■ 安全风险评估策略

- 支持40多种大类的风险检测规则
- 支持潜在危害分析-累计的发生次数或发生频率
- 支持关联事件分析-通过多个指标评估风险
- 支持黑白名单处理-降低系统漏报率和误报率

风险检测规则	风险检测规则
跨站点脚本	SQL注入
无效重定向	未经授权的标记
命令注入	XML外部实体注入
不安全传输协议	路径遍历
日志记录敏感信息	HTTP方法篡改
未捕获的异常	数据库访问违规
未经授权的介质	DOM跨站点脚本
XML注入	跨站点请求伪造
HTTP响应分解	JSON注入
弱认证（基本认证）	敏感目录访问
弱浏览器缓存管理	XSS跨站攻击

■ 安全风险评估策略（续）

- 支持20多种大类的风险检测规则
- 支持潜在危害分析-累计的发生次数或发生频率
- 支持关联事件分析-通过多个指标评估风险
- 支持黑白名单处理-降低系统漏报率和误报率

风险检测规则	风险检测规则
恶意代码指令分析	C&C通道检测
异常流量监测	水坑挂马检测
异常行为监测	文件共享传输检测
邮件鱼叉攻击检测	远程溢出攻击检测
漏洞扫描检测	Web后门检测
目标服务枚举	网站攻击检测
弱口令扫描检测	钓鱼/暗链检测
僵目蠕检测	网页篡改检测
隐蔽信道检测	ARP检测
Pass-the-ticket	Pass-the-hash
端口扫描检测	……

■ 异常行为分析与检测模型

数据全生命周期管理

数据采集 → 数据建模 → 数据分析 → 数据下钻 → 数据报告

■ 高级威胁检测及监测能力

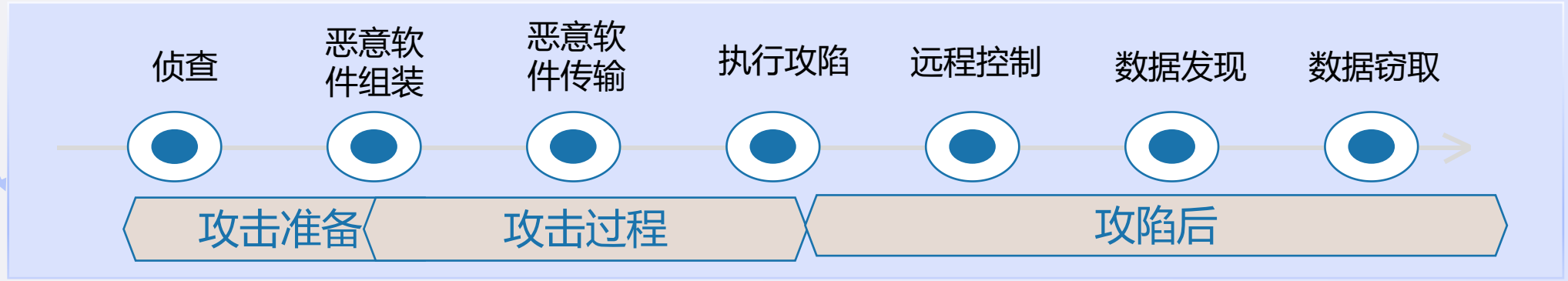
对网络安全情况进行实时统一监测，准确、及时发现各区域存在的渗透入侵攻击、非法远程控制、僵木蠕传播等隐患。

■ 安全事件响应及处置能力

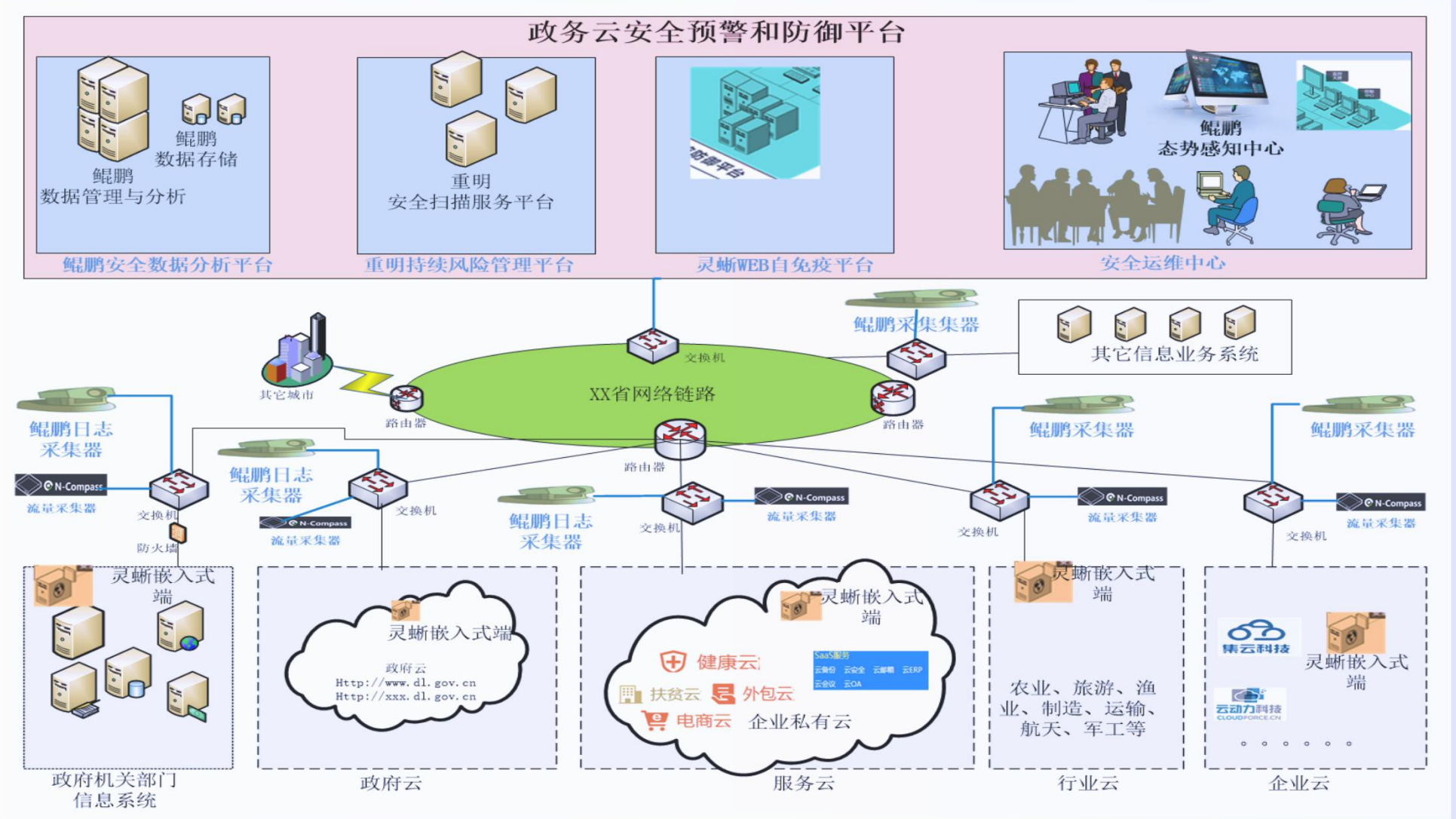
实现对重大安全事件的实时响应和快速处置。

■ 安全态势的全面感知能力

实时跟踪各类安全威胁的变化趋势，可视化呈现最新的安全态势。



■ 典型案例分析


政务云安全预警和防御平台
鲲鹏
数据存储
鲲鹏
数据管理与分析
鲲鹏安全数据分析平台
重明
安全扫描服务平台
重明持续风险管理平台
灵蜥WEB自免疫平台
鲲鹏
态势感知中心
安全运维中心
其它城市
交换机
XX省网络链路
路由器
路由器
路由器
鲲鹏采集器
其它信息业务系统
鲲鹏日志
采集器
N-Compass
流量采集器
交换机
防火墙
鲲鹏日志
采集器
N-Compass
流量采集器
交换机
鲲鹏日志
采集器
交换机
N-Compass
流量采集器
鲲鹏采集器
交换机
N-Compass
流量采集器
鲲鹏采集器
交换机
N-Compass
流量采集器
灵蜥嵌入式
端
政府机关部门
信息系统
灵蜥嵌入式端
政府云
Http://www.dl.gov.cn
Http://xxx.dl.gov.cn
政府云
灵蜥嵌入式
端
健康云
扶贫云
外包云
电商云
企业私有云
SaaS服务
云备份 云安全 云邮箱 云ERP
云会议 云OA
服务云
灵蜥嵌入式
端
农业、旅游、渔
业、制造、运输、
航天、军工等
行业云
集云科技
灵蜥嵌入式
端
云动力科技
CLOUDFORCE.CN
企业云

■ 典型案例思想


摸清家底
认清风险
找出漏洞
通报结果
督促整改
平台层
关键信息基础设施信息库
网络安全态势感知平台
网络安全通报处置平台
支撑层
专家队伍
技术支撑机构
产业联盟
(解决方案)

ANBAI TECHNOLOGY 安百科技

03

PART THREE

几点建议

■ 几点建议

- “没有网络安全,就没有国家安全”，提高安全意识，加大安全防护手段；
- 敏锐抓住信息化发展历史机遇,自主创新推进网络强国建设;
- 政府网站是政府形像和宣传窗口，最好风险评估和等级测评工作，防患未然；
- 提高站点防护手段，建设或完善安全预警和防御平台，阻止安全事件发生；
- 建设安全制度和规范，采用“安全最小原则”，谁主管谁负责；

ANBAI TECHNOLOGY 安百科技

PART FOUR

04

答疑

■ 疑问

感谢您的聆听