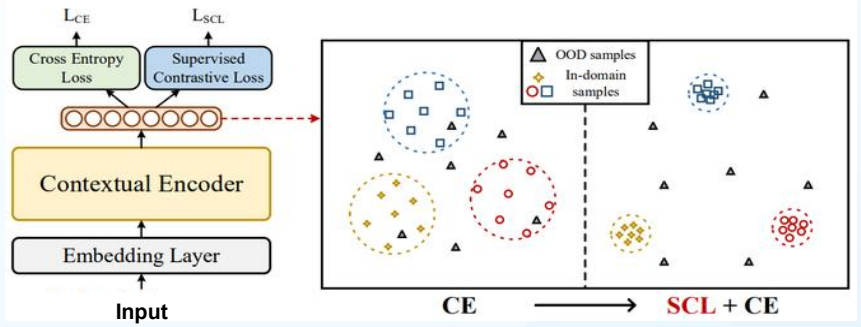
多任务学习 by Mixture of Experts

- 相较单任务训练，通过多任务学习能显著提升检测大模型在各下游任务上的表现和泛化能力
- 通过将模型进一步拆分成更小的专家子模型，减少了每个子模型的复杂度，降低了训练成本，并可以动态调整和按权重分配不同样本到不同专家子模型，提高了检测大模型总体的能力上限



对比学习

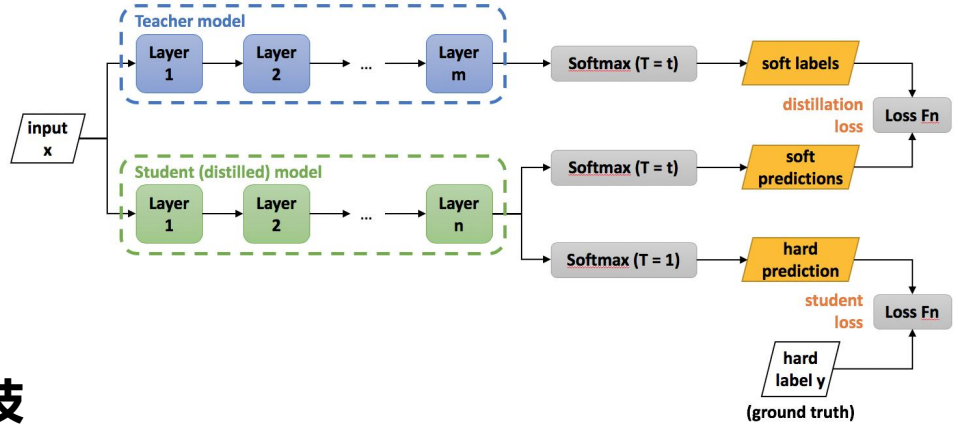
通过增加对比学习辅助任务，模型能进一步提升在对抗场景上的表现，同时能增强检测大模型在不同下游任务上的鲁棒性



检测大模型提升推理效率：多阶段的推理优化

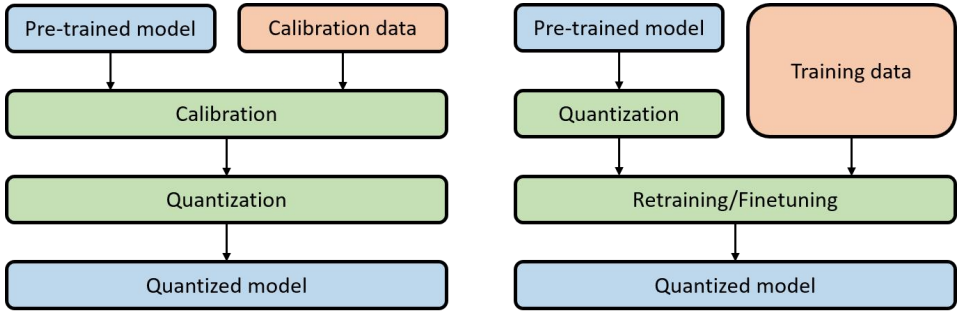
知识蒸馏

利用知识蒸馏的能力，将大模型的学习能力以及泛化性迁移到小模型上，并有效降低推理的成本



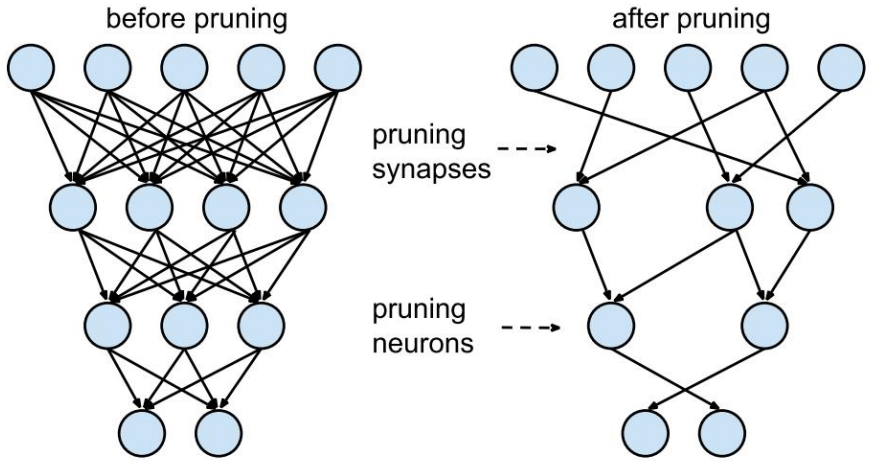
模型量化

使用量化感知训练(Quantization Aware Training, QAT)和训练后量化(Post Training Quantization, PTQ)等量化策略，能有效减少模型内存和存储占用，降低功耗并提升计算速度



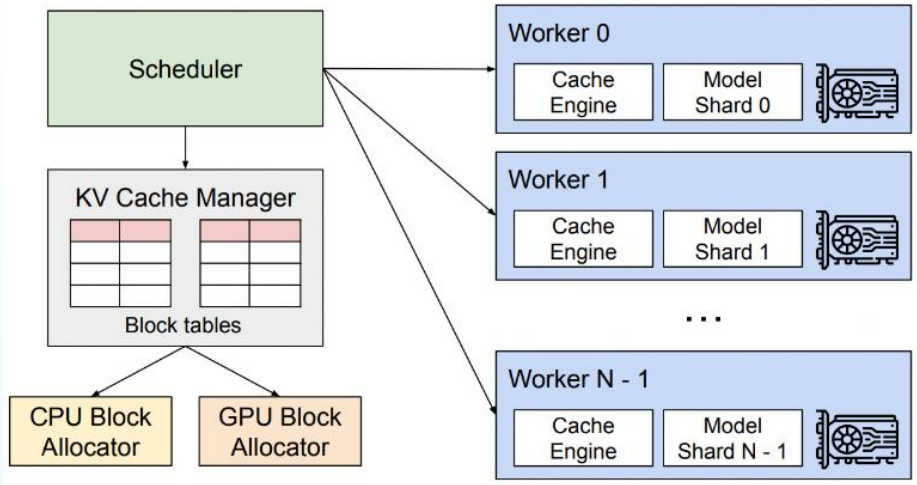
模型剪枝

通过删除模型中不必要的神经元或权重参数，减少模型的计算复杂度和存储空间，从而提高模型的存储效率和计算效率



Attention机制优化

通过PagedAttention 对注意力 key 和 value 进行内存管理，同时能连续批处理接入的请求，大幅提升模型推理性能和吞吐量



产品级的检测实践：规则引擎与大小模型的协同

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

FW

NDR

EDR

其他设备

攻击流量、日志

70% 已知威胁

规则/情报引擎

- WAF规则
- IPS引擎
- 启发式病毒库
- Snort
- IOC情报
- 特征库识别
- ……

匹配攻击特征

25% 变种攻击威胁

行为引擎(小模型，AI 1.0)

- 异常外联引擎
- SAVE引擎
- 行为聚类分析
- DNS安全检测
- 二分类/多分类
- UEBA异常行为
- ……

识别攻击行为

5% 高对抗的入侵威胁

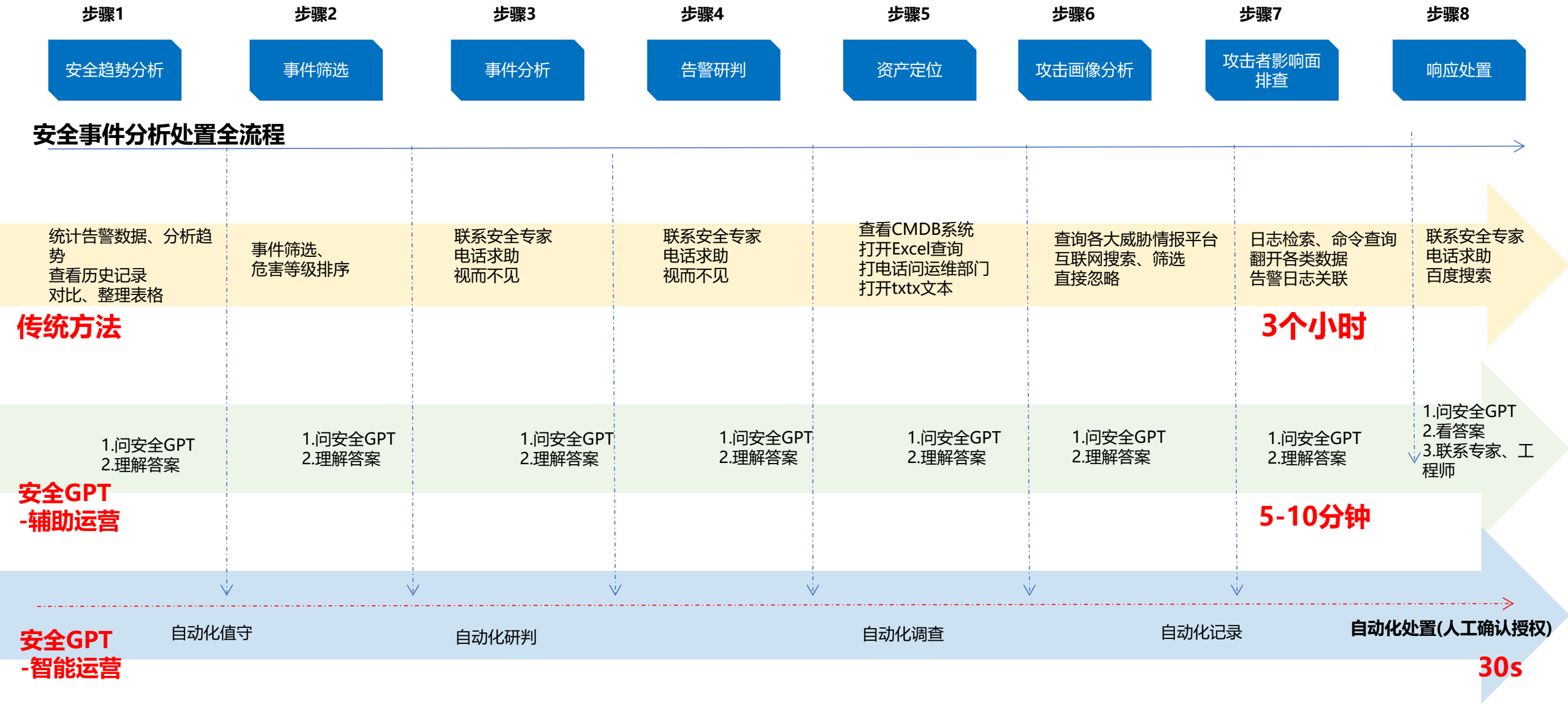
安全GPT引擎(大模型，AI 2.0)

安全GPT

- 0day利用及后续行为
- 编码绕过的Nday
- Web类变种黑客攻击
- 编码混淆、绕过攻击

理解攻击过程

安全GPT加持下，安全运营生产力的飞跃




SANGFOR
深信服科技
深信服智安全
SANGFOR SECURITY
谢谢聆听
让IT更简单，更安全，更有价值！