

从实战出发的网络安全等级保护2.0实践

亚信安全COO 陆光明





- > 网络安全等级保护2.0标准的理解
- > 践行"网络安全等级保护2.0"的几个观点
- > 网络安全等级保护2.0实践案例分享

新时代、新体系



习主席 4.19讲话



- 一、网络安全是整体的而不是割裂的
- 二、网络安全是动态的而不是静态的
- 三、网络安全是开放的而不是封闭的
- 四、网络安全是相对的而不是绝对的
- 五、网络安全是共同的而不是孤立的



新思路、新实践



从实战出发

新增内容

未知威胁防护

集中管控

溯源取证

邮件安全防护

剩余信息保护

个人信息保护

优化内容

安全审计

网络边界安全

网络访问控制

软件容错

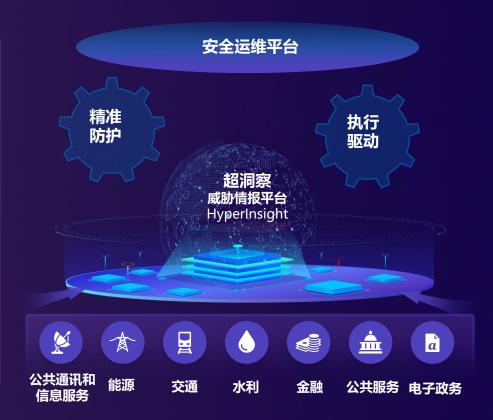
账号与口令

资源控制

强化设备与通信链 路冗余 防恶意代码与垃圾 邮件

.....

- () 主动防御
- **②** 安全可信
- 💿 动态感知
- ② 全面审计
- ◎ 应急保障



"践行网络安全等级保护2.0"的几个观点







以身份为基础,构建网络空间信任体系



以攻防为视角,提升全方位主动防御能力



以联动为策略,提升网络安全事件智能响应能力



以运维为关键,加强统一集中管控平台建设



从实战出发,建设自适应安全体系

以身份为基础,构建网络空间信任体系





身份即安全

- 以安全身份标识贯穿所有 业务应用
- 提供身份数据和隐私保护

身份即服务

- 提供内外融合的登录认证和身份鉴别服务
- 支撑内部、外部业务在内网、互联网及移 动端的开展









身份服务基础设施







内部系统 外部系统 第三方系统

未来:设备身份认证





终端

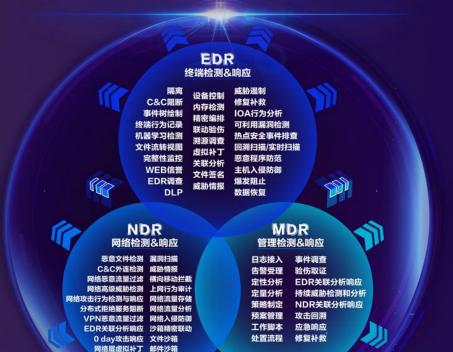
打印机

以攻防为视角,提升全方位主动防御能力





- 单点突破
- 命令与控制



横向移动

一 资料挖掘

一 资料盗窃

以联动为策略,提升网络安全事件智能响应能力 & III 信安全



持续检测 威胁发现

告警受理: 分类

告警受理: 优先级划分

检测阶段

威胁 处理响应

根据响应脚本,执行响应策略

响应阶段

威胁 定型分析

95% 的用户不需要验伤, 只需要定性分析, 快速完成修复补救



分 阶

威胁 定量分析

5% 的重点行业、重点客户、 为了保护核心信息资产,需要提 供完整的定性定量分析、攻击回 溯、验伤取证及事件调查报告

以运维为关键,加强统一集中管控平台建设





从实战出发,建设自适应安全体系



多层防御阶段

深度分析阶段

自适应阶段

特点

强调防御为主 聚焦防护产品和第三方安全基础服务 依赖个人专业能力

强调已知和未知威胁预防 聚焦安全策略自动实施 依赖联动能力 强调安全事件真实性 聚焦业务连续性 依赖应急响应流程

精密编排阶段

强调安全运营自动化 聚焦预测能力 依赖自我学习

加固和隔离系统 (漏洞以及补丁管理)

• 事故检测

• 调查及取证

基线系统攻击预测

阻断

- ・转移攻击
- ・ 事故预防 (黑白名单,病毒码)

检测

- · 风险确认和排序
- 事故隔离

响应

- 设计/模式改变
- ・ 修复/改善

预防

· 主动探索分析

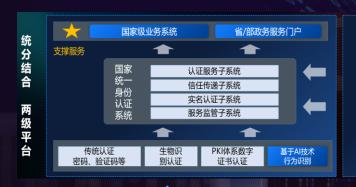
响应能力

长

短

网络空间身份管理体系实践案例-互联网+政务服务 Asialfo







全国一体化在线政务服务基础设施平台

- 以身份为核心的全国可信互认通道,实现跨地区、跨部门、跨系统的互联互通。
- 完善的用户信息隐私保护标准与技术体系,不惧拖库与信息泄露。
- 互联网级微服务系统架构, 10亿+用户规模7*24小时稳健支撑。



精准 防护 执行 驱动

数据湖

安全攻击技术视角

用户业务需求视角

安全管理聚合视角

数据价值经营视角

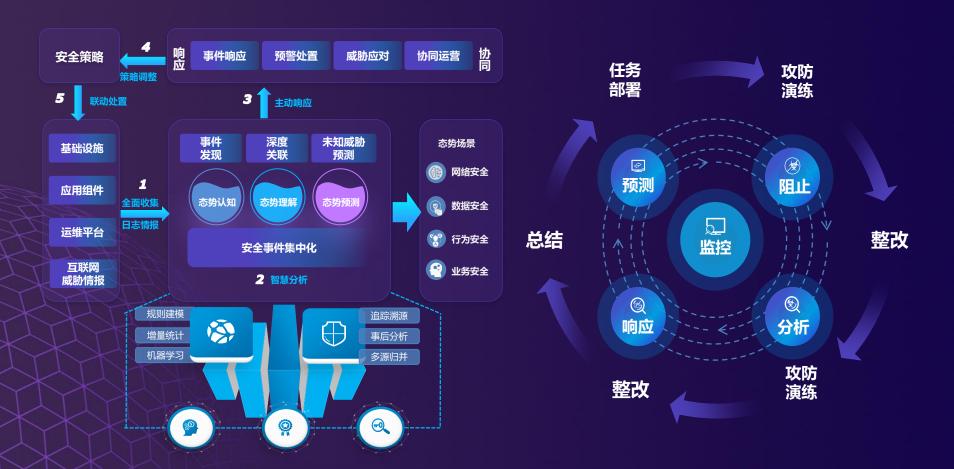
零信任



身份

动态感知和持续攻防演练实践案例-xx银行







THANK YOU