

xx大学安全运营上半年报告

2025年04月-2025年09月

汇报人

安全运营团队

部门名称

信息中心


目录

- 01** 安全运营目标达成情况
- 02** 安全运营工作详情
- 03** 关键问题分析研讨
- 04** 下半年工作目标及计划

安全运营目标达成情况


监管通报应对与攻防演练成果

监管通报应对

 **7*24小时监测保障：**学校核心系统需要7*24小时对外提供服务，一旦业务中断容易造成监管单位通报。

运营成果：通过7*24小时监测和重保值守，确保业务连续性，**未发生因安全事件导致的业务中断和监管通报。**

攻防演练

 **重要时期重保：**攻防演习等重要时期重保，确保安全事件100%及时有效处置。

运营成果：上半年共进行**6次**重保服务，保障了单位网络安全**"0事故"**产生，所有外部攻击行为均被有效防护。



0

监管通报次数



6

攻防演练次数



6

重保服务次数

安全运营工作总览

三大核心模块体系

工作总览

安全运营工作主要围绕三大核心模块展开：**安全风险预防**、**7*24小时监测响应**、**安全问题闭环**，通过主动发现、实时监测、持续跟进，确保网络安全态势可控。



安全风险预防

- ✓ 脆弱性管理
- ✓ 威胁对抗
- ✓ 主动发现隐患



7*24小时监测响应

- ✓ 资产管理
- ✓ 实时监测
- ✓ 节假日值守



安全问题闭环

- ✓ 问题持续跟进
- ✓ 风险消除确认
- ✓ 闭环率管理



285

服务器IP资产



626

安全漏洞总数



45

高危漏洞



2189

弱密码风险

安全运营目标达成情况

网络防护与勒索预防成效

网络防护成功率



勒索攻击拦截情况



91.13%

安全事件闭环率

72/79

事件处置情况

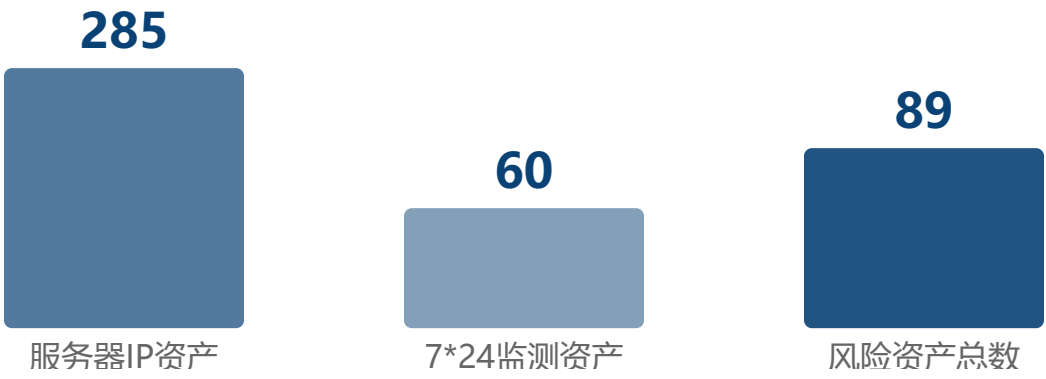
6次

重保值守任务

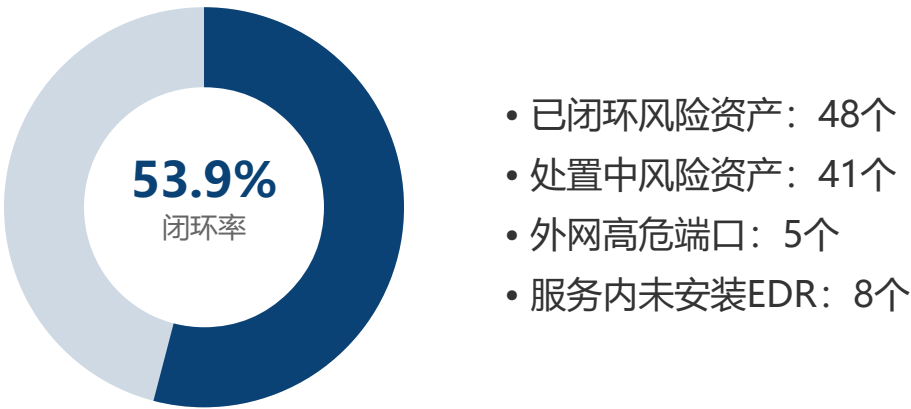
安全运营工作详情

资产管理与风险资产分析

资产统计概览



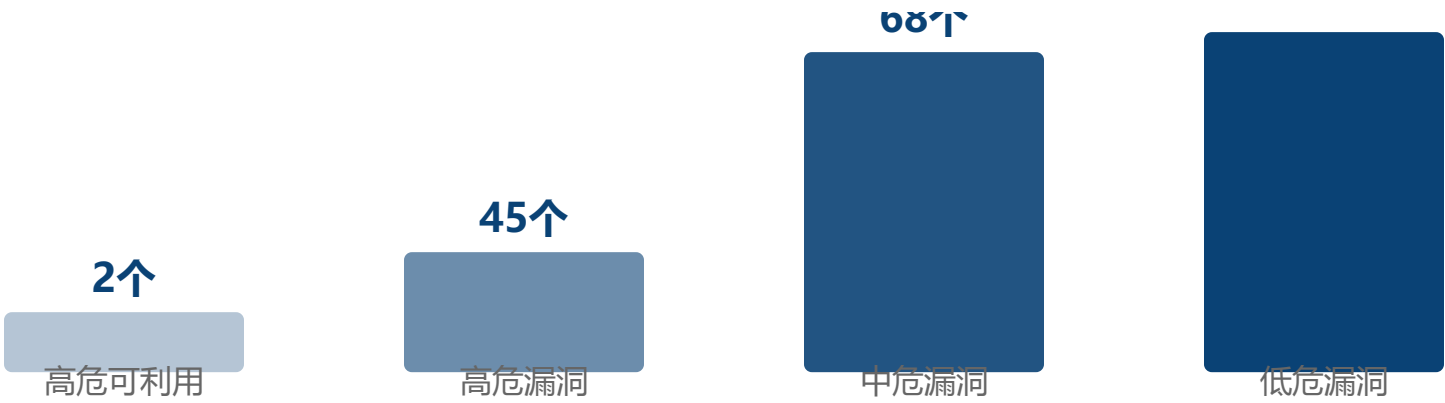
风险资产闭环情况



安全运营工作详情

脆弱性管理：业务漏洞发现与修复

漏洞风险等级分布



漏洞修复进展



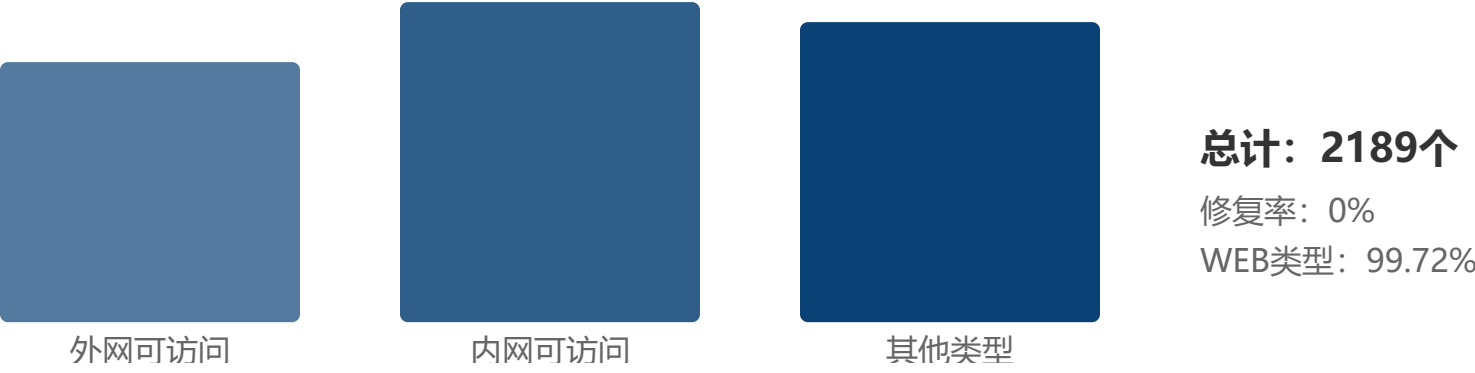
风险提示

⚠ 研究生院成绩打印系统存在SWEET32漏洞，有被劫持会话的风险

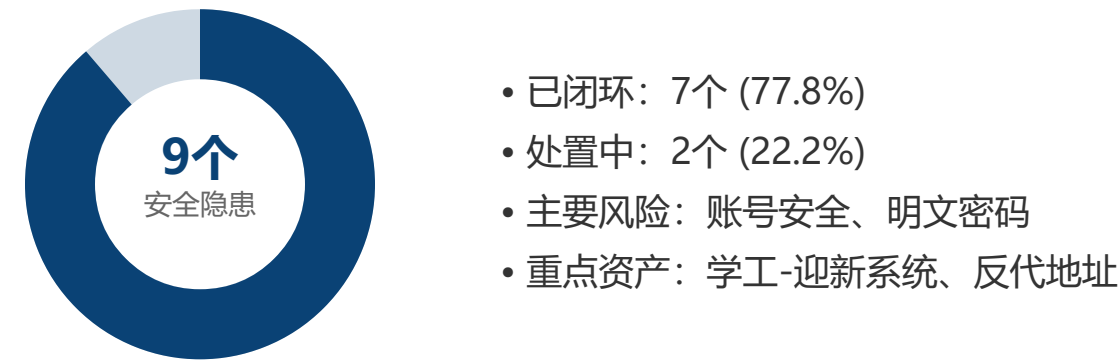
安全运营工作详情

脆弱性管理：弱口令风险与业务弱点

弱口令风险分布



业务弱点处置情况



50次

威胁情报推送

0次

威胁命中次数

100%

预警准确率

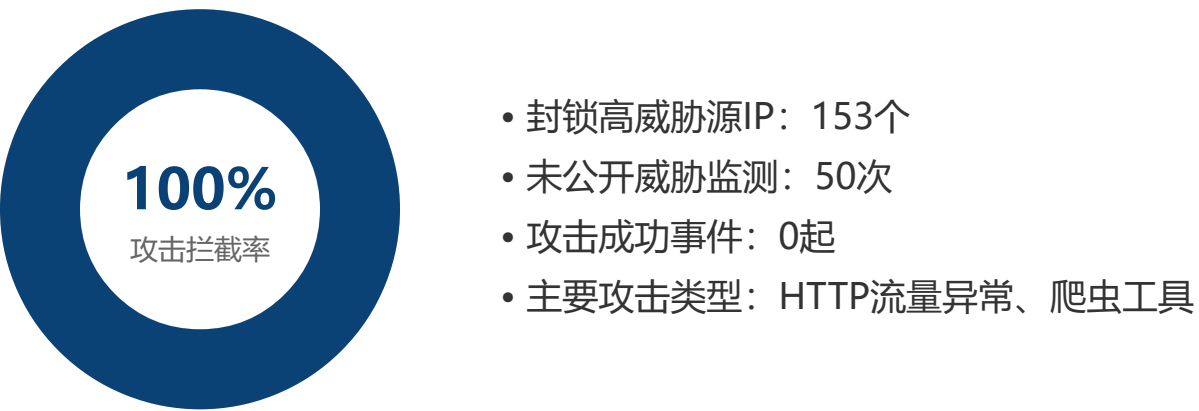
安全运营工作详情

威胁管理：外部攻击态势与防护

外部攻击态势分析



威胁防护成效




安全运营工作详情

威胁管理：策略检查与威胁情报




策略检查工作成果

**检查频次：**上半年共进行**6次**策略检查

当前状态：策略配置正常，不存在调优项

组件保障：EDR、SIP、AF等安全组件的序列号、规则库、关键防护功能均处于正常或已开启状态

威胁情报推送成效

**推送数量：**运营期间共推送漏洞威胁情报**50次**

命中情况：经检测**未发现**命中项

情报类型：威胁狩猎、紧急漏洞、安全通告等多元化情报

外部威胁事件处理

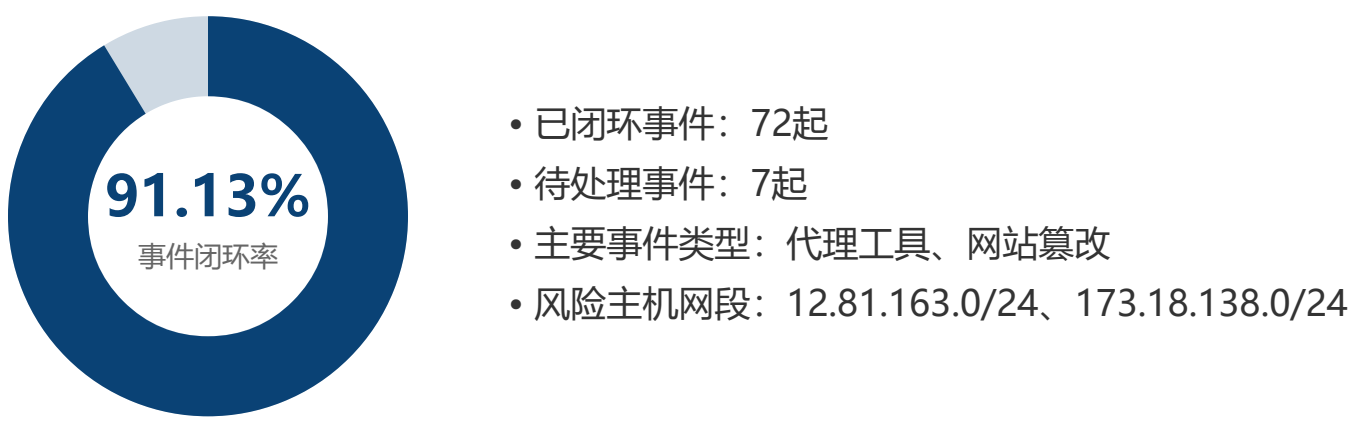
安全运营工作详情

事件管理：安全事件统计与闭环

安全事件分类统计



安全事件闭环处理情况




安全运营工作详情


事件管理：典型安全事件分析




安全事件总体情况

 运营期间新增安全事件**79起**，已闭环**72起**，闭环率**91.13%**
事件类型主要为**代理工具**与**网站篡改**
风险主机主要集中在**12.81.163.0/24**和**173.18.138.0/24**网段

典型事件案例




WebShell上传事件
主机173.18.13.37存在WebShell，已隔离文件并封堵恶意IP
建议：修复反序列化漏洞并重新部署源码




账号密码异地登录篡改事件
教务处老师账号被异地登录修改权限，原因为应用厂商认证漏洞
处置：已升级应用版本并封堵攻击IP


事件处置建议




定期开展安全意识培训




关闭非业务高危端口



加强网站篡改监测能力



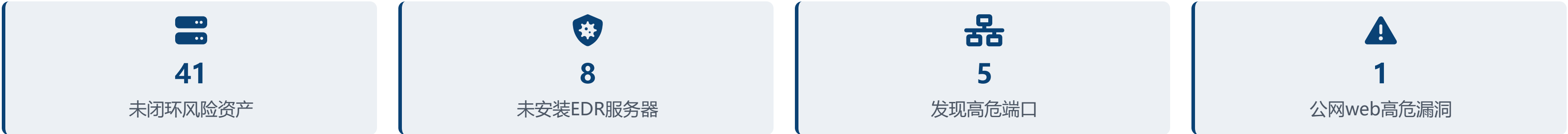
及时更新安全补丁






强化重点网段防护

关键问题分析研讨




遗留问题与改进方向







遗留问题-主机层面

-  **高危可利用漏洞闭环困难：**45个高危漏洞中442个处置中，黑客可能利用攻击导致数据丢失或勒索
-  **内网弱口令问题严重：**发现2189个弱口令，修复率为0%，攻击者可利用进行下一步攻击
-  **EDR部署不足：**8个服务器未安装EDR，未安装率86.6%，影响终端安全防护能力

通报应对差距分析

-  **缺乏深度检测：**无渗透测试和代码审计，无法发现业务逻辑漏洞
-  **情报能力不足：**AF设备版本不支持云威胁情报，威胁感知能力受限
-  **监测覆盖不全：**缺乏EASM服务监测敏感数据泄露，网站监测服务不足

改进方向建议

- | | |
|---|---|
|  技术层面： 升级安全设备版本，引入EASM服务，部署EDR全覆盖 |  管理层面： 建立强密码策略，定期开展安全意识培训 |
|  漏洞管理： 建立漏洞修复SLA机制，优先处置高危可利用漏洞 |  运营优化： 增加渗透测试频次，完善威胁情报体系 |

下半年工作目标及计划

四大领域工作规划

资产管理

持续进行资产管理和指纹识别，完善业务指纹库

脆弱性管理

发起全量漏洞扫描并跟进修复，实时监测弱口令

威胁管理

持续监测网络攻击，推送威胁情报，开展安全组件策略检查

事件管理

持续监测并协助处置高危异常，第一时间抑制影响

致谢

感谢各位领导和同事的支持与配合

让我们携手共创安全稳定的网络环境