面向电信行业的数据安全监管运营实践

绿盟科技

电信行业数据安全新特点

敏感数据比例大类型多管理难

运营商积累的业务数据含用户属性、通话、位置、上网行为等多种用户数据，大部分属于个人信息保存范畴，敏感数据比例高

数据经理数据解析、情绪】转化流程，以XDR数据、结构化数据、文本数据等多种形式存储处理，加大敏感数据管理难度。

敏感数据分布广泛，权限管控难度大

电信运营书对客户数据手机通过多个业务系统进行。业务支撑系统收集恶人信息、消费信息、业务办理信息、核心网络在提供通信服务过程中，积累用户通信、上网行为等数据。敏感数据信息分布在不同部门、网络中

在大数据业务开展过程中，数据在部门间流动，难以对敏感数据流转进行有效监控和权限管理

数据流转链路多，5G时代更复杂

进入5G时代，随着数据营销、数据决策业务的兴起，数据在运营商内部流转路径不断增多

同时，5G时代为以往的网络架构带来了变化，引入了新的数据网元，5G亦为垂直行业提供服务。为运营商网络带来更多的外部访问，数据外部流转路径不断增多。

新基建领域数据安全建设场景

5G 网络切片数据安全场景

5G网络切片是虚拟化端到端专用网络，承载智慧城市、智慧工业等各类5G垂直行业业务。切片中包含5G网络挂你、控制数据以及业务数据

第三方可通过数据共享获得切片运行状态、性能指标等数据，存在对外接口访问控制措施不严，导致切片敏感数据存在未授权访问等风险；存在因为网元切片资源共享导致的敏感数据暴露面增加风险

5G MEC数据安全场景

MEC节点可部署在边缘数据中心，靠近用户现场，处于先对开放的环境中，更容易被入侵，导致数据泄露或破坏。

MEC涉及的数据保护多种行业、个人用户应用数据。MEC定义的网络和第三方应用双向API通信机制，可以把用户数据、网络数据等通过API直接诶开放给第三方APP，第三方APP也可以直接运行在MEC节点上，产生了新的数据暴露风险。

工业互联网数据安全场景

工业互联网是5G垂直领域，行业覆盖智能制造、车联网、智能工厂。其敏感数据行业属性强、数据传输实时性要求高、数据类型复杂的特点

同时，工业互联网数据传输链路繁多。数据流转涵盖由移动智能终端到工业互联网企业到公有云再到国家级工业互联网平台的复杂流转线路

数据安全国家政策要求

电信行业数据安全法规体系

国家法律

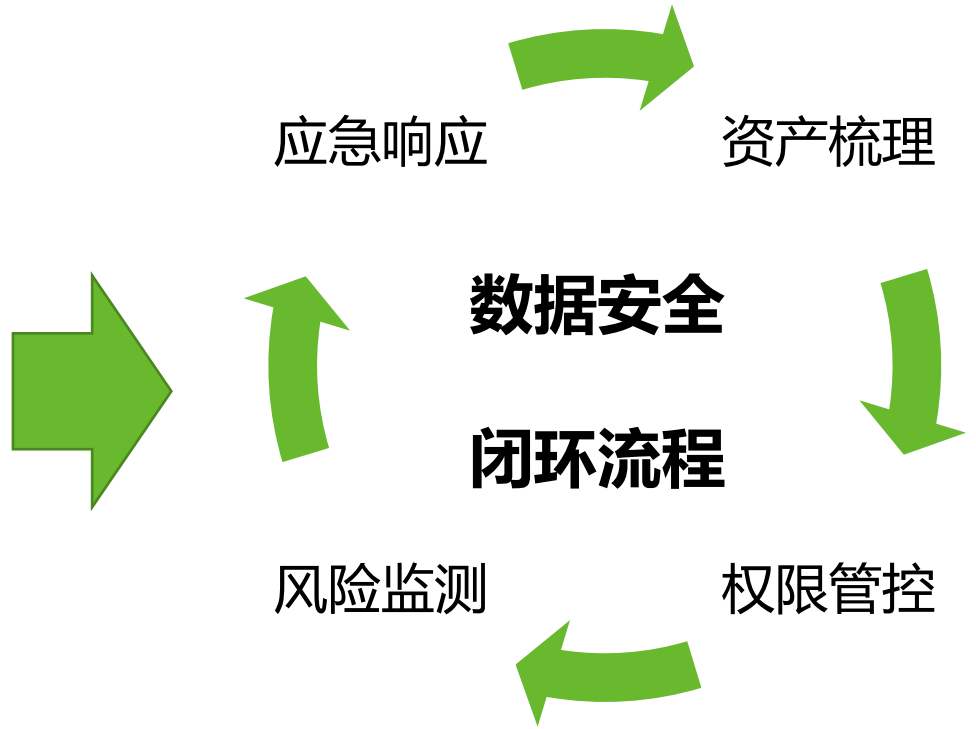
- 中华人民共和国网络安全法
- 中华人民共和国数据安全法（草案）
- 个人信息保护法（草案）

国家标准

- 信息安全 个人信息安全规范
- 信息安全 大数据服务安全能力
- 信息安全 数据安全能力成熟度模型
- 信息安全 大数据安全管理指南

行业标准

- 5G数据安全总体技术要求
- 电信网和互联网数据安全事件应急响应实施指南
- 电信大数据安全管控分类分级技术要求
- 电信运营商大数据安全风险及需求
- 基础电信运营企业移动网络客户信息安全管理框架



面向新形势新挑战的应对策略思考

放 安全开放

面向电信行业数据安全新趋势新挑战
建设行之有效的数据安全防护体系

在数据资产有效管理，数据安全充分保护的前提下有效支持数据开放与信息共享

管 有效监管

以数据资产流转作为数据安全监管的重中之重

基于流量、情报等多种监测手段结合安全大数据分析能力，有效监控数据资产异常流转

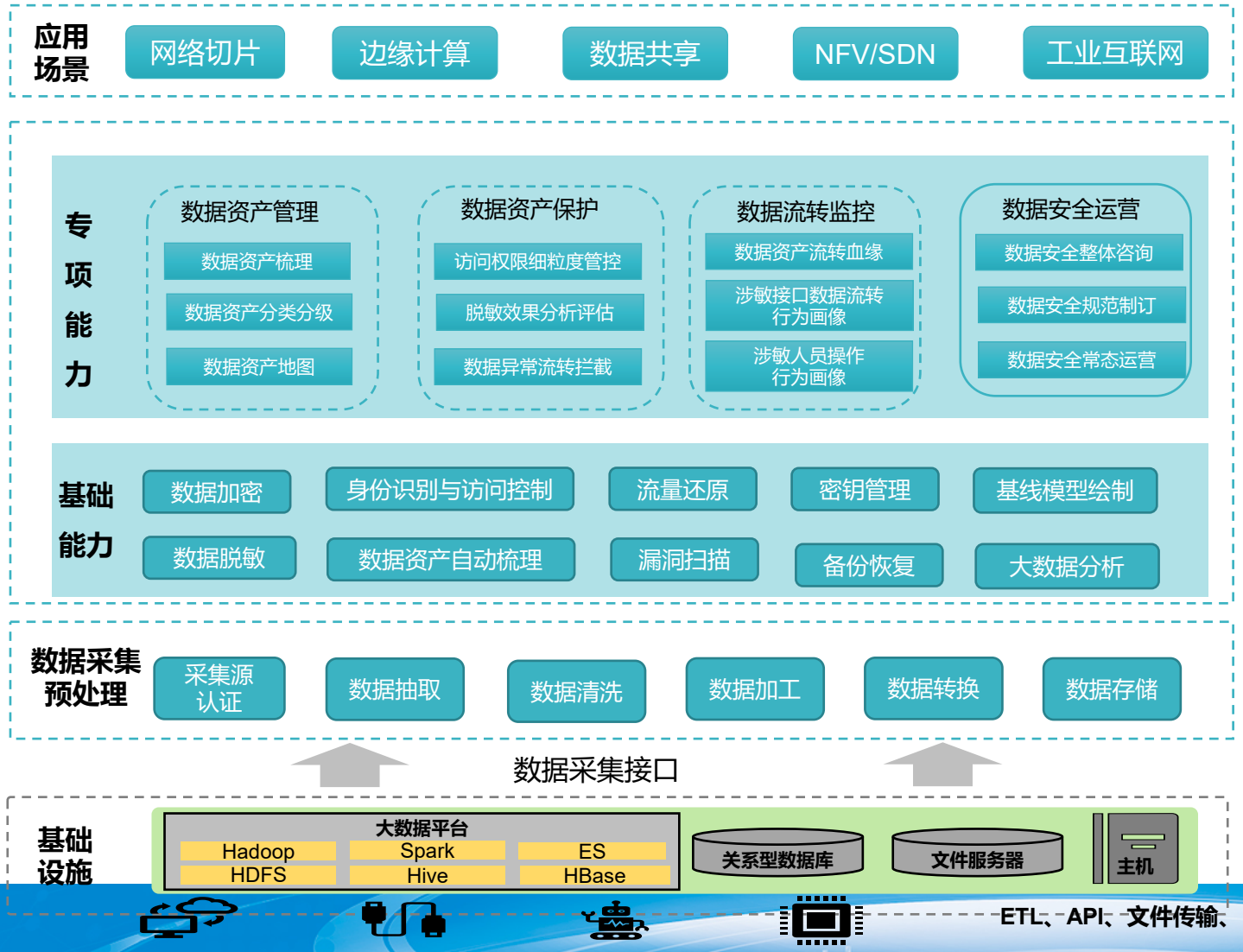
利用攻防演练等手段检验监控能力

服 服务业务

通过建设数据安全监管防护体系
有效服务业务数据开放与信息共享

通过多级数据安全体系间的资产特征、攻击特征、威胁情报共享，t提升数据安全治理能力

建设数据安全闭环监管运营体系



- 在电信运营商行业，应基于数据业务新特点、新挑战。构建数据安全IPDR监管运营体系。
  1. 对数据资产进行有效管理与分类分级，形成资产分布地图
  2. 基于国家行业相关规范与企业数据安全实际需求制定数据访问权限策略。利用多种技术、人力手段实现数据数据访问权限的细粒度管控
  3. 利用技术手段，构建涉敏数据流转血缘。并基于涉敏接口与人员绘制行为基线，利用大数据分析手段识别数据异常流转
  4. 利用多种运营手段，构建事前、事中、事后数据安全持续运营能力

基于自动化工具全面梳理数据资产

1、制定分类分级标准

数据类别分为4类及二级子类，
数据密级为分4级：**极敏感级**、**敏感级**、**较敏感级**、**低敏感级**。

类别	一级子类	二级子类
(A类) 用户身份相关数据	(A1) 用户身份和标识信息	(A1-1)自然人身份标识 (A1-2)网络身份标识 (A1-3)用户基本资料 (A1-4)实体身份证明 (A1-5)用户私密资料
	(A2) 用户网络身份鉴权信息	(A2-1)用户密码及关联信息
(B类) 用户服务内容数据	(B1) 服务内容和资料数据	(B1-1)服务内容数据 (B1-2)联系人信息
(C类) 用户服务衍生数据	(C1) 用户服务使用数据	(C1-1)业务订购关系 (C1-2)服务记录和日志 (C1-3)消费信息和账单 (C1-4)位置数据 (C1-5)违规记录数据
	(C2) 设备信息	(C2-1)终端设备标识 (C2-2)终端设备资料
(D类) 企业运营管理数据	(D1) 企业管理数据	(D1-1)企业内部核心管理数据 (D1-2)企业内部重要管理数据 (D1-3)企业内部一般管理数据 (D1-4)市场核心经营类数据 (D1-5)市场重要经营类数据 (D1-6)市场一般经营类数据 (D1-7)企业公开披露信息 (D1-8)企业上报信息
	(D2) 业务运营数据	(D2-1)重要业务运营服务数据 (D2-2)一般业务运营服务数据 (D2-3)公开业务运营服务数据 (D2-4)数字内容业务运营数据
	(D3) 网络及IT系统运维数据	(D3-1)网络设备及IT系统密码及关联信息 (D3-2)核心网络设备及IT系统资源类数据 (D3-3)重要网络设备及IT系统资源类数据 (D3-4)一般网络设备及IT系统资源类数据 (D3-5)公开网络设备及IT系统资源类数据 (D3-6)网络设备及IT系统支撑数据
	(D4) 合作伙伴数据	(D4-1)渠道基础数据 (D4-2)CP/SP基础数据

2、准备数据样本，建立敏感数据字典

用户身份信息
用户通讯信息
短信计费话单
短信统计话单
OA办公审批流信息
合同样本文件

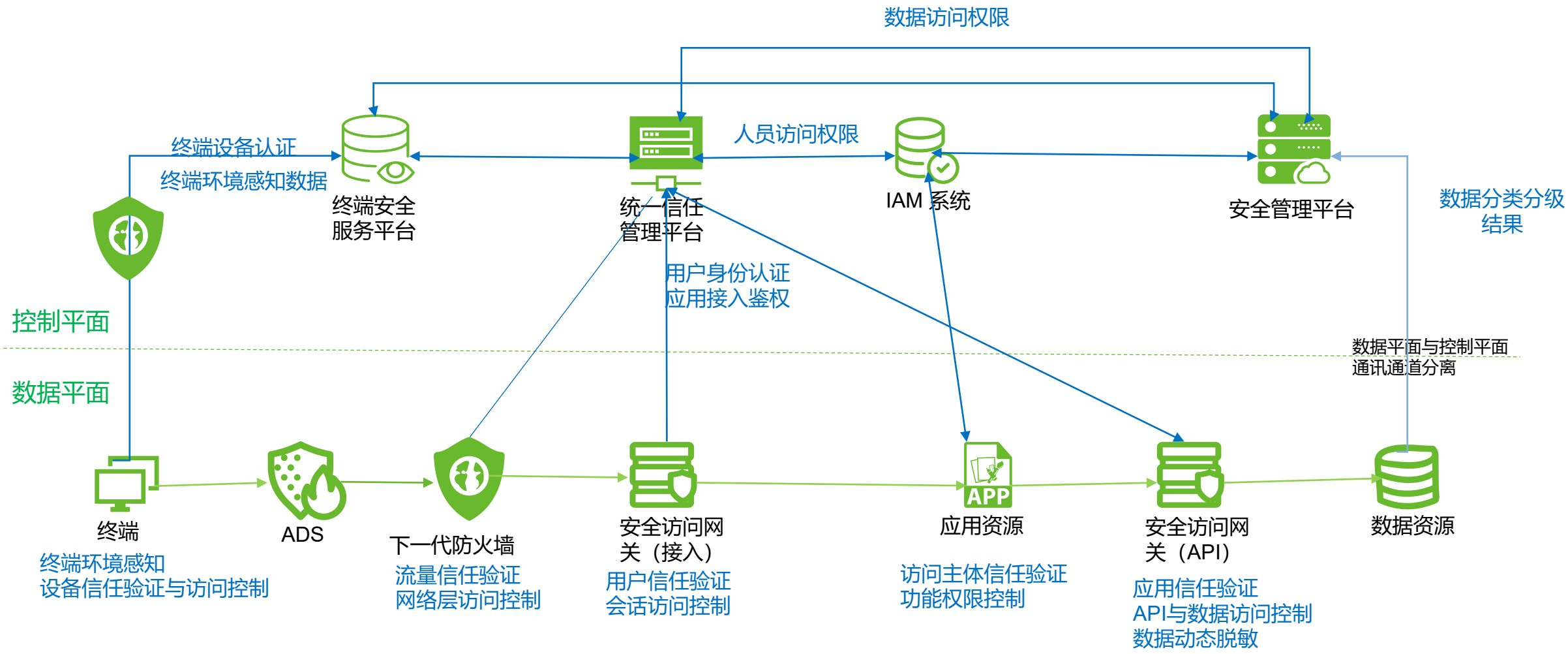
敏感数据类型	特征表示	分类	分级
用户身份信息（身份证、护照号等）	正则表达式	A1-1自然人身份标识	敏感级
用户通讯信息（电话号码、电子邮箱）	正则表达式	A1-2网络身份标识	敏感级
短信计费话单	复合规则	C1-2服务记录和日志	敏感级
短信统计话单	复合规则	C1-3消费信息和账单	较敏感级
OA办公审批流信息	复合规则	D1-3企业内部一般管理数据	较敏感级
合同样本文件	关键字规则	D1-2企业内部重要管理数据	敏感级

3、扫描数据库和文件存储系统，自动化数据测绘

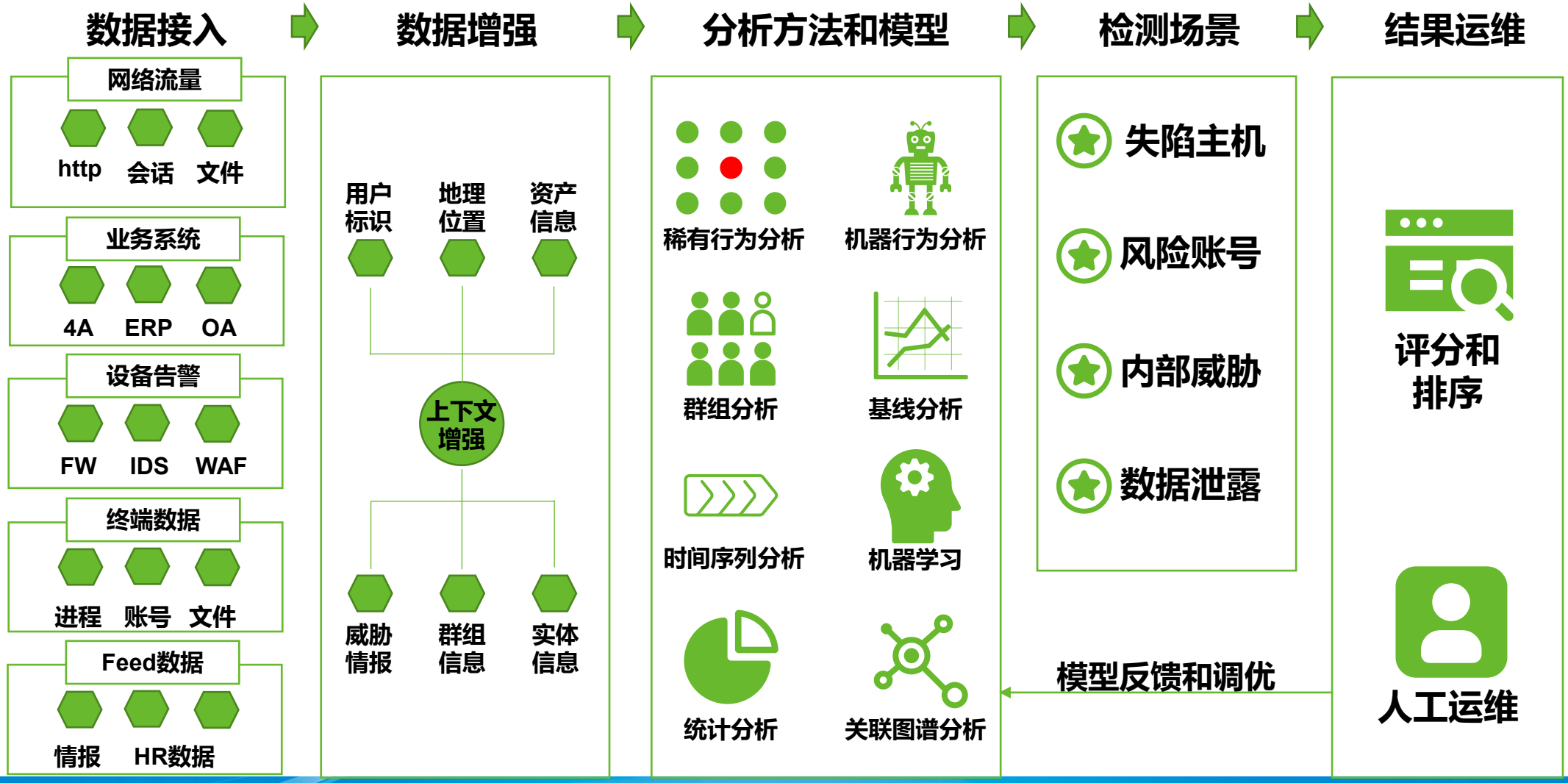
结构化/半结构化/非结构化数据扫描属性包括：

- 表名称/文件名称
- IP地址
- 数据库及实例位置/存储路径
- 敏感字段类型
- 记录行数
- 文本大小
- 数据表/文件业务类型标签
- 数据表/文件数据分类标签
- 数据表/文件数据分级标签
- 数据表/文件数据分布标签
- 数据表/文件属主账号
- 数据表/文件属组账号
- 数据表读写权限/文件读写执行权限（9元组）
- 扫描时间

基于数据与人员权限的数据访问保护体系

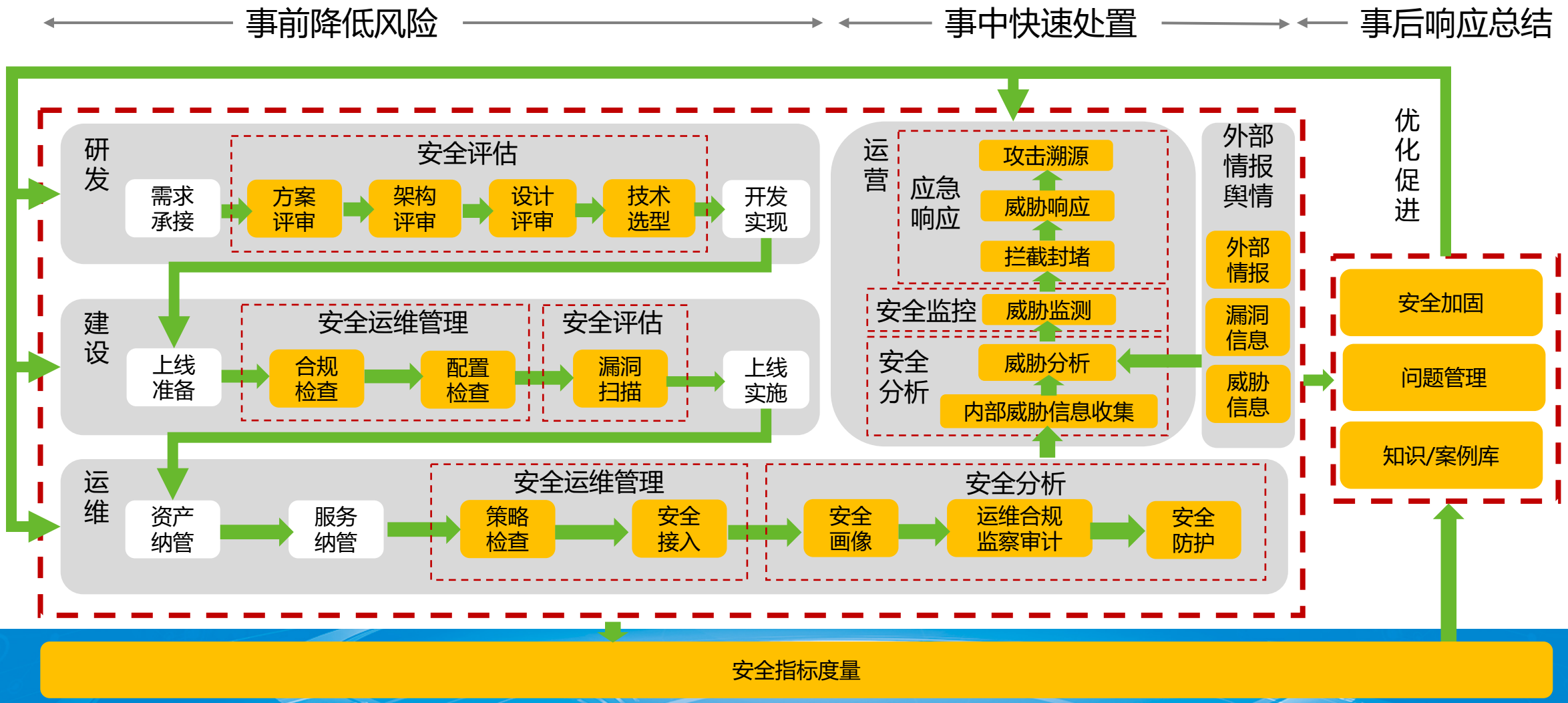


基于流量与大数据分析能力监控涉敏数据流转



持续数据安全运营与度量整体流程

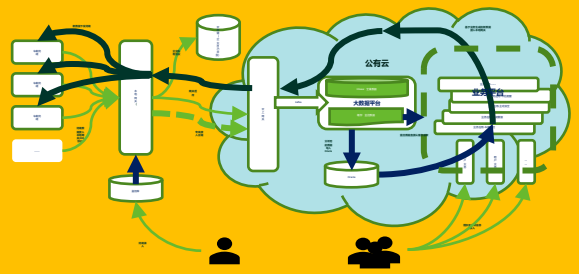
将数据安全运营流程串联在研发、建设、运维、运营的全生命周期中，实现事前、事中及事后的有机结合协同工作。



以攻促防，检验数据安全体系建设效果

演练目的

通过攻防演练，模拟真实数据窃取行为。检验组织数据安全体系在监测点、监测手段、分析能力、应急响应能力、回溯能力上的盲区与短板。查缺补漏，以攻促防



由于数据流转链路繁多，基于攻防手段可以有效发现薄弱环节和短板

基础信息

时间 / 被攻击对象 / 攻击特征（Cookie / UA / XFF / URL / Exploit / C&C / 地址池 / 密码 / 工具等）。

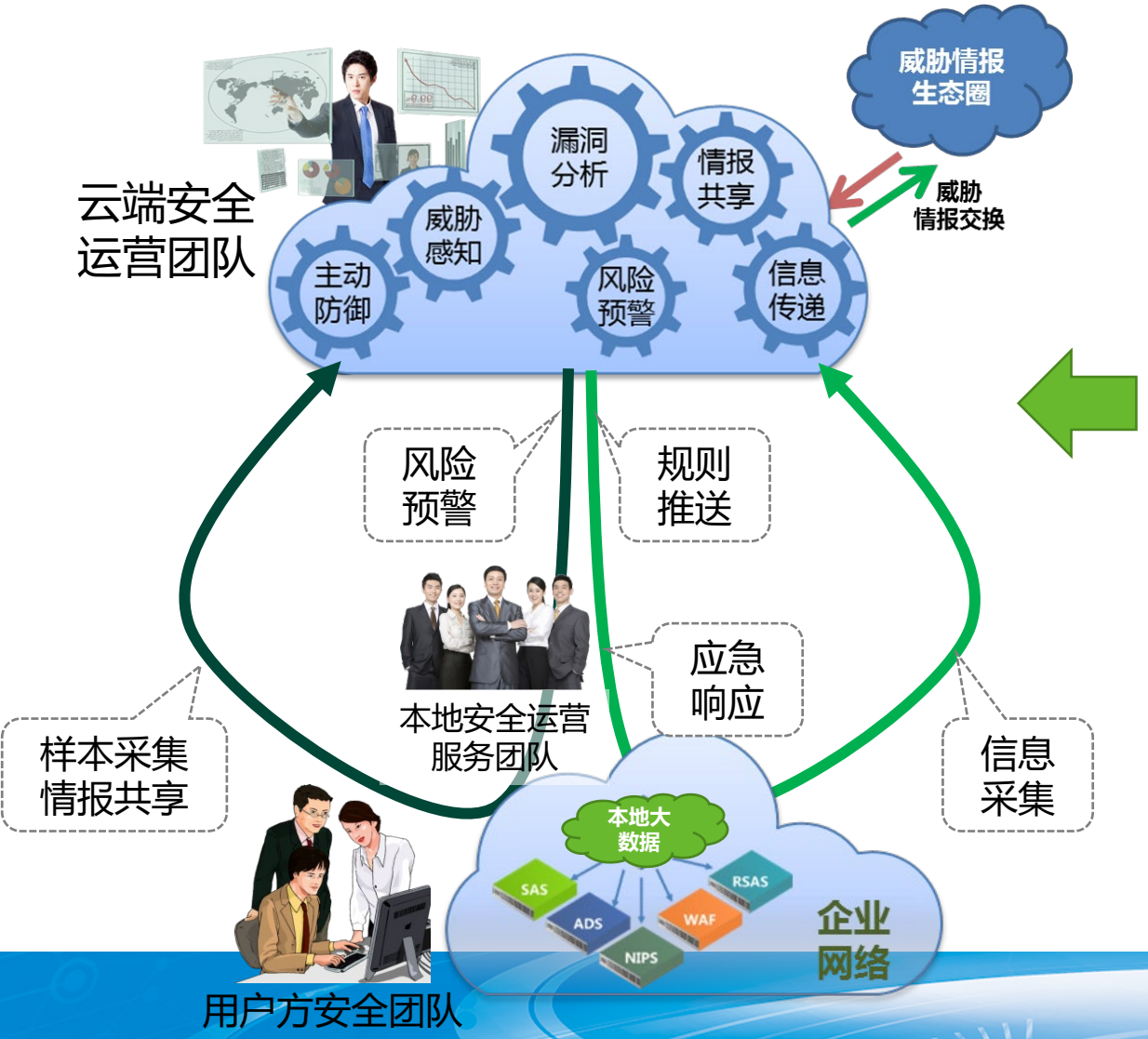
TTPS

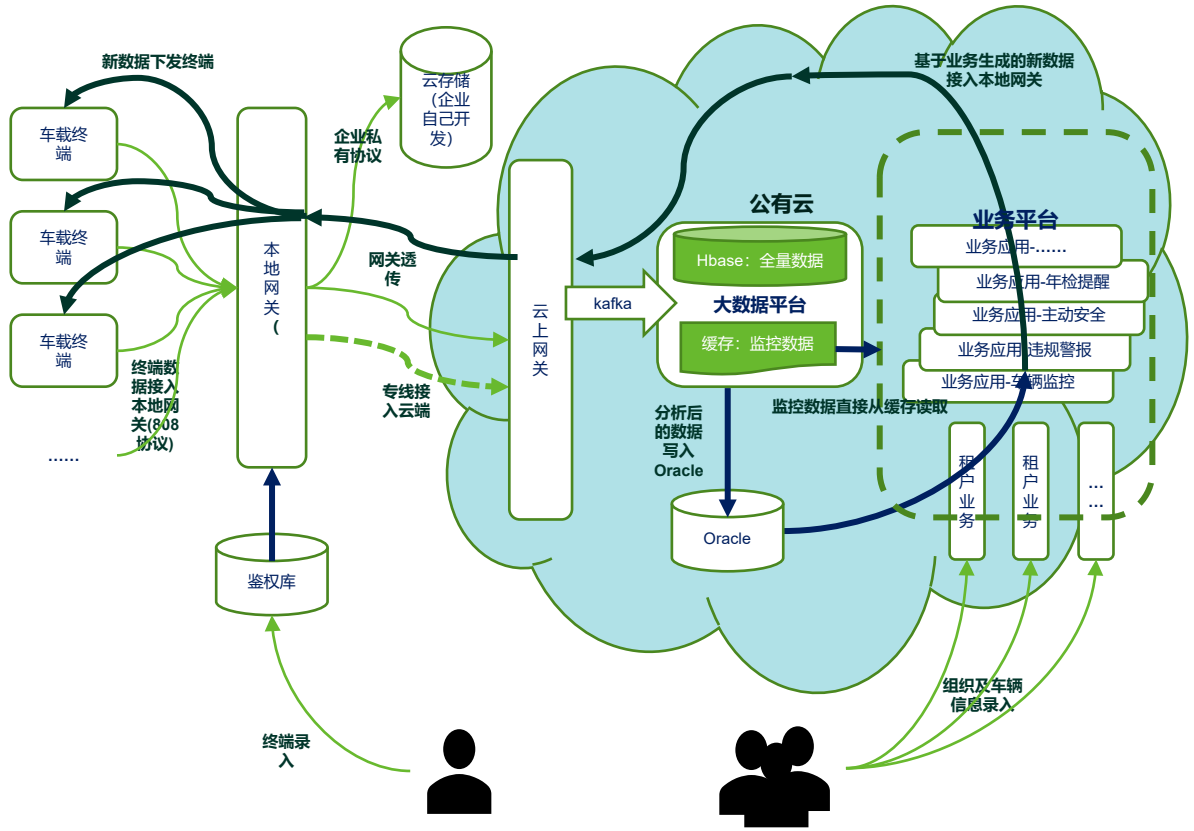
信息收集 / 漏洞利用 / 持久控制 / 虚拟逃逸 / A.B.U等特征。（Mirte ATT&CK）

情报信息

IP / 域名 / 手机号 / 邮箱 / 社交账号 / SRC / 社工库 / 照片 / 公司信息 / 样本IOC信息 / 图床等。

利用“云地人机”运营体系提高数据安全治理能力





工业互联网数据安全场景

THANKS

谢谢！