安徽文达信息工程学院
网络信息中心
网络安全月报（七月）

报告类型： 网络安全

报告周期： 2026-07-01 09:08:00 - 2026-07-30 08:18:00

报表项内容：

一、本月网络安全总体概况

二、互联网数字资产与暴露面风险

三、漏洞与脆弱性风险

四、内外网威胁事件与翻墙上网行为分析

五、整改及安全建设建议

六、下月重点工作提示

一、本月安全总体概况

7 月份平台累计监测 3901 个 IP，产生 63 万 + 条安全告警，研判识别 199 个存在高风险行为 IP；平台依旧未启用旁路阻断自动编排功能，所有威胁仅留存告警记录，无自动封堵处置，威胁处置全部依赖人工研判操作。

本期新增翻墙上网行为专项监测，监测发现 133 个 IP 使用翻墙代理工具、1 个 IP 访问境外邪教违规网站、622 个 IP 访问境外社交网站，违规网络访问行为问题突出。

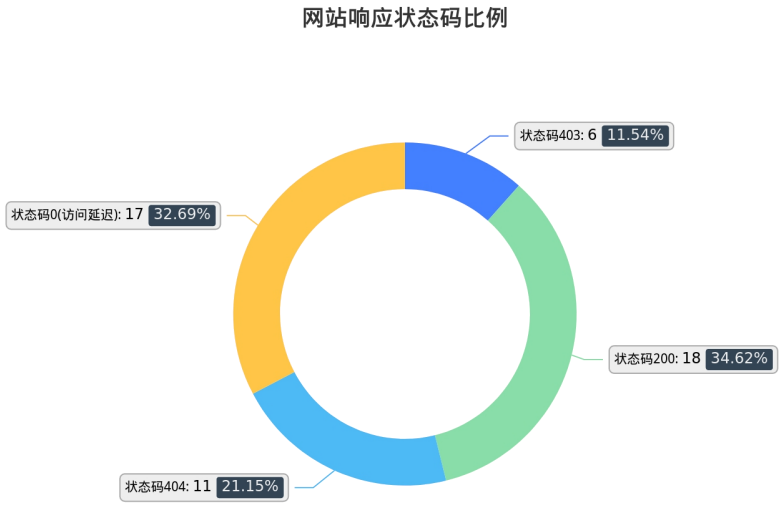
本月未发生重大网络安全事件，但多项安全风险仍然严峻：互联网存活 Web 资产 35 个，26 套业务后台登录入口直接暴露公网，新增 2 个敏感 API 接口；32 个网站存在 Struts2 等高风险易危组件；Web 系统存在 2 个高危漏洞、18 个中危漏洞；网站存在敏感文件泄露、JS 脚本黑链植入、业务系统频繁可用性故障。内网监测发现 2 台疑似失陷主机，187 台非法外联中毒主机，终端感染 xred 蠕虫、银狐远控等恶意程序。主机侧历史遗留大量未整改漏洞，FTP 弱口令风险持续存在；主机 Agent 部署数量仍为 0，主机测绘、主机脆弱性扫描任务未执行，主机层面安全监测存在盲区。

综合来看，学校主要风险集中在互联网暴露面管控不足、Web 业务系统漏洞隐患、内网终端病毒感染扩散、翻墙违规上网行为高发、安全防护能力缺失、漏洞闭环整改机制落实不到位**六大方面，需要开展专项治理，降低整体网络安全风险。

二、互联网数字资产与暴露面风险

2.1 互联网资产概览

本月监测存活互联网 Web 资产 35 个，本期无新增 Web 资产；未监测到存活互联网主机 IP 及互联网端口资产；未发现 ICP 备案、公众号、小程序、APP 等外部数字资产。
网站响应状态码统计：200 正常访问占 34.62%；404 占 21.15%；403 占 11.54%；访问超时占 32.69%，业务访问超时占比偏高，业务稳定性不足。



2.2 高风险暴露资产

1. 登录入口：共监测 26 个网站后台登录入口直接暴露互联网，包含邮箱管理员登录、报名系统后台等。后台直接对公网开放，极易遭受暴力破解攻击。
2. 敏感 API 地址：监测 5 个公网可直接访问 API 接口文档，本期新增 2 个 secret key 类型敏感接口，原有 3 个 Swagger- ui 接口。接口无鉴权控制，攻击者可获取接口参数，实施未授权访问攻击。
3. 易危组件：32 个网站使用 Struts2、Tomcat8.5 系列、CKEditor 等高风险组件，学校官网、报名系统、督导评教、邮箱系统均受影响，存在漏洞被入侵风险。
4.其它暴露风险：本期未发现公网泄露敏感代码片段、敏感文档、邮箱信息。

三、漏洞与脆弱性风险

3.1 互联网 Web 漏洞风险

本月互联网 Web 高危漏洞 2 个、中危漏洞 18 个，主要漏洞类型包含跨站脚本 XSS、CORS 跨域配置错误、明文凭证传输、应用错误信息泄露、JavaScript 库漏洞等。
受影响系统主要为学校官网、文达邮箱系统、学生综合管理服务平台、督导评教系统。官网存在跨站脚本漏洞；邮箱系统存在 CORS 配置错误、JS 组件漏洞；综合管理平台存在明文传输凭证、报错信息泄露风险。

3.2 内网主机脆弱性风险

主机扫描任务本期未执行，历史累计遗留漏洞数量较大：
优先修复漏洞：351 个
次要修复漏洞：1658 个
按需修复漏洞：619 个
弱口令：1 个

重点风险：内网 FTP 服务存在`root/root`弱口令账号，存在被爆破入侵风险；大量服务器存在 Apache、Tomcat、OpenSSH、Oracle 数据库、VMware ESXi 高危 CVE 漏洞，部分漏洞支持远程利用。

3.3 网站安全监测风险

本月网站安全监测结果：敏感词 0 条；敏感文件 1 个；黑链 / 挂马 7 条；网站篡改 0 条；可用性故障 27 起。

1. 敏感文件泄露：官网公开 Excel 文档，内部包含大量师生手机号信息，造成个人信息泄露。
2. 黑链植入：官网 js 脚本文件持续被植入色情、博彩类黑链跳转链接，损害学校公信力，会造成搜索引擎降权。
3. 业务可用性故障：学生综合管理平台、学校官网、邮箱系统频繁出现 502 Bad Gateway、访问超时故障，影响师生业务正常使用。

四、内外网威胁事件与翻墙上网行为分析

4.1 内网安全事件

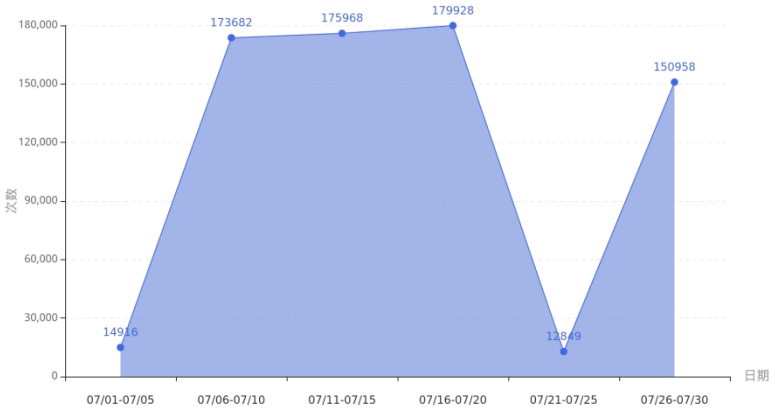
1. 可疑失陷主机：监测 2 台内网主机流量行为异常，判定疑似失陷，存在对外攻击行为，需要隔离、取证、全盘查杀病毒。
2. 非法外联中毒主机：共 187 台主机存在病毒木马外联告警，终端感染 xred 蠕虫家族、银狐远控、zegost 后门等恶意程序，持续访问外网 C2 恶意域名。蠕虫病毒存在内网横向扩散风险，全部告警处置状态为未处置。

现状：无主机 Agent，无法开展主机深度检测，风险识别仅依靠流量告警。

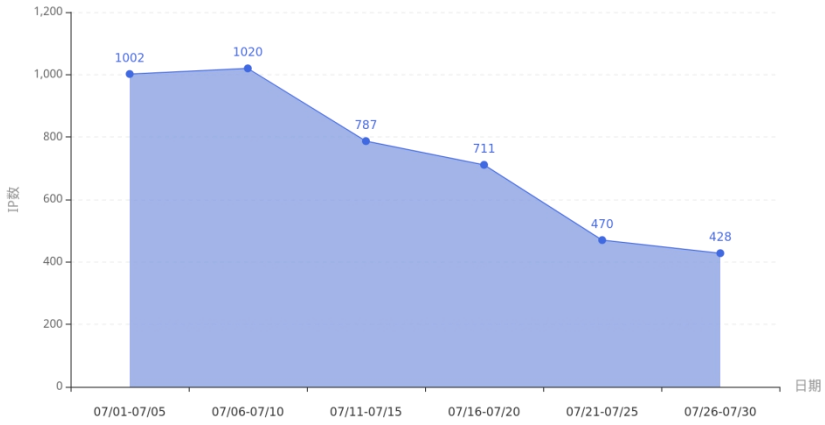
4.2 外网威胁告警

本月捕获外网攻击 IP171 个，其中高风险 IP10 个、中风险 IP17 个、低风险 IP144 个，0 个 IP 自动阻断，全部依靠人工处置。攻击来源包含安徽合肥、江苏南京、西班牙、俄罗斯等境内外 IP。
攻击行为以口令登录暴力破解、端口扫描、可疑网络行为为主；平台未开启自动阻断编排，恶意 IP 仅留存日志，可以持续探测校内资产。

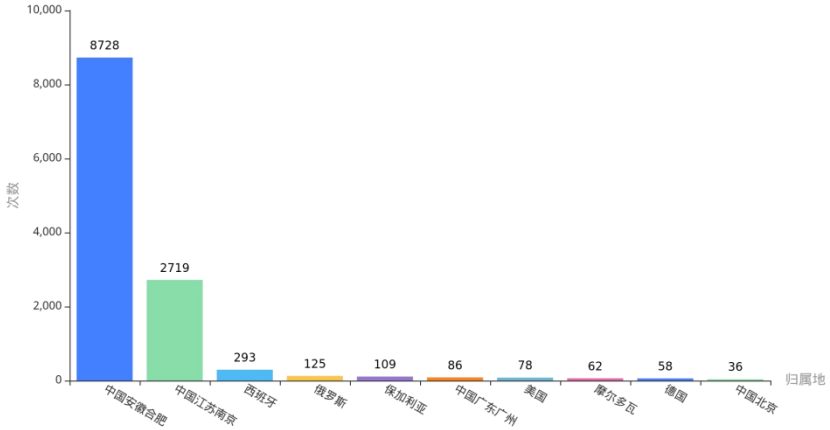
攻击次数趋势



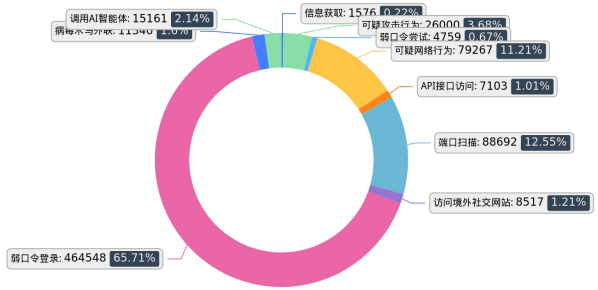
攻击IP数趋势



攻击归属地TOP10



攻击类型统计



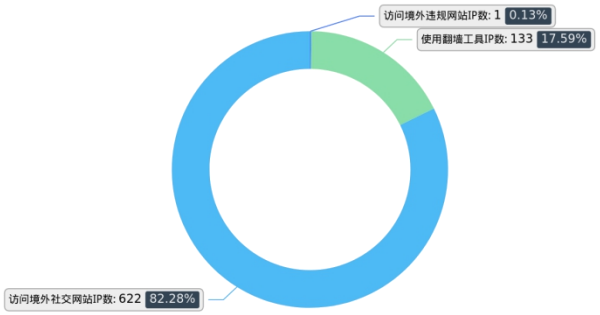
4.3 翻墙上网违规行为专项监测

监测周期内，共监测到 133 个 IP 使用翻墙代理工具、1 个 IP 访问境外邪教违规网站、622 个 IP 访问境外社交网站。

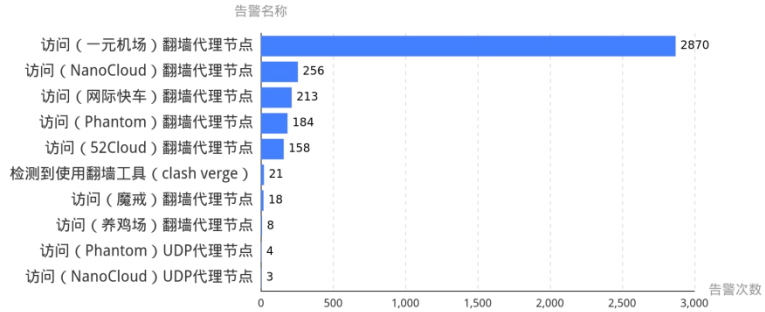
1. 翻墙代理工具行为：告警共计 14 类，其中 “一元机场” 代理节点告警数量最高，其次为 NanoCloud、Phantom 等翻墙工具，存在大量高频告警 IP，部分 IP 持续长时间使用翻墙代理。
2. 境外违规网站访问：1 台内网 IP 访问邪教类境外网站 www.soundofhope [.] org，属于严重网络安全违规行为，需要溯源核查责任人。
3. 境外社交网站访问：共 8 类境外社交网站访问记录，访问量最高为 facebook、youtube，其次为 twitter、instagram。

> 风险说明：私自使用翻墙工具违反网络安全相关管理规定，同时翻墙工具来源复杂，极易带入木马病毒，造成终端中毒、账号密码泄露；访问邪教违规网站存在重大意识形态安全风险，需要开展专项核查、警示教育。

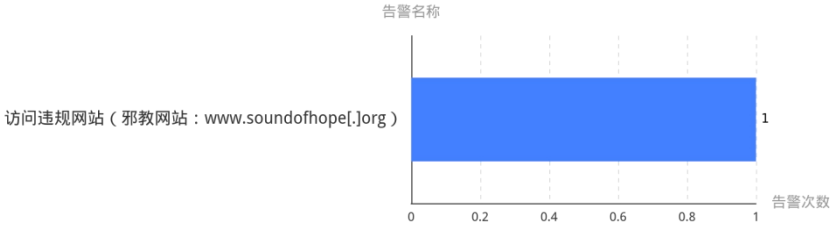
翻墙上网总体情况



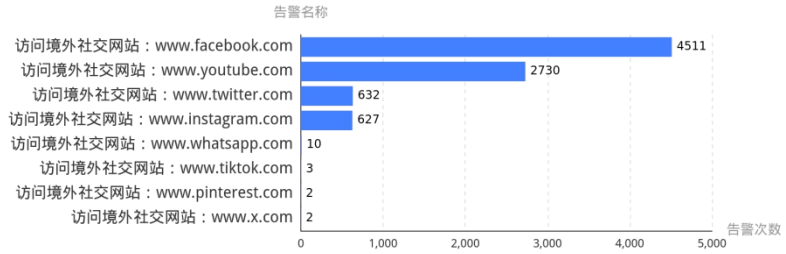
翻墙工具告警统计



境外违规网站告警统计



境外社交网站告警统计



4.4 安全运营任务执行现状

主机资产测绘：本期未执行
网站资产测绘：本期未执行
主机脆弱性扫描：本期未执行
网站脆弱性扫描：执行 8 个任务，扫描 4 个网站
网站黑链 / 敏感文件监测：下发任务监测 4 个网站
流量探针：部署 1 个流量探针，开展流量威胁监测
蜜罐部署：0 个蜜罐 IP，未启动
主机 Agent：0 台服务器 / 终端安装，在线 Agent 为 0

核心短板：主机测绘、主机漏洞扫描任务缺失，Agent 零部署，内网服务器、终端缺少主机层面安全检测，大量风险只能被动依靠流量告警发现，无法做主机基线核查、病毒查杀、异常行为监测。

五、整改及安全建设建议

5.4 漏洞闭环与防护策略

1. 建立漏洞分级整改台账，压实整改责任主体
依托平台扫描结果，完善漏洞整改台账，台账字段包含漏洞编号、受影响资产 IP/URL、漏洞风险等级、漏洞描述、影响业务系统、责任运维部门、整改时限、整改措施、复测结果。严格执行 “高危优先、业务优先”，将 Apache、Tomcat、OpenSSH、Oracle 数据库、VMware ESXi 等远程可利用高危漏洞列为第一优先级；官网、报名系统、综合管理平台、邮箱系统等关键业务资产漏洞优先处置。落实 “谁主管、谁运维、谁负责”，杜绝漏洞长期搁置。
老旧业务系统无法直接打补丁升级，需要书面记录现状，落实临时补偿防护手段，严禁只登记漏洞不做防护。
7 月仍然未执行主机资产测绘、主机脆弱性扫描任务，需要尽快补做，补齐主机侧漏洞数据，完善台账内容。
2. 落实漏洞整改- 复测闭环管理，杜绝虚假整改

严格执行 “漏洞发现→下发整改通知→实施修复→漏洞复测→闭环归档” 全流程闭环。漏洞修复后，不能仅依靠运维人员口头确认，需要通过安全平台重新扫描复测，确认漏洞消除后，方可标记闭环。复测仍存在漏洞的资产，执行二次督办，约谈运维负责人，深度分析无法整改的根因。
因业务兼容、系统停止维护等客观约束无法直接修复的漏洞，落实补偿防护，包含防火墙源 IP 限制、WAF 防护规则、网络逻辑隔离；开展风险评估，留存风险豁免审批文档，定期复评风险，条件具备时正式修复。
优先处置 FTP `root/root`弱口令，修改高强度密码，严格限制 FTP 访问源地址，整改完成开展账号安全专项复测，防范弱口令复现。针对 Web 系统 XSS、CORS 配置错误、老旧 TLS 协议、明文凭证传输等漏洞，督促网站运维完成配置加固。
3.启用平台旁路阻断编排功能，强化对外攻击自动防御能力
本月监测 171 个外网风险攻击 IP，包含 10 个高风险 IP，平台尚未启用旁路自动阻断编排，恶意 IP 只留存告警日志，完全依赖人工处置，响应滞后，容易错过攻击处置窗口期。尽快完成旁路阻断编排上线，配置自动化阻断策略：暴力破解、漏洞探测、恶意外联、Web 攻击等高风险源 IP 自动拦截；配置白名单，保障校内、合作单位合法 IP 不被误封；留存阻断审计日志，按月复盘攻击 IP、统计攻击趋势。同时保留人工处置流程，运维人员每日巡检外网告警，确认恶意 IP 执行手动拉黑，弥补自动策略覆盖不足。
4.常态化开展漏洞扫描与安全检测工作
改变主机漏扫长期不执行的现状，建立常态化扫描机制：主机脆弱性扫描至少每月执行一次；网站脆弱性扫描每两周执行一次；业务上线、版本迭代、配置变更后执行专项临时扫描，防止变更引入安全漏洞。依托资产测绘能力及时识别新增互联网暴露资产，做到新增资产即扫描。
分步推进主机 Agent 部署，优先覆盖核心业务服务器，逐步扩展到重点办公终端，补齐主机监测短板。定期核查扫描任务运行状态，及时处理任务失效、调度异常问题，避免扫描任务长期失效无人知晓。
5. 漏洞数据汇总分析，驱动系统架构优化
按月统计全部漏洞数据，梳理高频漏洞类型。针对反复出现的同类漏洞，溯源问题根源，区分开发编码缺陷、组件版本管控缺失、上线流程缺少安全检查。将统计分析结果同步开发、运维部门，推动安全前置到开发上线环节，从源头减少漏洞，而不是仅依赖事后扫描修复。针对大量 Struts2 组件风险，梳理业务系统清单，推进老旧组件升级或部署虚拟补丁防护。

5.5 安全管理建议

1. 分层分类开展全员网络安全宣传与技能培训，增加翻墙违规专题教育
面向不同对象开展差异化安全教育。面向全体师生，重点开展终端安全意识培训，讲解蠕虫病毒、远控木马、钓鱼邮件识别防范；重点增加私自翻墙上网的法律风险、意识形态风险警示教育，明确校园网禁止私自使用翻墙代理工具，讲解翻墙工具带来病毒感染、账号泄露的危害；针对监测到访问境外

邪教违规网站的 IP，开展溯源核查，对责任人开展警示教育。教育师生不运行来源不明软件，及时更新补丁和杀毒库，降低终端中毒概率，从源头减少非法外联、翻墙违规事件。

面向业务系统运维人员，开展专项安全运维培训，培训暴露面收敛、漏洞修复、Web 加固、恶意事件处置、日志审计实操，结合本月内网蠕虫感染、网站黑链、敏感信息泄露、翻墙违规等案例开展警示教育。

面向信息化安全管理人员，重点培训威胁研判、平台操作、网络安全事件应急处置流程，提升整体安全运营能力。培训做好签到、课件、记录归档。

2. 落实内网网络分区隔离，遏制病毒横向扩散风险

本月监测 187 台非法外联中毒主机、2 台疑似失陷主机，内网蠕虫病毒传播风险高。推进内网安全域划分，划分为办公终端域、学生终端域、业务服务器域、核心数据库域，域之间配置访问控制策略，严格管控跨域访问。办公、学生终端域禁止直接访问核心业务服务器；服务器之间按照最小权限开放端口，阻断蠕虫木马横向传播路径。

建立中毒主机快速隔离机制：平台监测恶意外联、失陷告警后，将主机隔离至隔离 VLAN，禁止访问内网其他业务，全盘杀毒、风险核验安全后恢复网络权限。配置边界 DNS 过滤、黑名单，拦截终端访问外网恶意域名、C2 服务器，阻断木马外联通道。针对翻墙行为，在出口做好策略管控，对翻墙代理节点域名、IP 做访问拦截。

3. 完善数据备份与网络安全应急处置预案，定期组织演练

梳理官网、报名系统、学生综合管理平台、邮箱等核心业务系统，落实本地 + 异地备份策略，执行全量 + 增量备份，定期验证备份数据可恢复性，应对网站篡改、病毒加密、系统故障瘫痪风险。

修订学校网络安全应急预案，明确事件分级、告警研判流程、处置分工、上报流程、溯源取证、事后复盘流程，针对网站黑链篡改、蠕虫大规模爆发、服务器入侵、敏感信息泄露、访问境外违规网站等典型场景编制处置操作手册。结合 7 月真实风险开展应急演练，模拟内网蠕虫爆发、网站黑链植入、翻墙违规意识形态风险场景，检验处置能力；演练完成复盘优化预案。严格落实网络安全事件上报制度，发生重大网络安全事件按照上级主管部门要求及时上报。

4. 强化系统上线变更安全管控，把好安全准入关口

建立系统上线、版本变更安全检查机制。新业务上线前完成安全测评、漏洞扫描、暴露面核查，禁止高危漏洞、后台管理接口直接暴露公网的系统直接上线。版本升级、配置修改完成后开展安全复核，避免变更引入新风险。新增 Web 资产第一时间纳入安全监测范围。

强化外包开发运维管理，对外包建设运维网站明确网络安全责任，要求外包遵循安全开发规范，交付系统完成自查；定期对外包运维网站开展安全抽查，防范漏洞、黑链、信息泄露。

针对 26 个直接暴露公网的后台登录入口，开展访问收敛，后台限制内网 / IP 白名单访问，远程运维优先使用 VPN、堡垒机。下线不必要对外公开 Swagger 接口，确需使用的接口增加鉴权控制，禁止公网直接访问。针对本期新增 secret key 敏感 API 接口，立即核查接口权限，关闭不必要对外访问权限。

5. 健全常态化巡检考核机制，推动安全风险闭环落地

执行月度网络安全风险巡检，依托安全月报跟踪上月风险整改情况，对逾期未整改风险持续督办。将网络安全风险整改落实情况纳入运维岗位绩效考核，提升运维人员重视程度。持续梳理全量资产台账，摸清互联网 Web、内网服务器、终端资产，消除资产 “看不见、管不到” 的盲区。持续优化平台告警规则，过滤无效告警，提升告警研判效率。按月向各业务主管部门通报本部门业务系统安全风险，压实业务部门主体责任，形成 “监测- 通报- 整改- 复测- 考核” 常态化安全管理闭环。

每月导出翻墙上网行为监测数据，对高频翻墙 IP 进行通报溯源，纳入网络安全考核管理。

6. 推进安全能力补齐建设

当前主机 Agent 部署为 0，主机测绘、主机漏洞扫描任务缺失，主机安全监测短板明显。分步推进服务器、重点终端 Agent 部署，实现主机日志采集、异常行为监测、病毒查杀、基线核查能力，改变只依靠外部流量扫描的被动防御模式。

评估 WAF、堡垒机设备使用效果；对公网暴露业务完善 WAF 防护规则；推广堡垒机开展服务器运维，减少直接对公网开放管理后台。梳理 Struts2 组件业务清单，制定组件升级或虚拟补丁防护方案。针对官网敏感泄露文件、JS 黑链开展专项清理，删除公网敏感文档，清除 JS 黑链代码，排查 Webshell 入侵痕迹。针对学生综合管理平台、邮箱系统频繁 502、访问超时，排查服务器资源瓶颈，优化业务，保障业务可用性。

六、下月重点工作提示

1. 优先处置内网 187 台非法外联中毒主机、2 台疑似失陷主机，分批隔离查杀，遏制蠕虫病毒扩散；
2. 专项处置翻墙上网违规行为：溯源访问境外邪教网站 IP，开展警示教育；梳理高频翻墙 IP，落实管控，加强全校翻墙安全宣传教育；
3. 互联网暴露面专项收敛：26 个后台登录入口、5 个敏感 API 接口整改管控；清理网站敏感泄露文件，清除网站黑链代码；
4. 补全主机测绘、主机脆弱性扫描任务，启动主机 Agent 部署试点；
5. 完成旁路阻断编排功能配置启用；
6. 开展高危漏洞、FTP 弱口令专项整改，完成复测闭环；
7. 完善内网安全域规划，推进网络隔离策略落地；
8. 开展网站可用性故障排查，解决官网、邮箱、综合管理平台频繁超时、502 故障。