xx大学安全运营上半年报告

2025年04月 - 2025年09月

安全运营工作总览

三大核心能力框架

风险预防

通过漏洞扫描、弱口令监测与威胁情报分析，主动识别潜在风险。运营期间发现626个安全漏洞（含高危45个），识别出2个高危可利用漏洞；累计监测2189个弱密码风险，未公开威胁50次，均完成风险评估与预警。

7×24监测响应

对60个服务资产实施全天候监控，累计分析589.39万余条外部日志，产生6.7万条告警，经专家研判识别90条有效威胁，全部及时响应处置。外部攻击平均每月98万次，“HTTP流量异常”与“爬虫工具”为主要攻击类型。

问题闭环

全年共发现90起安全事件，其中外网攻击11起、内网异常79起，涵盖WebShell上传、账号异地登录篡改等典型场景。通过快速隔离、封堵IP、加固系统等手段，实现72起事件闭环，整体闭环率达91.13%。

资产纳管规模：共识别285个服务器IP资产，60个服务资产100%纳入监测

风险资产处置：发现89个风险资产，完成48个闭环处理，持续推动剩余风险整改

外网暴露面管控：梳理5个根域名、308个子域名、377个对外Web资产，发现并预警5个高危端口

安全运营目标达成情况

网络防护、勒索预防及其他目标

【网络防护成果】

运营期间共监测外部安全日志589.39万余条，识别告警6.7万条，经专家研判确认90条有效威胁，均及时处置。对285个服务器IP资产全面摸排，60个服务资产实现7×24小时实时监控，防护覆盖率达100%。

【勒索攻击零发生】

通过EDR、SIP、AF等多层防护体系联动，持续监测内网异常行为，成功拦截11次实时威胁攻击，封堵153个高危IP。全年未发生勒索软件感染或数据加密事件，关键业务系统“零失陷”。

风险资产闭环率：发现89个风险资产，已闭环48个，闭环率53.9%

安全事件处置成效：全年共发现90起安全事件，闭环72起，闭环率达91.13%

外网资产暴露面管控：识别公网根域名5个、子域名308个、对外Web资产377个，发现并处置5个高危端口

脆弱性治理进展：扫描发现626个漏洞（含高危45个），识别弱口令2189个，持续推动修复中

资产管理详情

资产发现与风险闭环

资产总数

285个服务器IP资产

服务内纳入监测资产

60个

风险资产发现数量

89个

已闭环风险资产

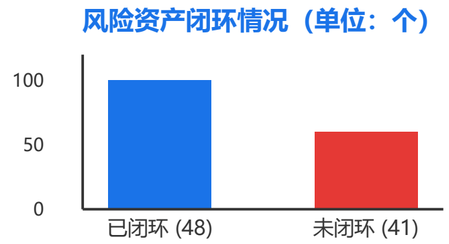
48个

未闭环风险资产

41个

对外Web资产数量

377个



威胁管理

外部攻击与情报响应

外部攻击总次数
589.39万次

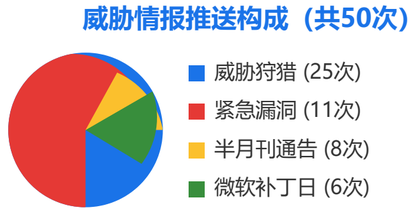
总安全告警数量
6.7万条

有效安全威胁和事件数量
90条

威胁情报推送次数
50次

威胁狩猎情报数量
25次

实时威胁告警次数
11次



事件管理

安全事件处置与闭环率

安全事件总数

90起

外网资产事件数量

11起

内网主机异常事件数量

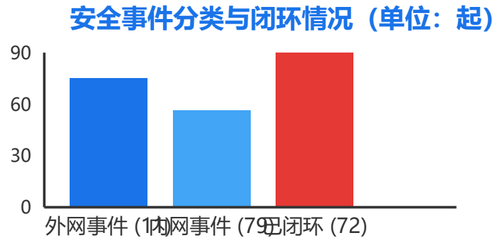
79起

已闭环安全事件数量

72起

安全事件闭环率

91.13%



增值服务

重保服务与网站监测

【重要时期值守】

在春节、五一、国庆、元旦及93阅兵等关键时期，共执行6次重保值守。期间加强监测与分析强度，每日推送安全日报，整体网络安全态势平稳，未发生攻击成功或业务中断事件。

【网站监测服务】

对互联网网站（如http://domain5.edu.cn等）实施7×24小时持续监测，本周期共发现网站篡改事件10个，已闭环处理3个；发生网站不可用事件1个，已及时恢复。部分篡改事件涉及外链植入，均已通过清理外链完成处置。

重保服务次数：6次

网站篡改事件数量：10个

已闭环网站篡改数量：3个

网站不可用事件数量：1个

安全意识与半月刊服务

安全通告与知识传递

【半月刊安全知识推送】

深信服安全团队定期发布《安全威胁半月刊》，内容涵盖国内外热点安全事件、漏洞动态、政策法规及防御建议，帮助单位持续提升安全认知水平，降低信息获取成本。

【紧急漏洞与补丁通告】

针对高危漏洞和微软补丁日，安全团队第一时间推送专项通告，提供资产影响范围分析、检测方法与修复建议，助力快速响应潜在威胁，预防攻击利用。

半月刊安全通告数量：共推送 8 次，覆盖最新威胁趋势与防护策略

微软补丁日通告数量：共发布 6 次，及时响应系统级安全更新

紧急漏洞情报数量：累计推送 11 次，涵盖Log4j、OA系统等高危漏洞

【安全意识宣导】

通过输出专题海报等宣传材料，围绕技术、操作与管理三类安全弱点开展全员意识培训，提升人员对钓鱼邮件、弱口令、非法外联等风险的识别与防范能力。

典型安全事件案例分析

代表性事件复盘

一、WebShell上传事件

典型事件描述：2025年4月14日，监测发现IP为12.255.16.252的服务器存在WebShell文件上传行为，文件名为d:\gwork\321321.aspx，攻击源IP为37.138.47.36，确认主机已失陷。

处置过程：立即隔离受影响主机，清除恶意文件，封禁攻击源IP，并更换系统密钥；同步联系开发商修复.net反序列化漏洞，建议重新部署系统并安装终端防护软件。

经验总结：业务系统存在高危可利用漏洞是攻击成功主因，需加强开发安全管控，修复前禁止外网暴露，同时部署EDR等终端防护措施提升纵深防御能力。

二、账号密码异地登录篡改事件

典型事件描述：攻击者利用应用厂商认证逻辑漏洞，通过IP 22.192.2.100从异地登录并篡改教务处教师账号权限，造成账号越权风险。

处置过程：通过SIP日志分析确认异常操作行为，在防火墙中封禁攻击IP，并重置受影响账号密码，关闭非必要远程访问权限。

经验总结：弱口令与认证逻辑漏洞易被利用进行横向渗透，建议强制实施密码复杂度策略、登录失败限制及多因素认证，提升身份安全防护水平。

共性风险：两起事件均暴露系统存在高危漏洞与弱口令问题，易被攻击者利用实现初始入侵与权限提升。

防护建议：加强漏洞闭环管理，推动开发商修复可利用漏洞；全面启用EDR、强化身份认证策略，实现快速发现与有效遏制。

关键问题分析研讨

遗留风险与改进方向

未闭环漏洞情况

当前累计存在未闭环漏洞 **442个**，主要集中在点击劫持（无X-Frame-Options头）等通用型漏洞。研究生院成绩打印系统存在SWEET32中间人攻击风险，需优先修复。

EDR覆盖不足问题

服务内共识别服务器资产285台，其中 **8台主机未安装EDR**，未安装比例高达 **86.6%**，导致终端防护能力薄弱，存在横向移动风险。

通报差距分析：现有弱口令检测手段依赖SIP流量分析和漏扫，缺乏主动渗透验证；建议补充逻辑漏洞测试，并推动业务系统强制密码复杂度与二次验证。

外部威胁监测短板：暂无EASM服务对暗网、Telegram等平台进行敏感信息泄露监测，存在数据泄露未被及时发现的风险。

根因总结

- 高危漏洞修复依赖厂商支持，闭环周期长
- 部分系统仍使用默认或弱密码策略，缺乏统一管控
- AF设备版本较低（8.0.85），不支持云威胁情报联动

致谢

感谢支持与协作

衷心感谢以下各方在安全运营工作中的大力支持与密切协作：

- ✓ 各业务部门的积极配合与信息共享
- ✓ 技术团队的快速响应与技术支持
- ✓ 安全团队的持续值守与风险闭环
- ✓ 外部合作伙伴的专业服务与协同防御
- ✓ 管理层对安全投入的坚定支持

携手共筑安全防线，持续提升防护能力。