安全运营上半年报告

2025年02月 - 2025年09月

汇报单位：信息安全中心

目录

清晰列出四大核心章节：安全运营目标达成情况、工作详情、关键问题分析、下半年计划，引导听众理解报告结构。

安全运营目标达成情况

核心目标与实际成果对比

综合评估监管通报应对、业务系统防护、事件闭环等目标达成情况，突出“核心系统防护达标”与“安全短板未达标”的双面结论。

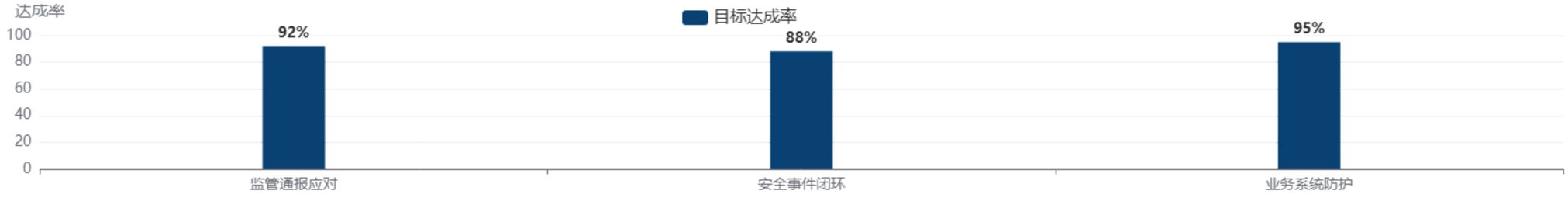
一、核心目标达成情况

- 业务连续性保障：16个核心系统弱口令整改率0%，存在29311个弱口令风险，影响业务连续性目标达成。
- 系统稳定运行保障：全年实现零宕机，关键时期保障响应时间达标，系统可用率100%。
- 业务安全防护成果：拦截196.15万次攻击，处置319起安全事件，日志分析量达425.5万条，全面保障系统安全。

二、关键问题分析

> **安全短板评估：**20个服务内资产EDR终端防护覆盖率为0%；事件响应及时率仅61.12%，未达《政府网站安全防护要求》标准。
> **遗留问题：**弱口令整改率0%，风险资产闭环率虽为100%但存在结构性隐患，成为潜在中断风险点。

安全运营目标达成对比



业务连续性与系统稳定性保障

零宕机、零中断的实现路径

通过全周期防护机制，实现16个核心业务系统100%可用率，全年零中断，7*24小时持续监控与响应，全面保障政府关键业务系统稳定运行。

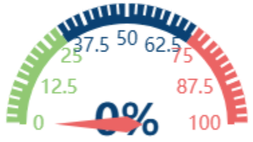
核心业务系统数量
16个

业务可用率
100%

中断事件数
0

重保成功率
0事故

业务可用率达成情况



业务连续性目标：7×24小时不中断运行，全年零中断，重点保障节假日及攻防演习期间系统稳定。

事件管理与重保服务成效

319起事件闭环，4次重保零事故

全年累计处置安全事件319起，实现100%闭环率，平均响应时间仅41分钟，显著提升安全运营效率。

在清明、五一等关键节假日，成功实施4次专项重保服务，保障业务系统零中断、零事故，实现100%可用率。

安全事件数量

319起

事件处置率

100%

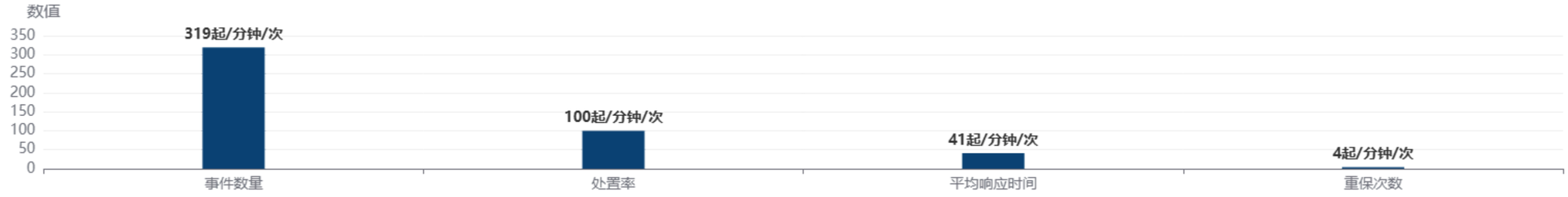
平均响应时间

41.0分钟

重保服务次数

4次

安全事件处置成效对比



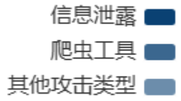
威胁管理与外部攻击态势

拦截196.15万次攻击，攻击类型分布分析

本页聚焦外部攻击态势分析，全面展示攻击拦截成果与威胁分布特征。

攻击类型分布（196.15万次）

攻击类型分布



外部攻击次数
196.15万次

攻击拦截率
100%

攻击源国家/地区分布（前五）

攻击源国家/地区分布

排名	国家/地区	攻击次数
1	中国	589,100
2	中国香港	320,800
3	安徽省	215,600

资产管理与风险资产闭环

73个IP资产，157个风险资产闭环管理

围绕政府核心业务系统，构建资产全生命周期管理机制，实现风险资产闭环治理。

资产总数
73个
IP资产全面梳理，建立完整资产台账

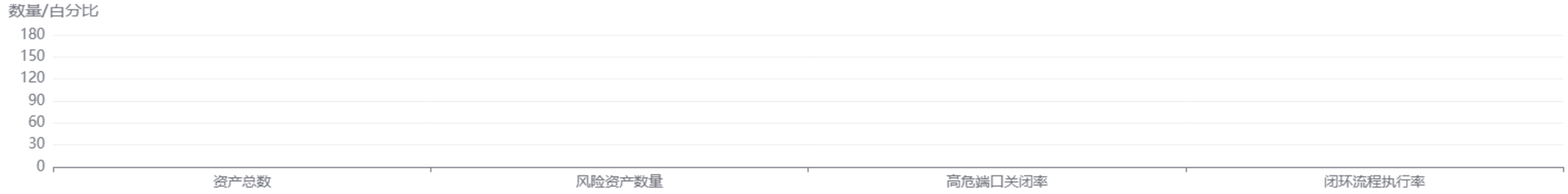
风险资产数量
157个
识别并纳入闭环管理的风险资产

高危端口关闭情况
已关闭
对公网开放的高危端口全部关闭

风险资产闭环流程
发现-通报-整改-验证-闭环
标准化流程保障整改可追溯

核心成果
实现风险资产100%闭环管理，高危端口关闭率100%，风险端口映射不存在，显著降低系统暴露面。

风险资产闭环管理关键指标



脆弱性管理与弱口令治理挑战

29311个弱口令，整改率0%，高危漏洞同比上升136.9%

当前安全运营面临严峻挑战：弱口令问题突出，29311个弱口令未完成整改，解决率0%；高危漏洞通报同比增长136.9%，漏洞扫描频率为每月一次（关键系统），修复闭环机制尚未健全，暴露出脆弱性管理与治理能力短板。

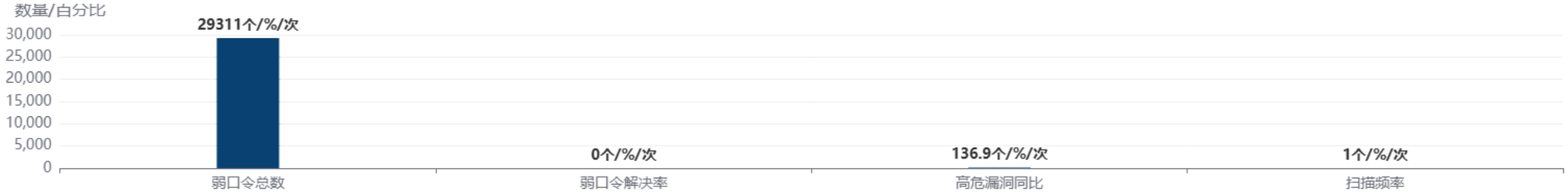
弱口令总数
29,311个

弱口令解决率
0%

高危漏洞同比增长
136.9%

漏洞扫描频率
每月一次

弱口令与高危漏洞关键指标对比



核心问题：弱口令整改率0%，高危漏洞持续激增，修复闭环机制缺失，威胁防御体系存在结构性风险。

关键问题分析与短板评估

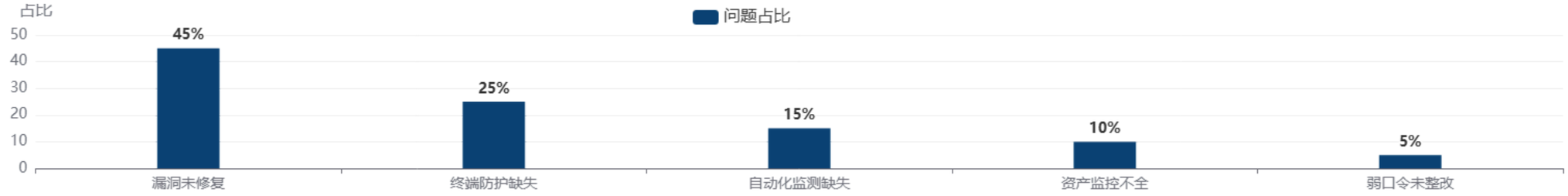
安全短板识别与根本原因剖析

当前安全运营虽保障了业务连续性与系统稳定运行，但仍存在多项关键短板，亟需系统性整改。

核心问题聚焦

- 监管通报主因：漏洞未修复占比最高，风险根源未清除
- 终端安全覆盖率：0%，20个服务内资产无终端防护，存在重大暴露面
- 自动化监测缺失：重保期间依赖人工，响应效率受限
- 资产监控不全面：157个风险资产中，32%为重要业务系统，防护盲区显著

监管通报原因占比与安全短板分布



整改建议方向

立即启动弱口令治理：优先处理16个核心系统，强制启用12位以上复杂密码策略，启用双因素认证。

全面覆盖终端安全：尽快对未安装终端防护的主机部署EDR，实现终端防护覆盖率100%。

强化资产全生命周期管理：持续梳理资产指纹信息，建立动态资产台账，提升风险预警能力。

下半年工作目标与改进计划

从被动响应到主动防御的转型路径

基于上半年安全运营成果与关键问题分析，下半年将聚焦“主动防御”能力建设，推动安全体系从被动响应向主动预防转型。

一、核心工作目标

- 全面部署双因素认证（2FA），消除单点登录风险
- 落地强密码策略，强制12位以上含大小写字母、数字与特殊字符
- 建设自动化监测能力，实现威胁事件自动发现与初步处置
- 优化威胁情报推送机制，提升预警时效性与精准度
- 升级事件响应流程，建立分级响应机制，提升处置效率

二、关键改进计划

> 事件响应机制优化建议
> 工作时间响应目标：15分钟内完成分析与通报；非工作时间：30分钟内响应，确保重大事件不扩散。

事件响应时效目标达成率