聚·变

第二届顺丰信息安全峰会分论坛

网络空间安全

平台化信息安全管理

HNA TECH GROUP

07.19.2018

CONTENT
目录

信息安全管理办公室团队和分工

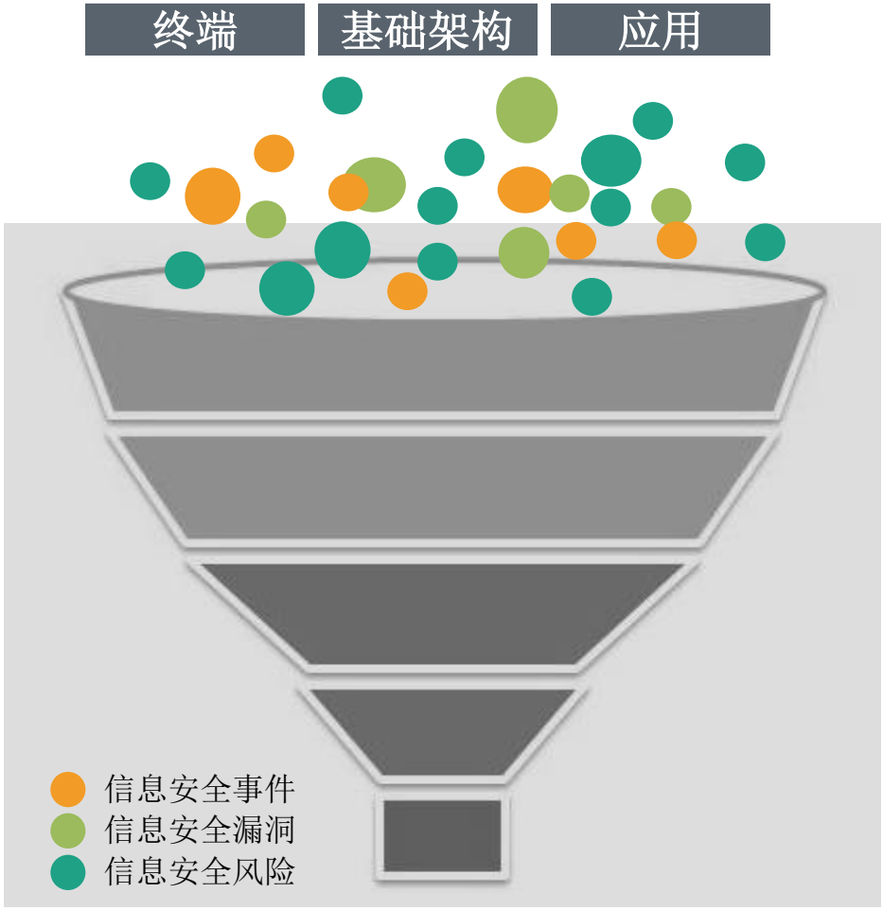
HNA 海航科技

信息安全管理体系	信息安全技术体系	信息安全应急响应	信息安全产品中心	信息安全研究中心
信息安全管理机制，制度，组织，流程的建立和管理。 信息安全风险和安全合规管理。	信息安全技术规划，咨询，评审，项目推进和标准落地 信息安全运维管理	对集团重要应用系统提供高级别安全漏洞挖掘和告警服务	自主知识产权的信息安全产品开发	前沿安全技术研究
• 建立安全管理规范和制度； • 推动各板块构建信息安全管理体系； • 信息安全风险评估； • 信息安全合规管理控； • 信息安全组织和流程建立； • 信息安全日常管理和沟通； • 信息安全培训；	• 信息安全技术规划； • 信息安全项目推进； • 信息安全技术架构评审； • 信息安全技术标准落地； • 信息安全运维管理	• 系统漏洞挖掘和通告； • 攻防技术研究； • 漏洞安全检查标准； • 攻防技术培训；	• IAM； • 安全工具开发；	• 开发安全研究； • 安全AI研究；

企业信息安全管理之 三横三纵

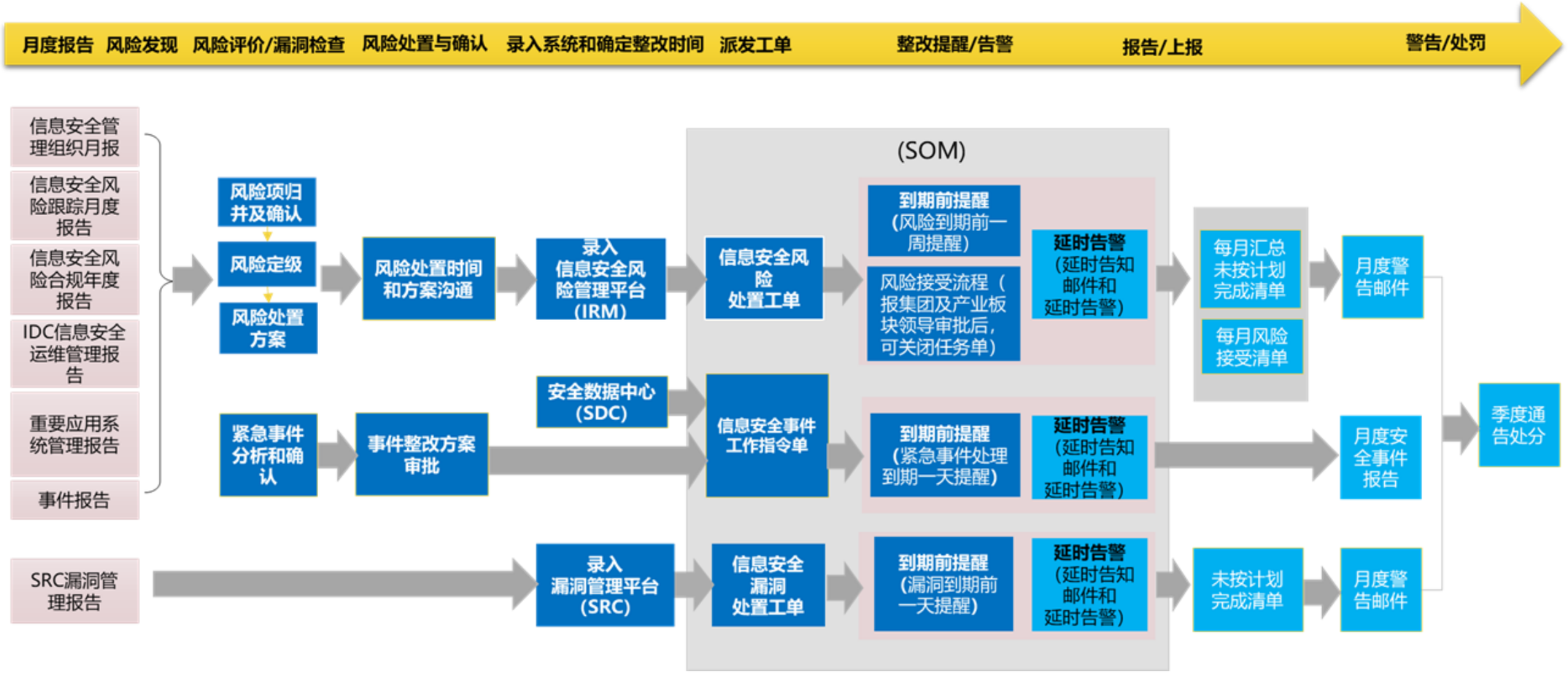
	壹 应用系统 信息安全	贰 基础架构 信息安全	叁 办公终端 信息安全
一 信息安全事件	发现快	响应快	处理快
二 信息安全漏洞	全系统	全周期	全流程
三 信息安全风险	早识别	早预案	早上报

企业信息安全管控工作思路



- 管理机制和制度
- 风险评估合规审计
- 立项安全技术审核
- 主动式安全渗透
- IT安全运维指标
- 安全防御体系项目
- 安全改进和处罚

日常安全运维流程


月度报告
风险发现
风险评价/漏洞检查
风险处置与确认
录入系统和确定整改时间
派发工单
整改提醒/告警
报告/上报
警告/处罚
信息安全管理组织月报
信息安全风险跟踪月度报告
信息安全风险合规年度报告
IDC信息安全运维管理报告
重要应用系统管理报告
事件报告
SRC漏洞管理报告
风险项归并及确认
风险定级
风险处置方案
风险处置时间和方案沟通
紧急事件分析和确认
事件整改方案审批
录入信息安全风险管理平台(IRM)
安全数据中心(SDC)
录入漏洞管理平台(SRC)
(SOM)
信息安全风险处置工单
信息安全事件工作指令单
信息安全漏洞处置工单
到期前提醒(风险到期前一周提醒)
风险接受流程（报集团及产业板块领导审批后，可关闭任务单）
到期前提醒(紧急事件处理到期一天提醒)
到期前提醒(漏洞到期前一天提醒)
延时告警(延时告知邮件和延时告警)
延时告警(延时告知邮件和延时告警)
延时告警(延时告知邮件和延时告警)
每月汇总未按计划完成清单
每月风险接受清单
未按计划完成清单
月度警告邮件
月度安全事件报告
月度警告邮件
季度通告处分

5大中心平台

SAC
态势感知中心

洞察安全状态

SEC
安全评测中心

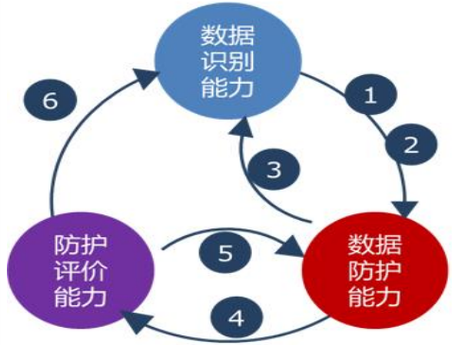
产品安全准入

SRC
应急响应中心

红蓝对抗

SSC
安全服务中心

自助式安全服务



DSC
数据安全中心

数据安检服务

CONTENT

目录

个人隐私数据保护合规要求

HNA 海航科技

欧盟通用数据保护条例（GDPR）

- 强调个人信息处理合法公平透明、目的限制、最小数据、准确性、存储限制和保密性完整性保护六大原则
- 保障数据主体知情权、数据、纠正权、被遗忘权、限制处理权、数据移植权、拒绝权和自主决策权八大权利
- 要求数据控制者能够具备证据证明自己符合合规要求

- **普通违规行为处罚1千万欧元或者2%的上一财年全球收入（以较高者为准）**
- **重大违规行为处罚2千万欧元或者4%的上一财年全球收入（以较高者为准）**

网络安全法

- 收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
- 不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
- 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。
- 应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

个人信息安全规范 GB/T 35273

- 明确个人信息处理安全责任、目的明确、最小够用、同意和选择、质量保证、确保安全、主体参与和公开透明原则
- 明确个人信息收集、存储、使用和转让披露过程以及全生命周期过程中通用的安全要求
- 提供隐私声明和个人信息安全风险评估的实践参考

- **由有关主管部门责令改正**
- **警告、没收违法所得、处违法所得一倍以上十倍以下罚款**
- **对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款**
- **责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照**

敏感数据地图


扫描任务
分布服务器
Exchange /SharePoint/数据库
数据扫描
适配器
发现事件
扫描任务
文件服务器
SMB/NFS
共享目录
删除
隔离
复制
保护
机密信息分布视图
扫描任务
本机磁盘目录
终端
Windows/Mac
网络发现：
扫描分析存储在网络共享、Sharepoint、Domino、数据库等位置的数据，并对命中策略的内容进行记录
终端发现任务：
扫描分析存储在终端的数据，并对命中策略的内容记录进行记录

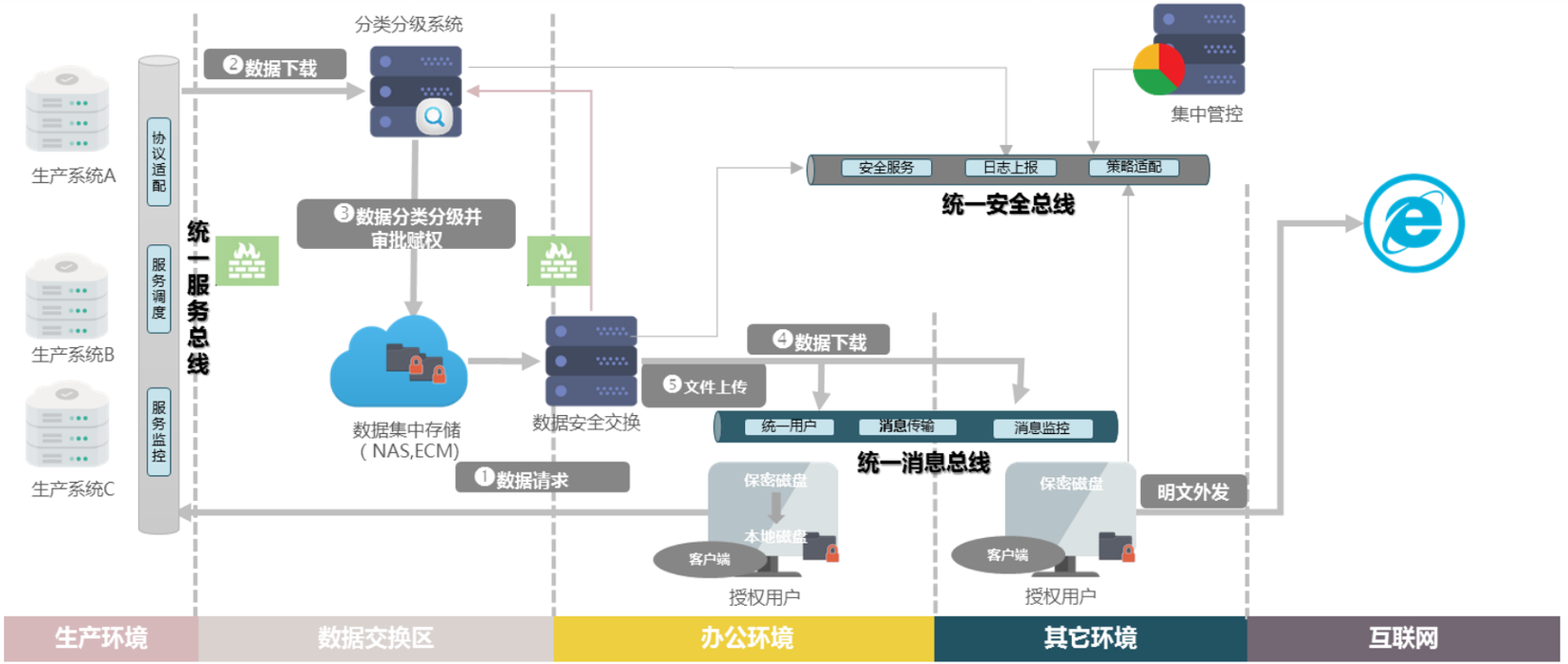
敏感数据生命周期管控方案

数据安全管控中心

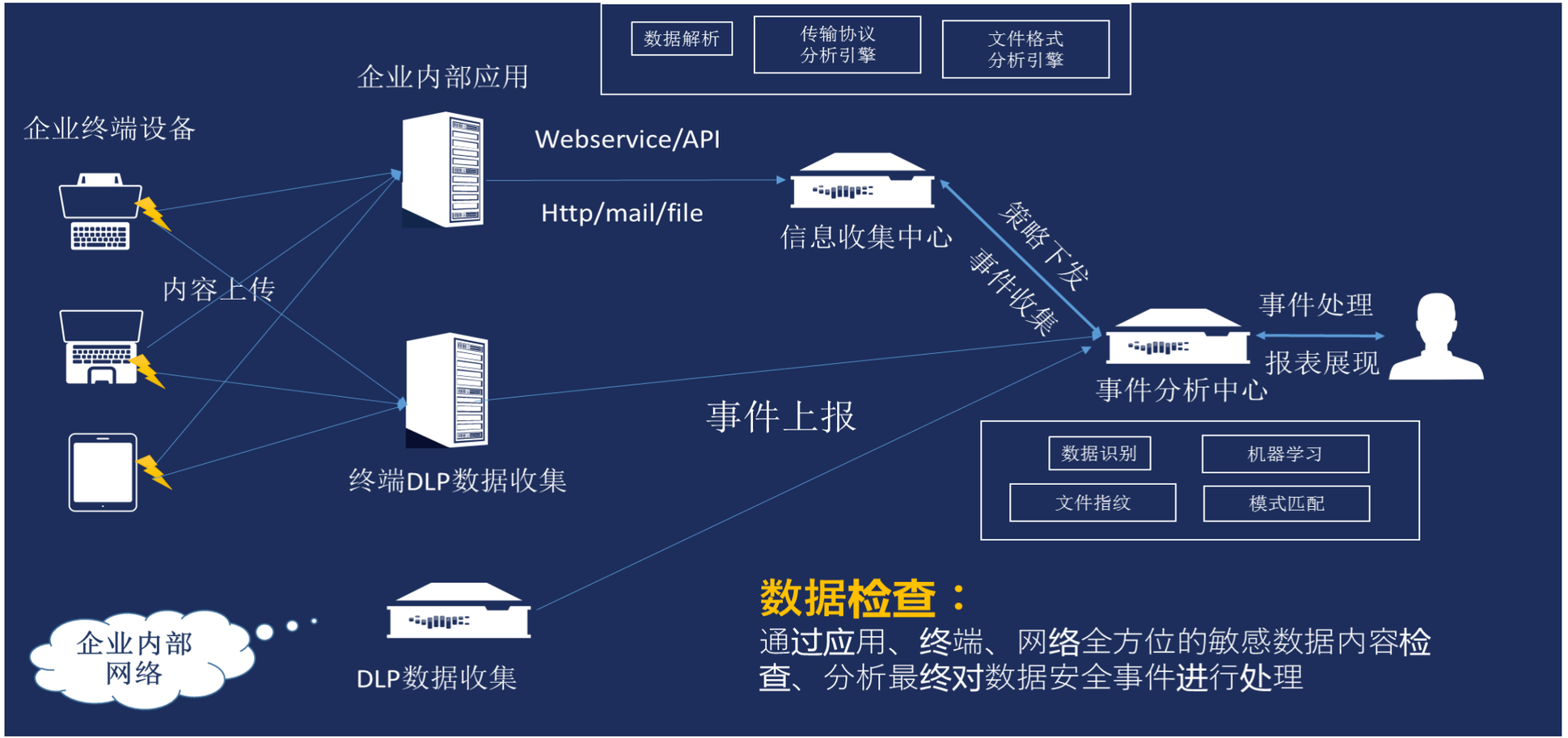
HNA 海航科技

数据安全架构设计思路

在完成核心数据识别及分级分类指导下对结构化和非结构化数据统一管理；	结构化数据资产根据其重要性采用存储加密和使用脱敏技术进行安全防护；	非结构化数据的防护采用集中存储加三总线的构建思路完成安全服务集成、安全风险集中管控、统一流通使用和监控审计的统一收集，实现数据全生命周期防控；



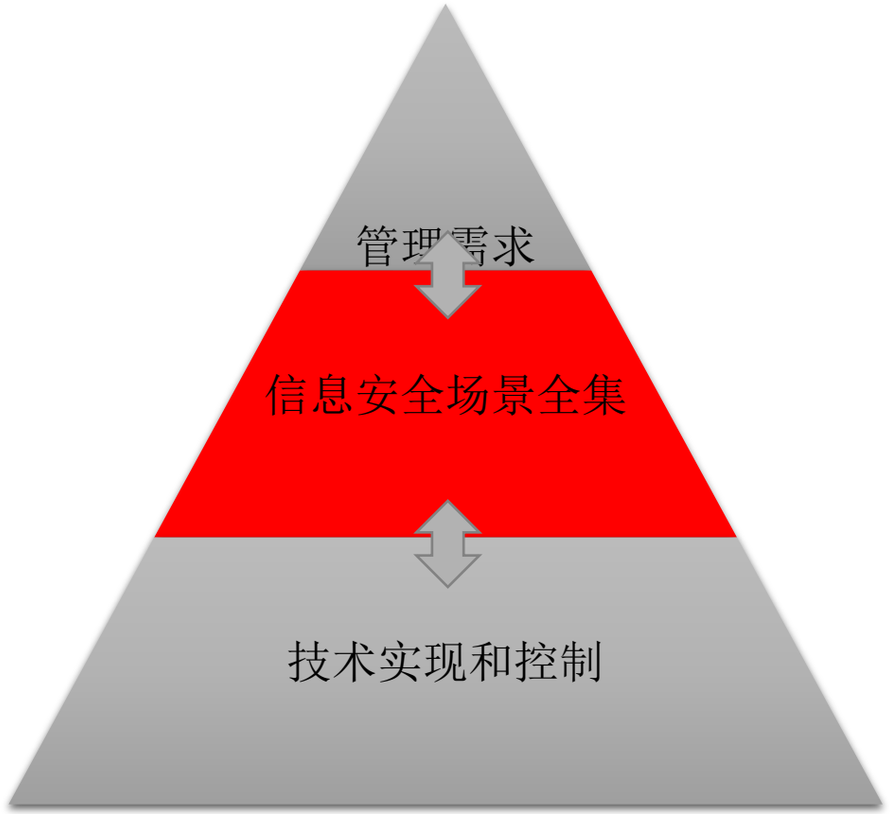
数据安全检查中心


数据解析
传输协议
分析引擎
文件格式
分析引擎
企业内部应用
企业终端设备
Webservice/API
Http/mail/file
信息收集中心
策略下发
事件收集
内容上传
事件处理
报表展现
事件分析中心
事件上报
数据识别
机器学习
文件指纹
模式匹配
终端DLP数据收集
企业内部
网络
DLP数据收集
数据检查：
通过应用、终端、网络全方位的敏感数据内容检查、分析最终对数据安全事件进行处理

CONTENT
目录

1. 平台化信息安全管理思路
2. 数据安全检查平台
3. 信息安全场景平台

USE CASE 安全场景的意义



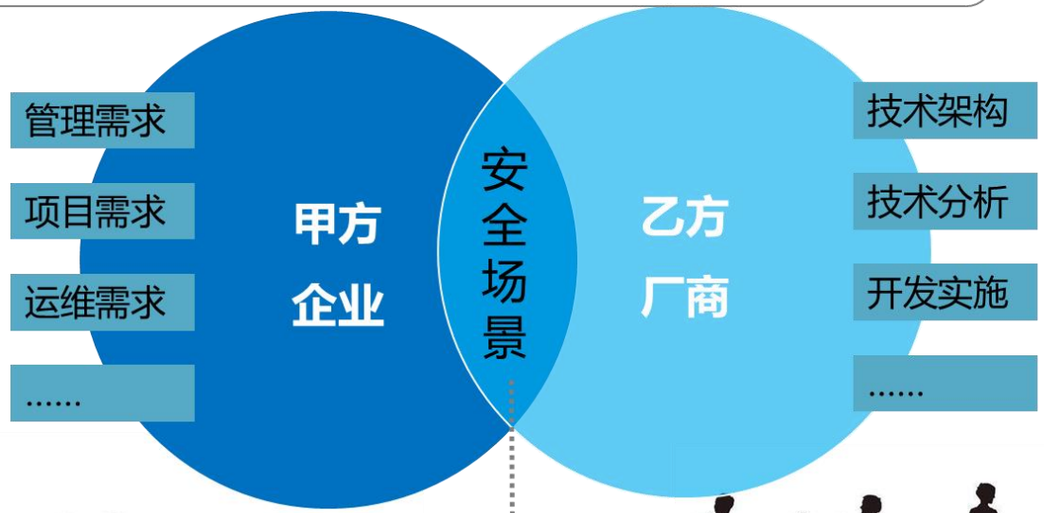
场景，让业务管理需求与技术控制措施得以良好的衔接

意义与价值

1. **信息安全技术向业务和管理转化**
2. **实现业务管理和安全技术实现的衔接**
3. **更直观的管理和展示安全管控效果**
4. **更有效的指导和推进安全方案和控制措施的实施**

国内信息安全问题

安全场景缺失：
- 乙方厂商更多关注安全技术分析和实现，对于客户的安全需求并无深入了解
- 甲方企业因安全资源有限，无法进行场景梳理



甲方企业

- 甲方受资源所限
- 乙方不关注
- 安全场景存在空白

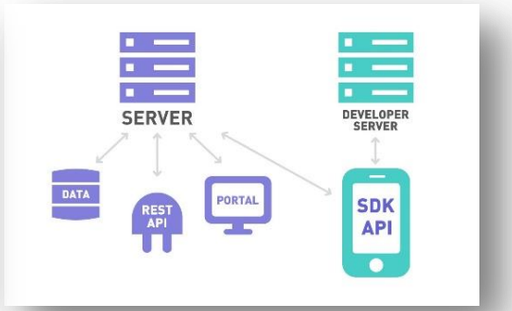
技术厂商

信息安全场景分类

基础架构场景

基础架构场景的部署，可识别感知和防护主机、网络、操作系统等全基础架构架构层面的风险与攻击

- **主机安全场景**
- **配置与操作系统场景**
- **网络安全场景**
- **云基础架构安全场景**



应用系统场景

应用系统场景部署，可识别感知和防护应用系统层的风险与攻击

- **前端安全场景**
- **中间件安全场景**
- **数据库安全场景**
- **应用系统数据安全场景**

用户终端场景

终端场景部署，可识别感知和整体防护用户终端层面的风险与攻击

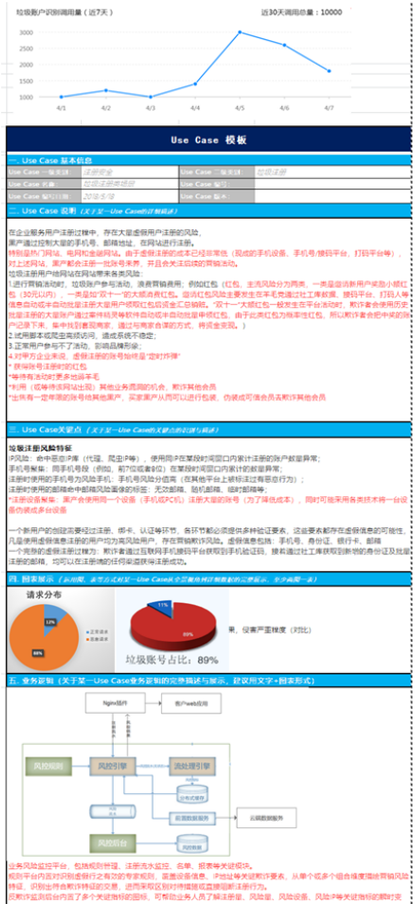
- **终端环境安全场景**
- **终端访问安全场景**
- **终端数据安全场景**
- **终端行为审计安全场景**

业务场景

业务场景部署，可识别感知和防护业务层的风险与攻击

- **账户注册安全场景**
- **用户登录安全场景**
- **营销活动类安全场景**
- **数据爬取安全场景**
- **……**

信息安全场景样例



Use-Case示例图

- 以联盟为基础，制定和发展SDC场景编写标准范式
- 对各厂商场景进行评审和认证
- 与各个厂商共同运营、共同发展场景库联盟与场景知识库

信息安全场景联盟

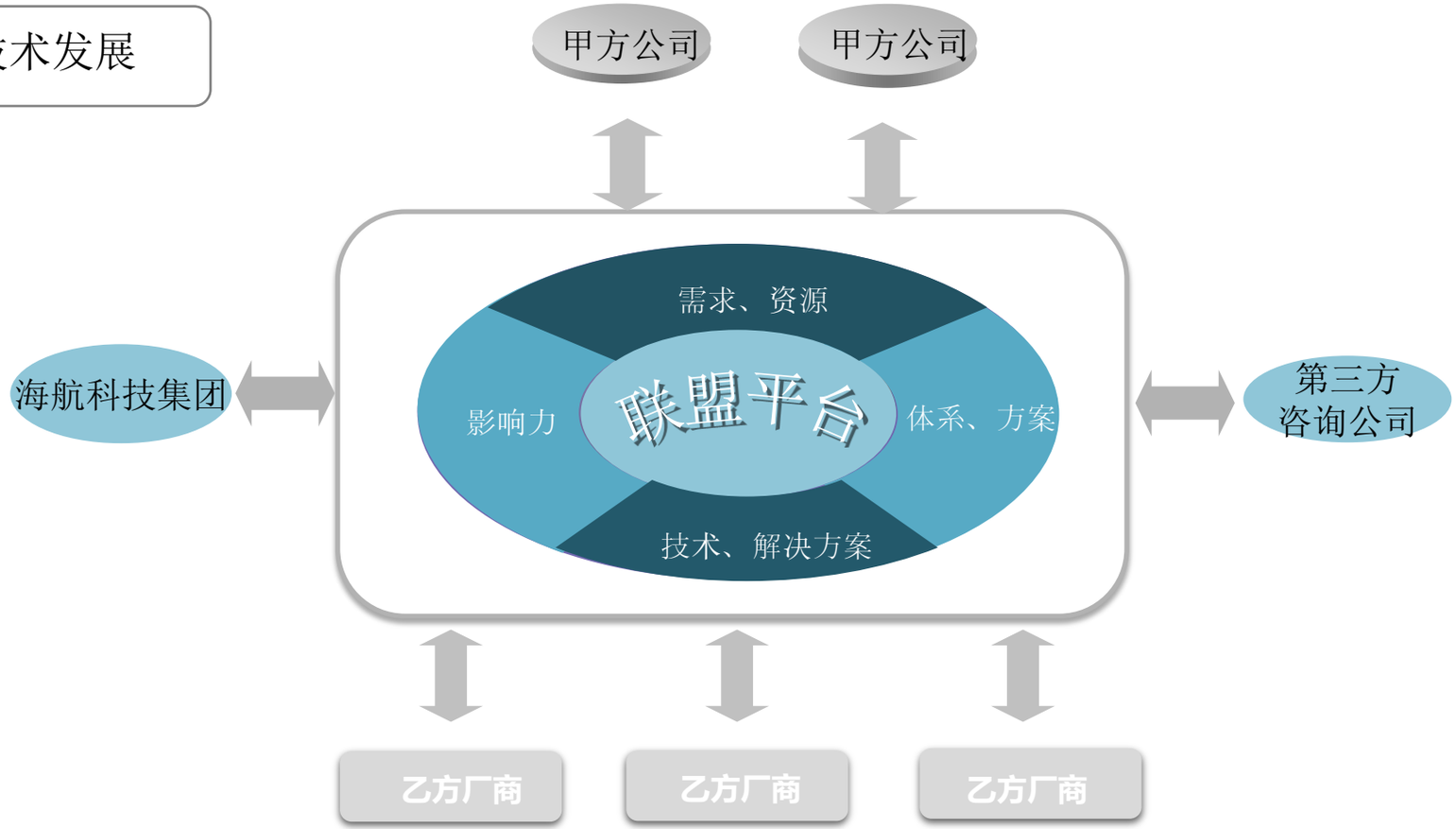
成立信息安全场景库联盟，引领行业产品技术发展

场景库联盟平台

- ✓ 以场景为切入点，为甲方和乙方提供各类场景咨询与解决方案
- ✓ 与甲方、乙方、咨询方机构共同合作，打造共享型联盟平台
- ✓ 利用海航产业资源，推动场景技术发展体系化建设

定义规则

- ✓ 充分利用海航自身优势，牵头完成场景库联盟建设，制定联盟运营机制、定义场景库分类标准、技术标准、体系标准



THANK YOU