网络安全创新大会
Cyber Security Innovation Summit

建设新一代金融业安全运营与智慧感知平台

马晨怡 光大银行科技部安全处安全运营工程师

全球网络安全形势

网络安全创新大会 Cyber Security Innovation Summit

关键设施安全提升到国家安全高度

- 网络攻击成为全球仅次于“极端天气”和“自然灾害”的**第三大威胁**。
- 据联合国裁军研究所报告显示，世界多国已经成立了总数超过**220支**专业网络战部队。
- **国家入局**关键基础设施攻击，网络安全成为国家安全战略
- **网络武器**研发投入巨大，已具备多种打击能力。
- 攻击范围**扩散多领域**，军工、水电民生、金融、金融

委内瑞拉遭受某组织策划的严重的网络安全攻击，导致全境大面积断电，国家接近崩溃。

网络部队在打击“伊斯兰国”的战役中支持美国及其盟国成功的实施打击活动。

网络安全上升为国家战略领域

- 各国加快网络空间安全的战略举措和法规研究、制定工作，网络空间安全和治理成为各国战略安全的“国之大事”。
- 高度重视**关键基础设施**安全
- 配套系列标准发布，重视**新技术风险**
- 数据保护方向完善，**重视个人隐私权益保护**
- 由政府、行业组织和**社会**公共监管

2017年7月颁布《网络安全法》，2020年10月21日，全国人大法工委公开就《中华人民共和国个人信息保护法(草案)》征求意见

2015年美国签署《2015年网络安全法案》

2016年7月6日欧盟正式通过首部网络安全法《网络与信息系统安全指令》(NISD)

网络空间“无硝烟”战争频度加重

- 恶意攻击者队伍不断壮大，攻击方式呈现多样化，手段包括诈骗、钓鱼、勒索、社工、ATM感染、域名劫持、资金盗取、信息泄露等。
- 网络安全形势日趋严峻，APT攻击增多
- 黑客攻击手段不断升级
- 网络诈骗产业规模迅速扩大，信息泄露严重

荷兰三大银行频遭 DDoS 攻击，导致网络服务业务下滑

朝鲜Hidden Cobra组织通过一种新的Flash 漏洞攻击土耳其金融系统。

世界多地 ATM 机遭遇“Jackpotting” 攻击，自动吐钞

国内网络安全政策制度体系

以《网络安全法》为纲，《关键信息基础设施保护条例》为指导，参照网络安全架构和安全保护基本要求等国家标准，以”实战化，体系化，常态化”为新理念，持续加强“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”六防能力建设。（三防六化）

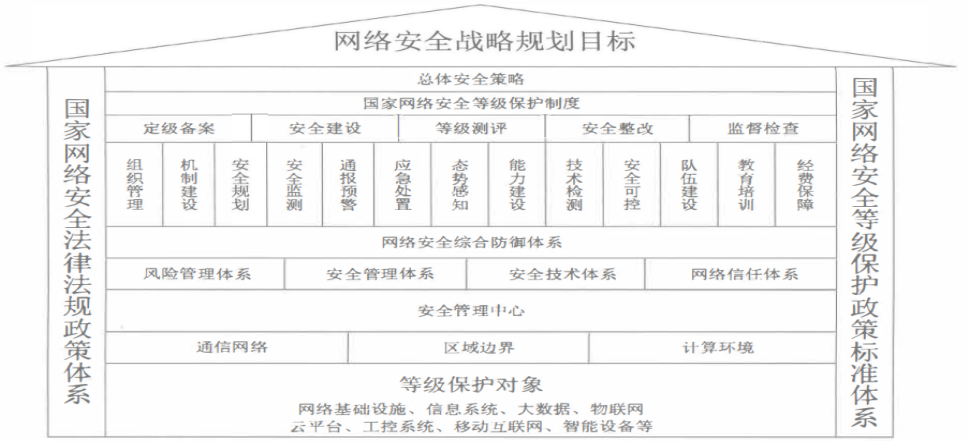
法律 网络安全法

法规 关键信息基础设施保护条例

国标

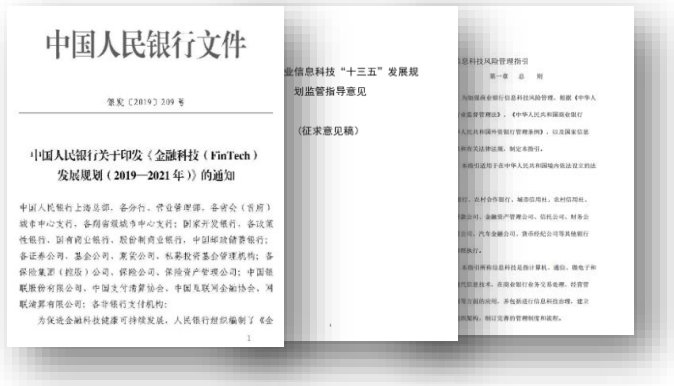
补充性国家标准

- 网络安全框架
- 安全保护基本要求
- 检查评估指南
- 保障指标体系
- 安全控制措施



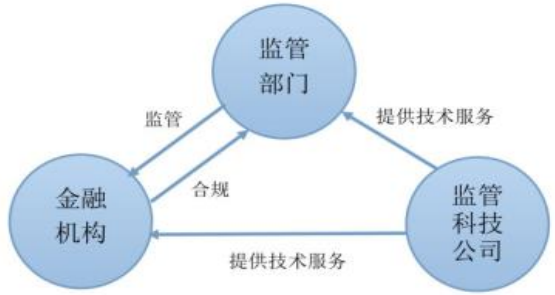
金融行业态势感知体系发展方向

在信息安全形势愈发严峻，金融行业作为国家关键基础行业面临巨大挑战，上级监管部门发布多项安全运营与态势感知相关指导意见，安全监管要求愈发全面和严格，同时考虑企业自身安全发展诉求，对态势感知体系建设提出新的要求。



- 着力完善**金融信息基础设施建设**，着力巩固金融网络安全，增强安全生产和**安全管理能力**；
- 加强网络**安全态势感知**，动态监测分析网络流量和网络实体行为，绘制金融网络安全整体态势图，准确把握网络威胁的规律和趋势，实现**风险全局感知和预判预警。**
- 商业银行应依据信息科技风险管理策略和风险评估结果，实施全面的**风险防范措施,**
- ……

行业指导



- 金融科技应用成为银行业竞争新高地，但目前整个行业安全评估和安全技术投入不足，金融科技安全生态尚未形成。
- 现场监管力度增强，非现场检查内容丰富，监管要求趋于严格化，监管重心从制度层面转移到执行层面

金融科技发展和监管要求

- A、威胁检测能力
- B、攻击防御能力
- C、威胁监控能力
- D、事件响应能力
- E、漏洞运营能力
- F、安全态势感知平台建设

企业安全发展要求

网络安全攻防对抗升级

■ 网络攻击产业化、精准化、移动化、技术化

趋势一 用户个人信息泄露助长网络黑产发展

趋势二 针对金融APP的木马攻击呈现高度定制化趋势

趋势三 “羊毛党”造成的损失日益严重

趋势四 生物识别技术引入新的风险点

趋势五 短信验证风险依然需要高度关注

趋势六 互联网金融生态引入新攻击面

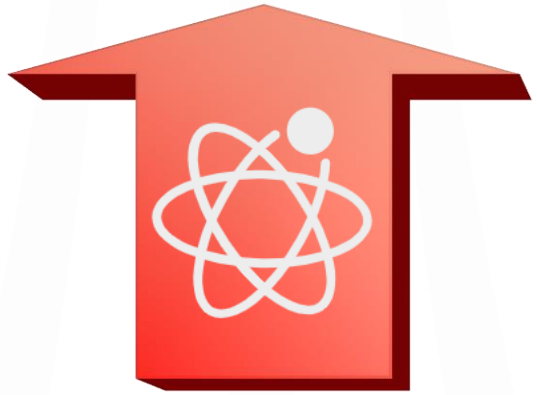
■ 攻防新态势

有组织的对抗增多 | **勒索软件成为头号敌人** | **人的因素倍受关注** | **漏洞数量创新高** | **隐私保护任重道远**

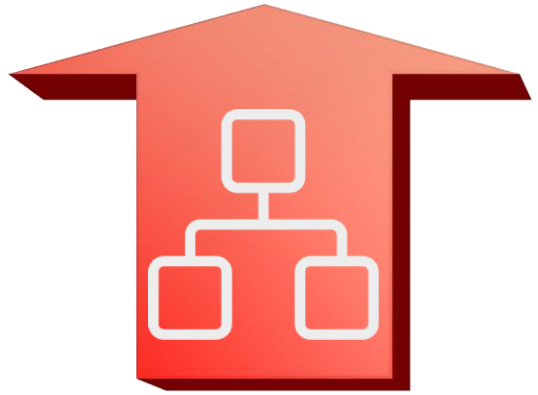
- 有较大规模组织的对抗日益增多，大量恶意网络攻击行为。
- 勒索软件加速演变进化，并在技术迭代、勒索方式（数据泄露+加密勒索）等方面不断进化，变得更加复杂和难以防范，一旦攻击得手能够快速横向移动导致企业业务瘫痪。
- 33%的企业网络安全或者数据安全事件与员工错误有关，企业员工的安全意识培训已经从可有可无的可选项变成“刚需”，安全意识培训是安全人士认为最有效的网络安全措施。
- 2020 年上半年业界总共提交9000 个安全漏洞，全年漏洞数量有望创下新高（突破两万），其中移动漏洞（Android 漏洞）数量同比增长50%。
- 个人金融C1、C2、C3级别信息，以及验证码、人脸等信息广泛运用到用户认证、业务交易中，使不法分享获取个人金融信息更容易，身份证、手机号、卡号金融信息三要素的组合资金欺诈频发。

平台建设新要求

理念升级



技术升级



组织升级

国际形势严峻

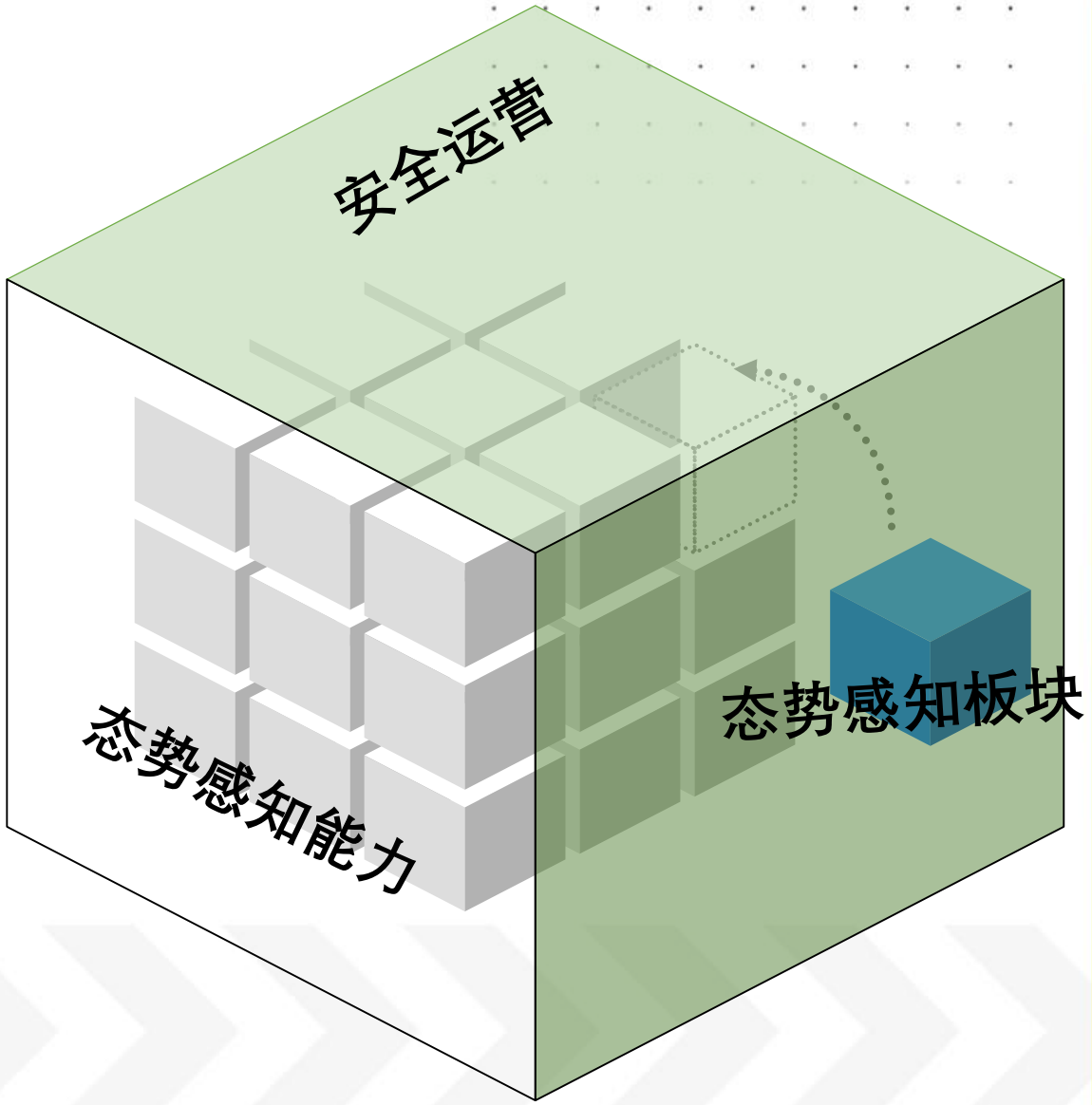
政策法制健全

安全发展诉求

攻防对抗升级

安全运营与态势感知关系

- 安全运营不等于安全态势感知，安全运营的范围更广泛，安全运营是一个工作领域，安全态势感知则是此领域下其中一种能力（围绕威胁）。安全态势感知平台就是为了提供这种能力支撑而建设。
- 安全态势感知平台不是一个独立的平台，更不是单一某家安全厂商的产品，是一个包含多个板块，各自分工，密切交互的生态。
- 核心：安全实时计算、安全数据图谱、安全AI、威胁态势感知与响应



理念升级

SIEM安全信息与事件管理

- 目标：
- 解决安全数据集中化和告警消减的问题；
- 特点：
- 安全设备日志统一收集
- 告警集中监控
- 安全事件分析及审计

SOC安全运营中心

- 目标：
- 支撑信息安全运营整体闭环，监测、分析、响应、协同工作；
- 特点：
- 流程电子化
- 分析智能化
- 防御协同化基

安全运营与智慧感知平台

- 目标：
- 围绕安全威胁发现、分析、处置开展深入能力建设，辅以大数据技术、人工智能、资产和情报实现安全态势感知。
- 特点：
- 以威胁感知为核心
- 安全实时计算为支撑
- 数据驱动
- 自动化、智能化、可视化

技术升级—智慧态势感知体系整体架构

智慧安全态势感知体系

网络安全法律法规政策体系

安全指挥与决策

专家系统 | 指挥系统 | 沙盘推演 | 事件协作 | 通知通告

安全感知场景

安全大脑

安全可视化

威胁检测 | 威胁分析 | 应用系统现象 | 安全事件流程 | 自动化响应 | 多维指标 | 威胁情报

实时分析引擎 | 离线分析引擎

安全数据中台

数据存储 | 数据索引 | 数据治理

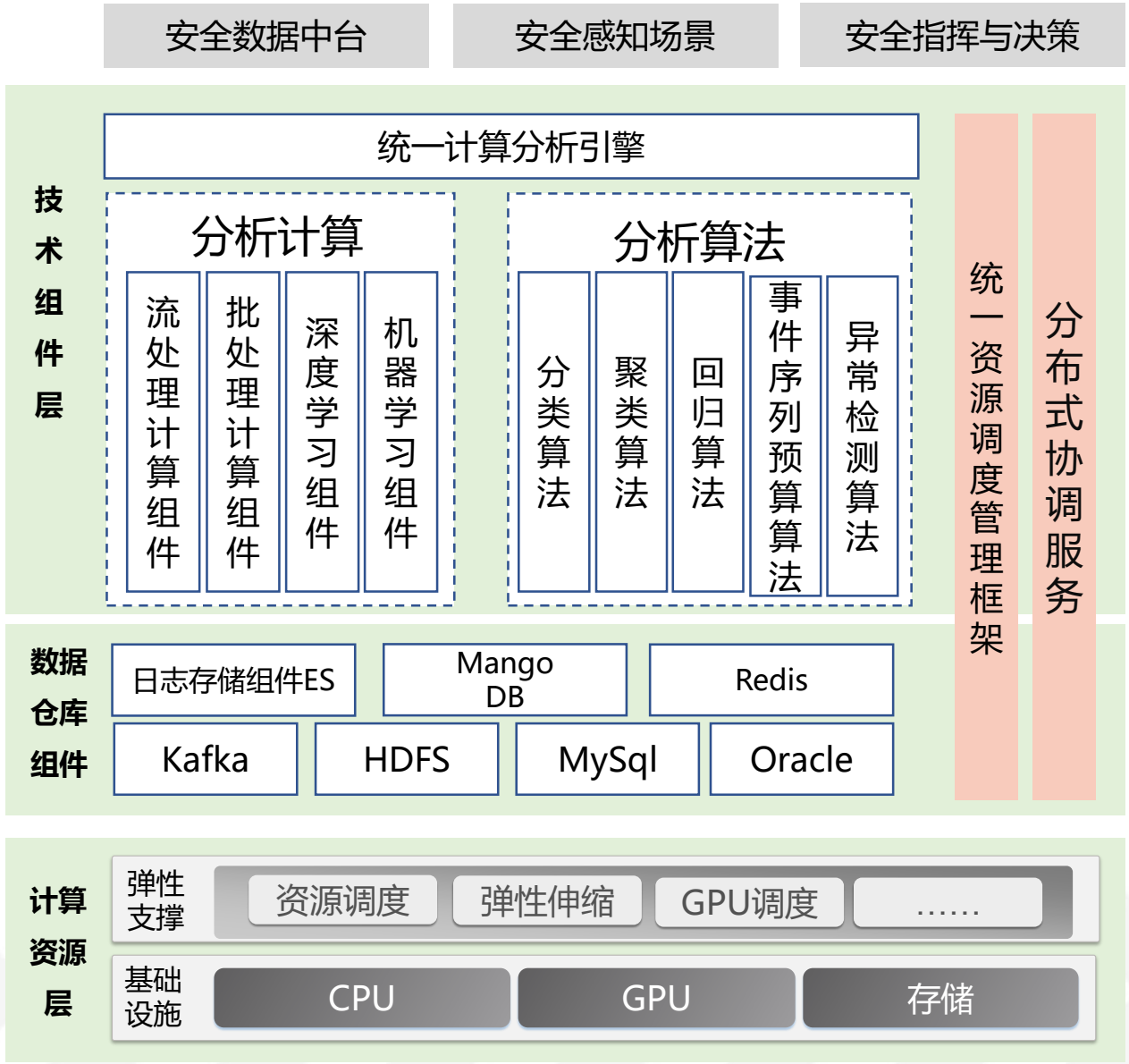
数据采集 | 数据处理

安全计算与存储平台

大数据存储 | 大数据检索 | 实时计算 | 离线计算

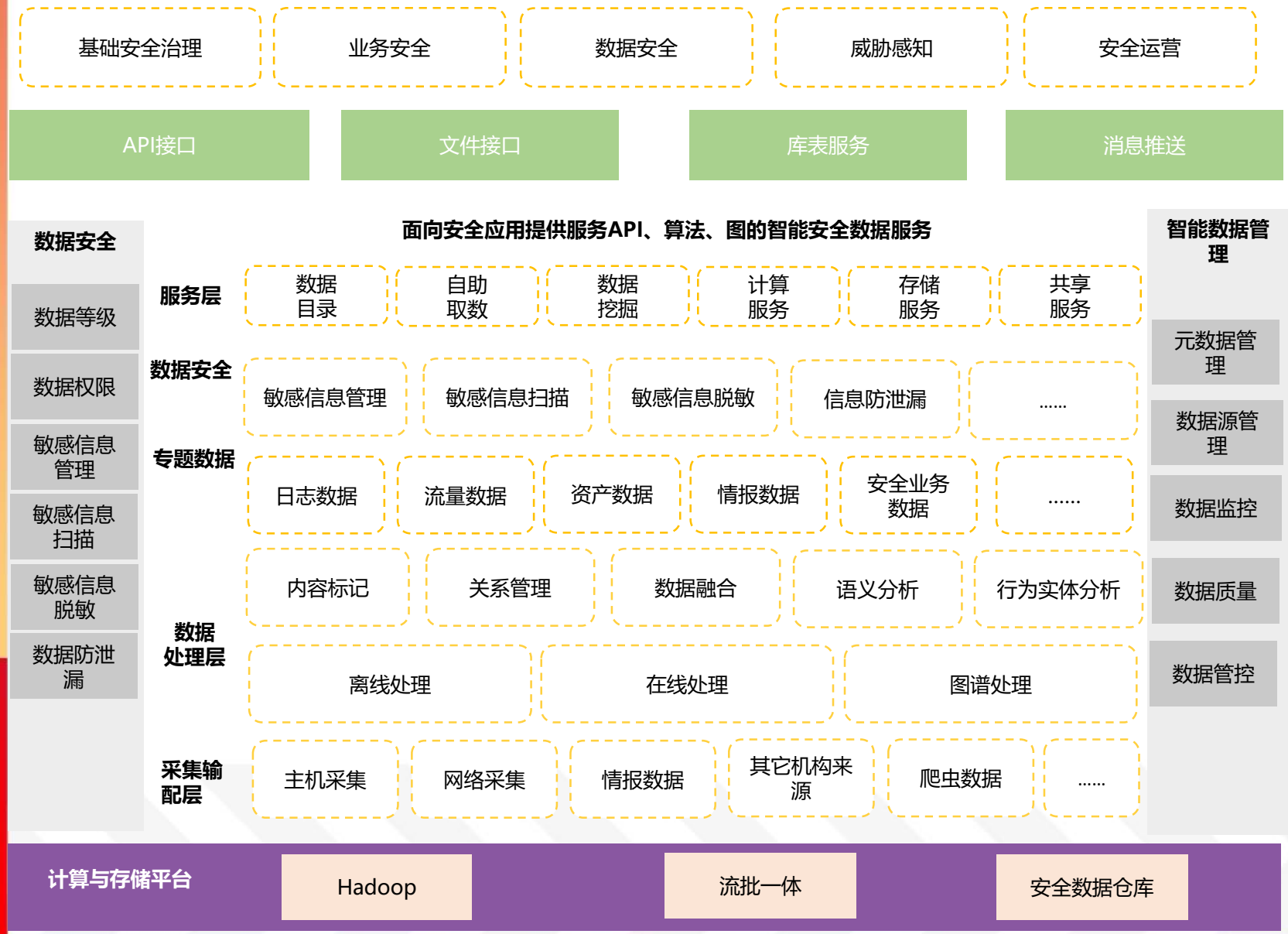
网络安全等级保护政策标准体系

安全计算与存储平台



技术指标	平台数据处理能力
数据处理能力	• 20亿条/天， • 3.4TB/天， • 处理性能峰值为100M/秒
实时查询能力	• 存储数据量2TB/天，可供查三个月内数据 • 300TB数据 • 30用户并发查询效率2秒以内
离线分析能力	• 3.4T/天，存储6个月; • 支持TB级数据备份能力 • 分钟级别离线分析能力
统计结果数据能力	• 1亿条/天 • 支持3个月存储150TB数据秒级实时统计
模型分析计算能力	• 支持40个模型实时分析计算

安全数据中台



- **数据服务：**根据上层威胁分析或者上层业务应用的需要对外部系统提供海量、快速、规范的数据服务
- **数据萃取：**构建网络安全态势要素原始库、资源库、主题库、知识库,实现海量安全数据的有效融合
- **数据治理：**数据治理主要对多源、异构数据进行清洗和过滤、标准化归一化、标识、分层等操作，对杂乱的数据进行处理，逐步对数据进行萃取，提炼价值，形成对上层提供数据服务的能力
- **数据采集：**通过主动采集和被动接收的方式，采集网络安全防护系统数据，服务器及主机数据、网络骨干节点数据、资产脆弱性数据、威胁感知数据、协同合作数据六类数据。

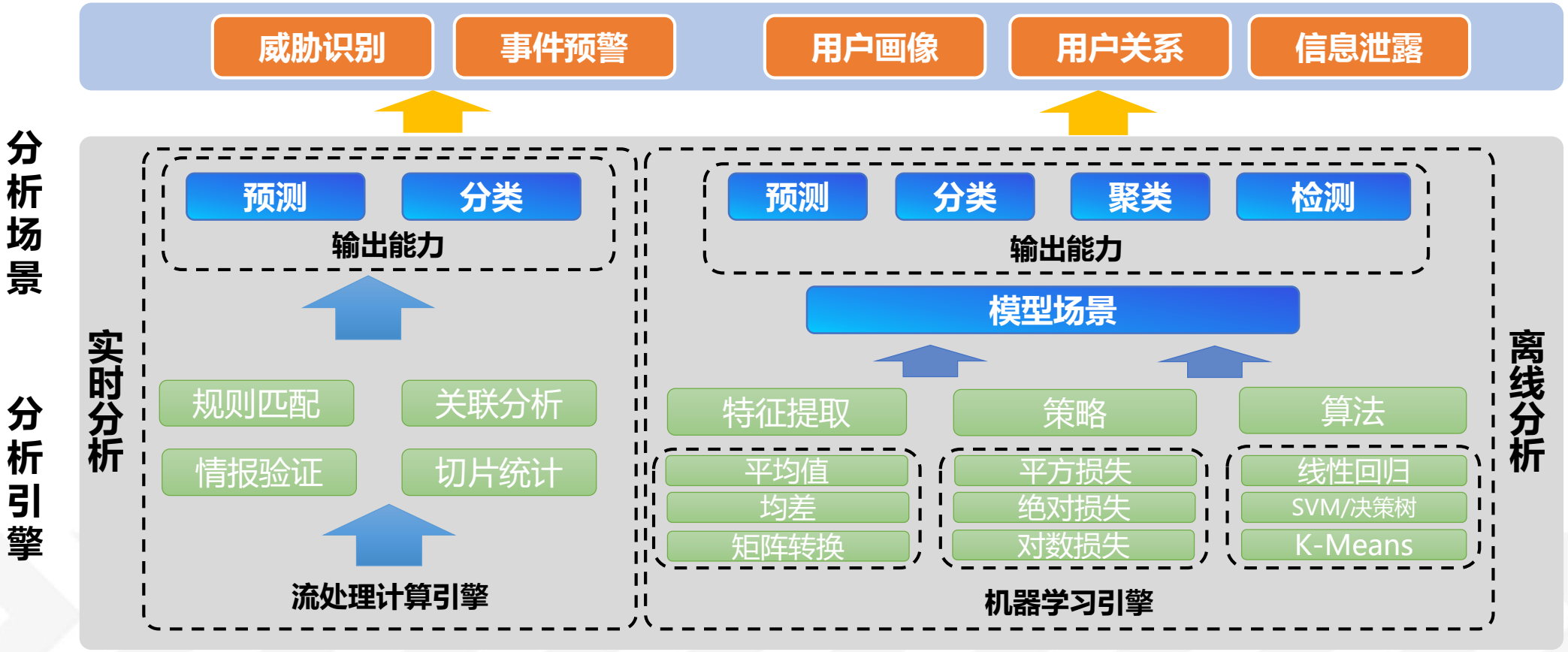
安全数据图谱

安全数据图谱将数据横向划分为日志域、流量域、资产域、情报域、业务域等多个主题域。

应用日志	系统日志	终端日志	网络日志	安全设备日志	中间件日志
DNS流量	HTTP流量	邮件流量	HTTPS流量	互联网出口流量	云内东西向流量
应用资产	系统资产	网络资产	终端资产	安全设备资产	暴露面资产	人员资产
恶意IP	恶意URL	漏洞库	恶意邮箱	恶意样本	处置预案库	知识库
威胁告警	异常行为	业务预警	访问行为	恶意代码	脆弱性	运营指标

安全大脑

安全大脑，作为智慧安全态势感知平台的核心，其充分发挥大数据平台技术的优势，以安全数据为基础，综合利用人工智能、行为分析、大数据分析、知识图谱、关联分析等多种分析技术，构建安全分析场景，对海量数据进行多维、智能的持续分析，实现对威胁的精准识别和研判，威胁自动化响应，通过持续动态学习机制，持续进化企业安全防御能力。



安全大脑应用效果

通过安全大脑建设，安全态势感知能力将从检测、分析、处置、治理四个方向提升。

一体化安全监测、防御能力

- 安全设备与态势感知平台的大数据能力实现打通，为安全设备端进行大数据分析赋能；
- 安全设备端与大数据端的能力逐渐实现分层和协作，为安全防护架构有带来质的提升；
- 黑灰产与我行的对抗转变为人-机或机-机对抗，我行的对抗效率是质的飞跃

安全治理能力

- 机器代替人力，风险、事件和漏洞的发现能力和效率成指数提升
- 依托大脑逐步实现安全治理的动态分析和风险预警，管理效率得到明显提升

安全分析自动化研判能力

- 实时的大数据分析能力有监督的实时学习能力
- 无监督的实时学习能力
- 动态的学习与防御能力

监控->分析->防御全流程自动化处置能力

- 依托安全数据湖输出的数据能力，逐渐形成全面的安全监测场景覆盖
- 经过专家训练和调教的分析模型7*24小时运转，配合强大的安全计算能力支持，高效识别安全威胁
- 经过精细编排的处置动作，根据分析结果自动化地适时启动高阶和低阶防御模式，消除风险于无形

组织升级

网络安全创新大会
Cyber Security Innovation Summit

Before

监控团队

分析团队

团队资源不足，
基于监管合规进行工作开展

After

攻防团队

监控小组

分析小组

攻击小组

数据团队

数据治理小组

数据建模小组

团队资源按需补充，组织分工精细化发展，建里总分一体的安全组织架构
面向实战化的安全运营工作开展，保障光大新型动态防御体系建设团队资源

未来思考

网络安全创新大会
Cyber Security Innovation Summit

1 大数据计算平台

- 夯实基础，持续优化大数据计算平台的数据处理能力和稳定性。
- 组件扩充，基于上层应用要求，按需引入计算组件、存储组件，
- 通过资源扩容和技术升级，核心在于算力和存储能力的提升，100PB数据的处理能力

2 安全数据中台

- 采集范围扩大，履行企业安全配置管理数据库定位，汇聚全网安全数据、统一数据结构、制定开放标准。
- 持续治理，沉淀数据价值，持续提升威胁分析的准确性。
- 着重进行AI计算能力补充，为平台注智提供支撑。
- 数据质量和数据治理标准，加入AI

3 安全场景

- 整合内外部数据分析团队资源，在做好外部威胁识别的同时，开展内部用户实体行为分析、威胁智能决策场景研发。
- 引入自动化编排能力引入，通过场景编排，精准高效的形成自动化响应处置能力，驱动的各设备协同工作，提升安全响应的速度和效率。

4 上层应用

- 实现安全应用解耦，构建安全能力中台，面向前台应用，实现安全能力规模化开放复用，实现安全服务按需申请、灵活配置、快速交付，最终实现上层应用的高效研发。

网络安全创新大会
Cyber Security Innovation Summit

THANKS