大数据环境下的数据安全过渡

国网思极检测技术（北京）有限公司

演讲人：赵明明

安全形势

2017年，数据泄露、网络攻击、漏洞发现、会议活动、投资并购等各个层面呈爆发态势，无论在数量还是影响面上，均超过以往任何年度。

政策法规篇

从欧盟的《通用数据保护条例》(GDPR)到美国的《国家网络事件响应计划》(NCIRP)，再到俄罗斯的虚拟专用网(VPN)禁令和中国的《网络安全法》，个人隐私保护与商业利益和国家安全交织，网络空间安全成各国政府政治、经济博弈关注重点。

√欧盟的《通用数据保护条例》(GDPR)将于2018年5月25日正式实施，受到影响最大的是与欧洲有着密切商业往来的跨国公司。一是合规投入。根据普华永道的调查，大部分美国公司认为将花费100万到1000万美元的投入以满足合规。二是罚金。违反GDPR规定的公司，可被罚款高达2000万欧元或是公司全球年收入的4%处罚。有咨询公司表示，在GDPR实施的头一年中，有可能开出60亿美元的罚金。

√《中华人民共和国网络安全法》已于今年6月1日实施，网络安全法最重要的意义在于，从法律层面上把我国网络安全工作提高到了国家安全战略的高度，强调对关键信息基础设施及个人信息数据的保护，明确了国家、主管部门、网络所有者、运营者及普通用户各自的责任以及违规后的相关处罚。在合规应对实施环节，从网络运营安全、网络信息安全及关键信息基础设施保护等三方面，就“相关责任方”、“管理措施”及“技术措施”等三个维度总结了具体实施要点。

√数字化进程扩大网络安全产业，各国安全政策压缩彼此市场空间。数字化进程不断的促进网络安全市场空间的扩张，努力向前发展的企业不可避免的倾向使用先进的技术。而网络安全又是国家安全的重要组成部分，因此各国出台相应保护自我的政策无可厚非。但更大的主题是人类的科技发展，各国之间是一个竞争与合作的“命运共同体”。自主可控与开放创新，封闭与开源，永远都是在争议中前行的话题。因此如何在符合对方国家大政策体系和规范的前提下，尽最大能力地将自身的技术和产品融合到当地的安全生态圈中，是跨国安全企业在未来几年的重要挑战。

安全形势

网络安全事件篇

1. 信息泄露创历史记录

2017年仅上半年泄露或被盗的数据（19亿条），就已经超过了2016年全年被盗数据总量，全年预计将超过50亿条。其中，仅雅虎一家就达到了30亿条。

2017年的信息泄露事件呈现以下特点：

√ 随着云计算、大数据和物联网的普及，信息泄露事件呈现高速增长趋势。信息泄露涉及行业广泛，但重点集中在互联网、政府机构及金融行业。

√ 数据泄露导致企业严重损失，高管担责。今年瑞典的内政部长和基建部长，因数据泄露事件而引咎辞职。我国的《网络安全法》今年已经正式实施，确定了“防止网络数据泄露或者被窃取、篡改”是网络运营者的法定义务。

√ 内部威胁成信息泄露重要途径。包括内部员工的恶意或无意泄露，以及第三方供应商带来的风险。尤其是后者，近年来重大的信息泄露事件都与第三方供应商相关。如塔吉特的空调供应商，斯诺登是NSA承包商，动态供应链是必然趋势，但每家供应商都潜在着扩大了机构或企业的网络攻击面。由供应商引起的第三方风险，已经成为当今网络安全领域的一个普遍性问题。

2. 网络攻击无所不在

随着物联网设备的激增，网络攻击目标泛化，并成指数级增加。2017年初Fortinet的一份调查显示，针对物联网的攻击达到250多亿次。尤其是5月份爆发的WannaCry勒索软件，成为近几年来为数不多的全球性安全事件之一。

√ 网络攻击载体和目标多样化。海陆空交通系统，工业生产系统，以及各种物联网设备和加密货币，均为网络攻击的载体和目标，不管是出于政治原因还是经济目的，未来越来越多的创造性手段将会被攻击者采取和使用，而只要有网络延伸到的地方，就可能成为被攻击的目标。

√ “犯罪即服务”的商业模式是勒索软件、恶意软件传播以及DDoS等大规模恶意行为泛滥的关键原因。“犯罪即服务”极大的降低了攻击成本和攻击难度，即使是初级罪犯也可随时发动网络攻击，再借助“零日漏洞”，极易给全球互联网带来重大破坏。。

√ 网络武器已被全世界采用。网络攻击背后的国家力量日趋明显，无论是对关键设施的长期渗透，各个国家竞选系统的入侵，还是对社交舆论的风向控制，以及对“零日漏洞”的交易、利用，甚至是对加密货币的攫取，背后都闪现着国家支持的黑客的影子。网络攻击，已经横跨政治、外交、商业、军事、关键基础设施和社交媒体等数字化时代必定导致数字化国防，网络成战场，代码即武器。

3. 邮件安全问题突出

电子邮件成网络安全重灾区，不管是鱼叉式邮件还是商业欺诈，都有着惊人的破坏力。前者是发动APT攻击和大范围传播恶意软件的典型入口，后者据FBI的统计，2013至2016年商业欺诈邮件(BEC)已造成53亿美元的损失。

√ 电子邮件内容事关重大。由于电子邮件办公已经在各行各业充分普及，从个人敏感信息到重要商业机密，再到核心知识产权，电子邮件都是最为主要的传输通道，一旦泄露后患无穷。

√ 电子邮件的安全地位不容忽视。不管是大规模的恶意软件传播，还是针对性的APT攻击，无论是广撒网式的个人骗局，还是精心设计的商业欺诈，邮件都是第一入口和最大入口。

√ 警惕网络钓鱼和商业欺诈邮件的激增。据美国联邦调查局今年5月的统计，BEC（有时也称钓鲸邮件）在两年时间里，达到了2370%的惊人增长率，而钓鱼邮件的增长率已经超过了恶意软件。虽然邮件安全网关和机器学习等技术手段可以在一定程度上进行防范，但建立起良好的网络安全意识教育机制，才是应对社会工程手段攻击最为有效的方法。


淘宝.zip\taobao.com\买家邮箱（2200
FDQ-1001.TX
weibo.com.dbf
收件箱
星标邮件
已发送
草稿
已删除
垃圾邮件
已删除邮件
广告邮件
病毒文件夹
订阅邮件
导入邮件
Eml导入邮件
benenet31@163.com
时尚家饰-工艺品-十字绣（41万）

2018/5/23

漏洞篇

1. 漏洞数量增长史无前例
2. 漏洞可能出现在各个层面
3. 漏洞披露问题的两难
4. 漏洞披露时间缩短
5. 漏洞发布渠道变多
6. 漏洞利用工具批量化
7. 补丁制作周期加长
8. 漏洞交易开始公开化

√ **安全产品不一定安全。**无论是杀毒软件还是防火墙，抑或是安全机制，用于安全防御的事物本身也能成为漏洞的藏身之处。
√ **底层漏洞防不胜防。**芯片或固件一旦出现漏洞，卸载软件、打补丁、重装操作系统均无法彻底解决问题，而更新固件或是更换芯片意味着巨大的困难。
√ **通信协议或标准漏洞影响面巨大。**动辄影响上亿的设备，而协议的更新换代则需要度过漫长的时间周期。
√ **数字化应用的爆发带来漏洞的爆发。**无论是移动设备还是物联网设备，无论是虚拟化还是云计算与开源社区，在今年都呈飞速上升与扩展的趋势，因此漏洞的爆发应在意料之中。
√ **长老级漏洞与难打的补丁现象固疾难除。**出于各种原因，许多补丁事隔很长时间才能得到修复，甚至是永远不会修复。而只有修复之后，才谈得上更新。最后，对老旧系统的更新可能才是真正的挑战。
√ **零日漏洞与开源。**不谈国家强制力量，零日漏洞的一大根源是开源代码的不断扩散。每年1110亿行代码的扩张量，越来越多的开发者加入开源模块、组件、库的复用队伍。开源安全责任重大，与社区中的每一个人都有关。

安全形势

黑客在大众眼中很神秘，其实从技术角度来看，黑客的技术也是通类划分。自从2010年信息泄漏开始进入大众视角来看，国内黑客技能基本上局限在web漏洞发现能力上，老一代黑客逐步隐藏的更深。

重点在潜伏

- 研究操作系统底层漏洞
- 研究通信协议漏洞
- 精通底层语言
- 不关注数据-可以输送大批精品数据
- 具备高层次木马开发
- 擅长隐藏行踪
- 熟练掌握APT

→ **传统黑客**

新一代黑客 ←

重点在数据

- 关注web应用漏洞
- 关注数据库安全
- 会使用脚本语言
- 熟练使用工具
- 多数不会实际渗透
- 基本上不会写木马
- 不掌握APT攻击

1 大数据的矛盾

2 业务过渡周期

3 旧技术新环境

一、大数据的矛盾

大数据产生的来源

1、交易数据：电子商务和企业应用的数据：ERP、B2B、B2C、C2C产生的数据。
2、交互数据：是指来自相互作用的社交网络的数据；包括人与人交互产生的数据、人与机器设备交互产生的数据。

大数据产生的主体

1、少量企业产生的数据。
2、量人产生的数据。
3、巨量机器产生的数据。

大数据产生的特点

1、数据产生由企业内部向企业外部扩展。
2、数据产生从互联网向移动互联网扩展。
3、数据产生从互联网向物联网扩展。

一、大数据的矛盾

参考NIST SP 1500-4规范中对大数据架构框架的描述，可将大数据平台分为基础设施、网络系统、平台构建（大数据存储应用组件）、数据处理应用（大数据计算应用组件）、数据采集模块（大数据采集应用组件）

一、大数据的矛盾

2014年2月27日
中央网络安全和信息化领导小组宣告成立

2015年8月31日
国务院发布《促进大数据发展行动纲要》

2016年3月17日
十三五规划纲要正式发布，第六篇 拓展网络经济空间，第二十七章 实施国家大数据战略

2016年4月19日
习近平总书记在网络安全和信息化工作座谈会中指出，应加快构建关键信息基础设施安全保障体系。

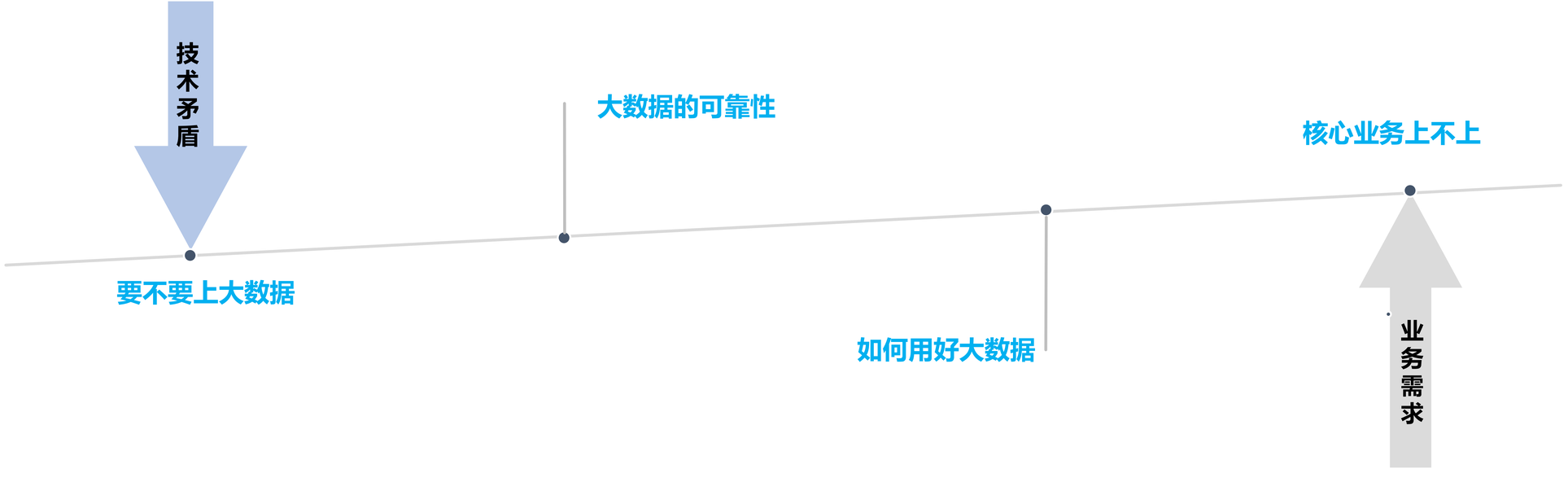
2016年8月25日
交通运输部办公厅发布《关于推进交通运输行业数据资源开放共享的实施意见》

2017年4月8日
发布《大数据安全标准化白皮书及路线图》，并开展大数据安全标准的研制

2017年6月1日
全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行《中华人民共和国网络安全法》

2017年12月8日
中共中央政治局就实施国家大数据战略进行第二次集体学习

一、大数据的矛盾



一、大数据的矛盾

数据防护的目标
电力数据定义与需求

目标定义：电力主业生产数、电力辅业处理数据、电力辅业决策分析数据、电力营销数据、电力信息化数据、电力传输过程数据、平台化数据、关键分析数据、安全数据等等

关键内容：

1、跨专业数据应用方式
2、业务数据梳理模式
3、梳理治理行业落地标准
4、数据传输全过程跟踪
5、数据应用全过程管控
6、数据全生命周期管理

管理制度

数据管理体系

数据存储 | 数据收集 | 数据传输 | 数据应用 | 数据处理

安全管理体系 | 安全技防体系

电力调度专业	电力运检专业	电力营销专业	电力信息专业
电量数据	检修数据	用户数据	办公数据
调度数据	杆塔数据	计量数据	人员数据
电能数据	终端数据	售电数据	运行数据
地理数据	地理数据	营业数据	其他数据
。。。	。。。	。。。	。。。

防护方式

专网隔离 | 数据专用 | 数据脱敏 | 治理管控

运行队伍

1 大数据的矛盾

2 业务过渡周期

3 旧技术新环境

二、业务过渡周期

系统规模

- 几百个业务系统
- 几万张数据库表
- 几十万个字段

存储复杂

- 关系型数据库
- 文本文件
- 内存对象
- K-V结构NoSQL
- 列模式数据仓库
- 基于Hadoop的分布式文件系统

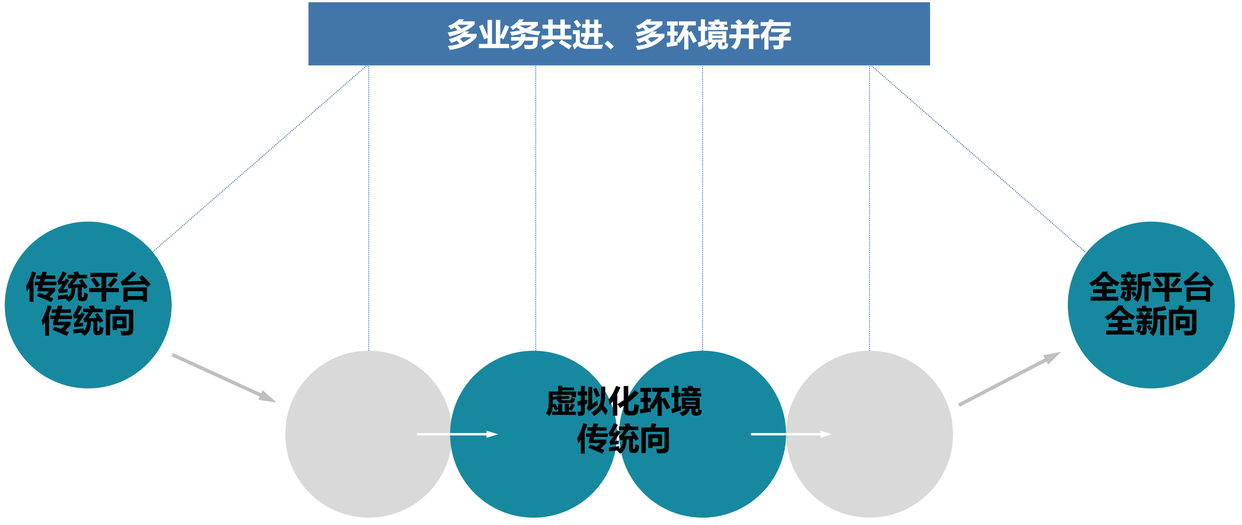
采集复杂

- 基于SQL
- 存储过程
- Perl/Python脚本
- Java语言
- MapReduce并行采集

电网大数据应用特点——“大”

二、业务过渡周期

在一定应用与建设周期内，解决多环境并存的数据权属与管控机制，是电力大数据安全的巨大挑战



二、业务过渡周期

Volume（大量） Variety（多样） Velocity（快速）
Veracity（真实性） Visualization（可视化）Value（商业价值大）

MySQL

集中式

Microsoft SQL Server

结构化

ORACLE

关系型

迁移进化

分布式

非结构化

非关系型

1 大数据的矛盾

2 业务过渡周期

3 旧技术新环境

三、旧技术新环境

身份认证	• 没有密码验证的账户体系 • 没有分权的账户管理功能
访问控制	• 继承了LINUX的权限体系 • 授权方式为自主授权
配置补丁管理	• 配置文件，加密密钥，证书等众多管理工作 • 如何保持开源库是最新
审计日志	• 没有主客体访问行为的详细日志 • 单一的日志记录，无法分析出安全事件
监控	• 继承了LINUX的权限体系 • 授权方式为自主授权
脱敏	• 配置文件，加密密钥，证书等众多管理工作 • 如何保持开源库是最新

三、旧技术新环境

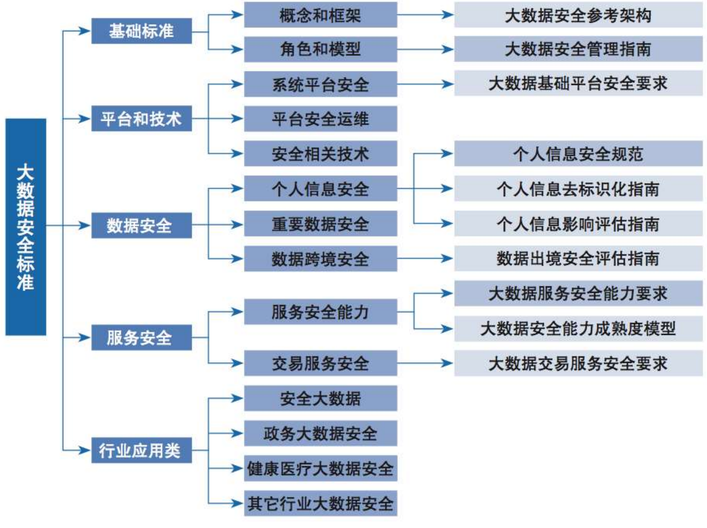
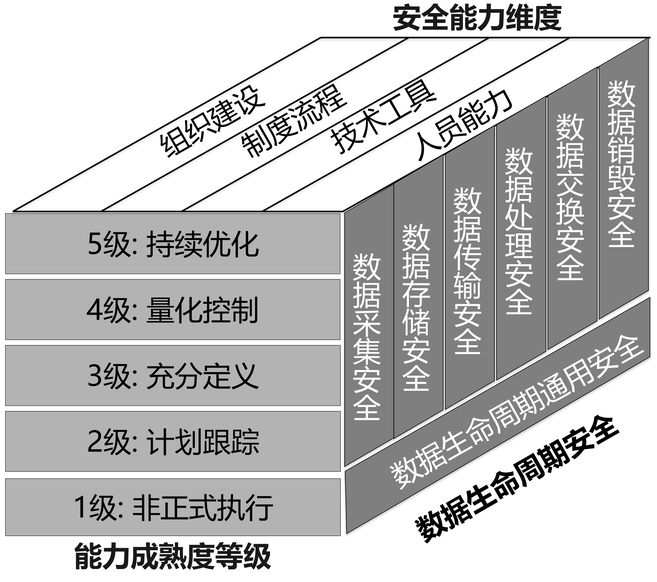
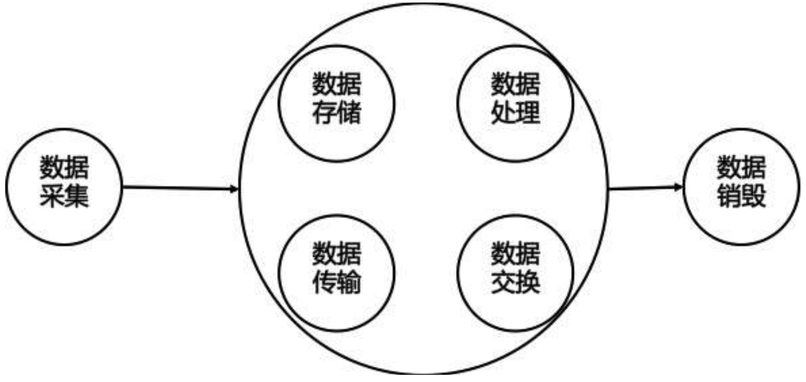
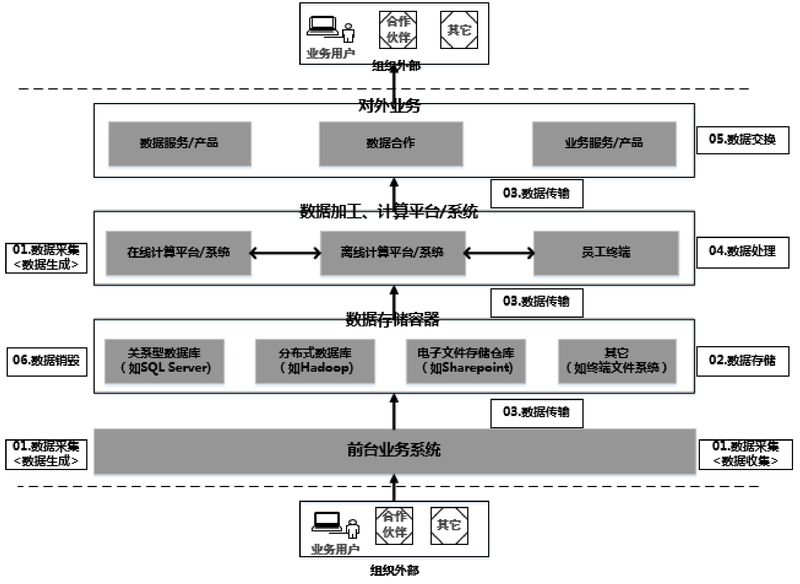


图3-2 大数据安全标准规划



三、旧技术新环境


数据采集
数据存储
数据处理
数据传输
数据交换
数据销毁


业务用户
合作伙伴
其它
组织外部
对外业务
数据服务/产品
数据合作
业务服务/产品
05.数据交换
03.数据传输
数据加工、计算平台/系统
01.数据采集<数据生成>
在线计算平台/系统
离线计算平台/系统
员工终端
04.数据处理
03.数据传输
数据存储容器
06.数据销毁
关系型数据库（如SQL Server）
分布式数据库（如Hadoop）
电子文件存储仓库（如Sharepoint）
其它（如终端文件系统）
02.数据存储
03.数据传输
01.数据采集<数据生成>
前台业务系统
01.数据采集<数据收集>
业务用户
合作伙伴
其它
组织外部

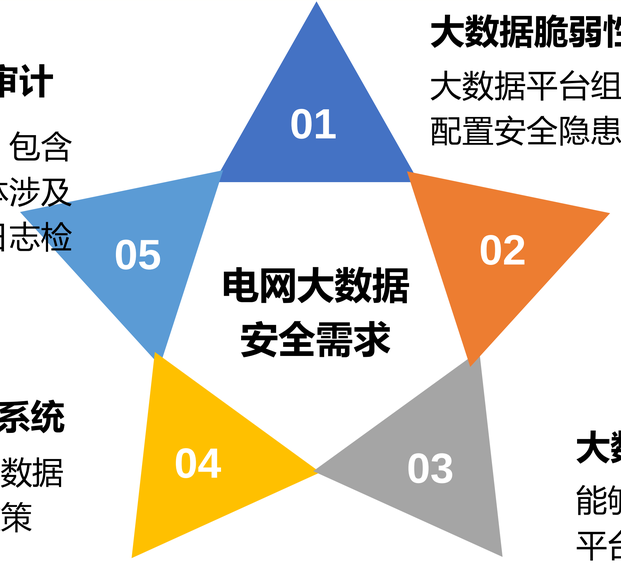
三、旧技术新环境

大数据安全审计

大数据平台组件行为审计，将主客体的操作行为形成详细日志，包含用户名、IP、操作、资源、访问类型、时间、授权结果等，具体涉及新建事件概览、风险事件、报表管理、系统维护、规则管理、日志检索等功能。

大数据脱敏系统

针对大数据平台存储数据全表或者字段进行敏感信息脱敏，启动数据脱敏不需要更改大数据组件的任何内容，只需要配置相应的脱敏策略。



大数据脆弱性检测

大数据平台组件周期性漏洞扫描和基线检测，扫描大数据平台漏洞以及基线配置安全隐患；包含风险展示、脆弱性检测、报表管理和知识库等功能模块。

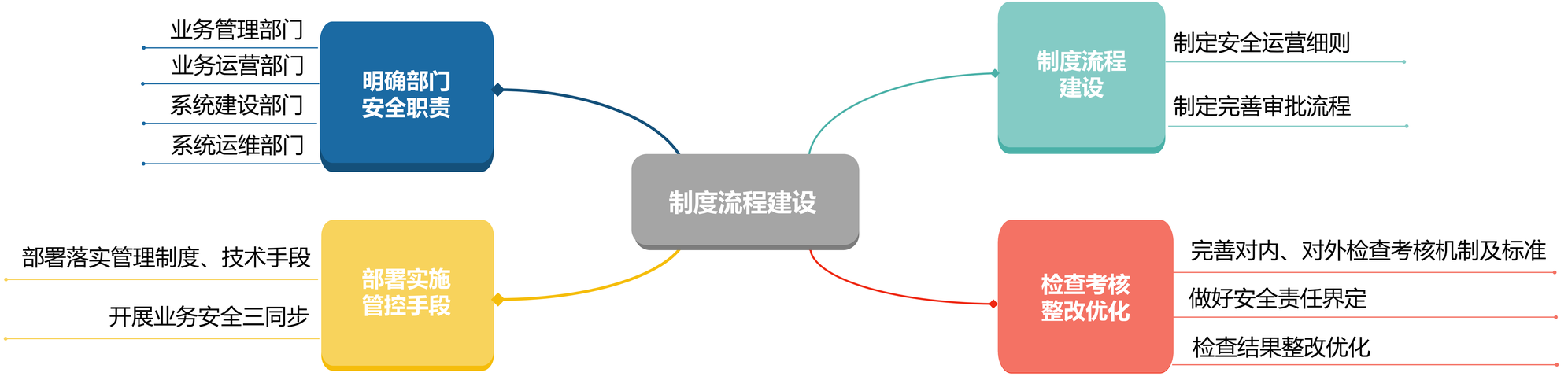
大数据敏感数据发现

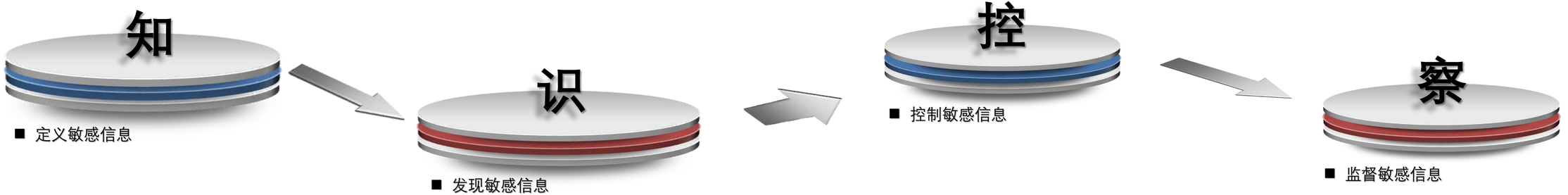
能够自动识别敏感数据，并对敏感数据进行分类，且启用敏感数据发现策略不会更改大数据组件的任何内容。

大数据应用访问控制

能够对大数据平台账户进行统一的管控和集中授权管理。为大数据平台用户和应用程序提供细粒度级的授权及访问控制。

三、旧技术新环境


制度流程建设
明确部门
安全职责
业务管理部门
业务运营部门
系统建设部门
系统运维部门
制度流程
建设
制定安全运营细则
制定完善审批流程
部署实施
管控手段
部署落实管理制度、技术手段
开展业务安全三同步
检查考核
整改优化
完善对内、对外检查考核机制及标准
做好安全责任界定
检查结果整改优化



什么是敏感数据

- 敏感数据定义
- 敏感数据安全等级
- 敏感数据属性类别

敏感数据在哪

- 敏感数据定位
- 敏感数据所属

需要控什么

- 外部攻击窃取
- 内部数据访问
- 对外数据共享

敏感数据如何被使用

- 敏感数据被谁使用
- 是否存在违规使用
- 敏感数据访问趋势

三、旧技术新环境

合作方管理框架

- 事前防范：组织责任管理、制度流程建设、数据资产管理、合作方调研审查；
- 事中管控：人员及账号权限管理、平台安全管理、数据共享管理、系统建设代维管理、数据代分析挖掘管理、业务合作方数据安全管理；
- 事后稽核：审计管理、安全合规检查、安全预警管理和合作伙伴考核。

合作方管理要求

- 应用合作方人员的账号、权限管理；
- 应用合作方人员操作记录详细日志；
- 应用合作方人员访问敏感数据等关键操作进行二次授权；
- 定期对合作方实施信息安全培训及教育；
- 合作方均需签署信息安全责任承诺书和保密协议；
- 加强合作方人员安全管理，应在其上岗前签订个人保密协议。

关于国网思极检测公司

公司介绍

- 国网思极检测是由国网信产集团中电普华公司单独出资成立的一家专门从事软硬件检测、信息安全技术服务、信息安全技术研究等的高科技公司，初创团队由原中电普华公司信息安全事业部积累了10年的信息安全专业团队、业界资深技术专家组建成立而成，致力于为客户提供信息安全服务及整体解决方案。

发展愿景

- 成为国内一流的软硬件检测实验室及能
- 拥有一支专属行业的信息安全服务“特

家小

公司资质

- 目前公司拥有“CNAS信息安全检测实验
- 信息安全风险评估证书（一级）、信息

联系我们

Contact Us

国网思极检测公司

地址：未来科技城国家电网园区

EMAIL: zhaomingming@sgitg.sgcc.com.cn

THANKS