安全运营上半年报告

2025年04月-2025年09月 | 运营成果总览

监测资产
285个

安全告警
6.7万条

有效威胁
90条

事件闭环率
91.13%

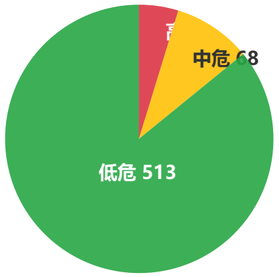
重保服务
6次0事故

封锁高威胁IP
153个

主要风险问题与整改建议

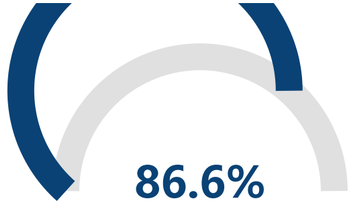
风险分析与应对措施

漏洞分布情况



总计发现漏洞 626 个，其中高危可利用漏洞 2 个

EDR安装率



未安装率 13.4%，需加强EDR覆盖

626
发现漏洞总数

2,189
弱密码风险

41
未闭环风险资产

整改措施清单

EDR安装率提升
对未安装EDR的8台服务器进行强制部署，提升覆盖率至100%

漏洞修复优先级管理
重点修复2个高危可利用漏洞，优先处置中危及以上风险

弱口令强制整改
对2,189个弱密码进行批量强制修改，建立密码复杂度策略

下半年工作计划与目标

持续优化安全运营体系

资产管理持续梳理

- 全网资产标准化流程管理，跟进资产新增替换
- 服务器网段指纹识别完善，覆盖308个子域名
- 提升威胁及脆弱性匹配准确率至95%以上

脆弱性管理

- 服务内资产全量漏洞扫描，月度1次覆盖
- 弱口令实时监测，外网高权限账号优先修复
- 漏洞修复闭环率提升至85%

威胁管理

- 持续监测外部攻击行为，7×24小时响应
- 行业威胁情报按需推送，内部资产命中检测
- 安全组件策略检查，季度3次优化

事件管理

- 高危异常实时预警，第一时间抑制
- 事件处置闭环率提升至95%
- 重大活动期间网络安全0事故

时间节点安排

Q3（7-9月）：资产梳理、漏洞扫描、策略优化

Q4（10-12月）：弱口令整改、威胁狩猎、应急演练

年度评估：12月底完成整体效果评估