校园网络IPv4/IPv6威胁监测与处置体系的规划与实践

东北大学 王宇

2020年12月2日

东北大学

东北大学，辽宁沈阳，门户网站：www.neu.edu.cn（neu6.edu.cn、neu.cn）

- 始建于1923年4月26日，是一所具有爱国主义光荣传统的大学。1928年8月至1937年1月，著名爱国将领张学良将军兼任校长。
- 1949年3月，沈阳工学院 —》1950年8月，东北工学院 —》1993年3月，复名为东北大学。
- 国家首批“211工程”和“985工程”重点建设的高校，2017年9月，经国务院批准，进入一流大学建设行列。
- CERNET东北地区网络中心、CNGI-CERNET2沈阳核心节点和中国教育科研网络ChinaGrid东北大学节点依托高校。

报告简介

- 年会录用论文《校园网络IPv4/IPv6威胁监测与处置体系的规划与实践》
  - 作者：王宇，温占考，王卫东，王兴伟
- 论文相关工作主要由温占考、王卫东两位老师日常建设和运维，我个人只是系统化和文字化，以满足学术论文的基本要求。

报告简介

- 2019年CERNET年会报告“新形势下高校网络安全管理”：网络安全等级保护2.0视角下的高校网络安全建设
- 2020年CERNET年会报告
  - 从攻防演练视角，聚焦重要时期网络安全保障需求，对高校网络安全体系建设进一步系统化和体系化；
  - 结合学校信息化建设和网络安全工作阶段性成果，介绍东北大学校园网络监测与处置体系方面的实践和经验。

报告提纲

- 信息化建设和网络安全工作阶段性成果
- 日常时期和重要时期网络安全保障需求
- 校园网络威胁监测与处置体系规划与实践
- 结束语

信息化建设和网络安全工作阶段性成果

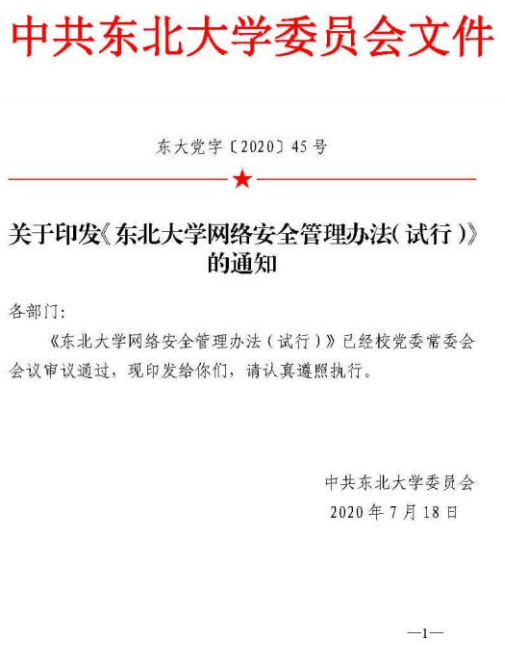
信息化建设和网络安全工作阶段性成果

- 2018年学校组建信息建设与网络安全办公室，信息化建设和网络安全工作进入新阶段。
- 在学校党委领导和支持下，信网办领导班子和全体人员共同努力实现：
  - 分散建设向统筹建设转变
  - 多头运维向集中管控演进
  - 杂乱服务向集约服务推进
  - 数字校园向智慧校园过渡

信息化建设和网络安全工作阶段性成果

- 2020年下发多份信息化建设和网络安全相关文件
  - 《东北大学网络安全管理办法（试行）》（东大党字〔2020〕45号）
  - 《东北大学落实网络安全责任制考核评价实施办法（试行）》（东大党办字〔2020〕11号）
  - 《东北大学信息化项目建设管理办法（试行）》（东大校字〔2020〕67号）
  - 《东北大学网站群管理规范》（东大信网字〔2020〕4号）
- 2020年开始对各部门开展网络安全责任制考核评价

信息化建设和网络安全工作阶段性成果



中共东北大学委员会文件

东大党字〔2020〕45号

关于印发《东北大学网络安全管理办法（试行）》的通知

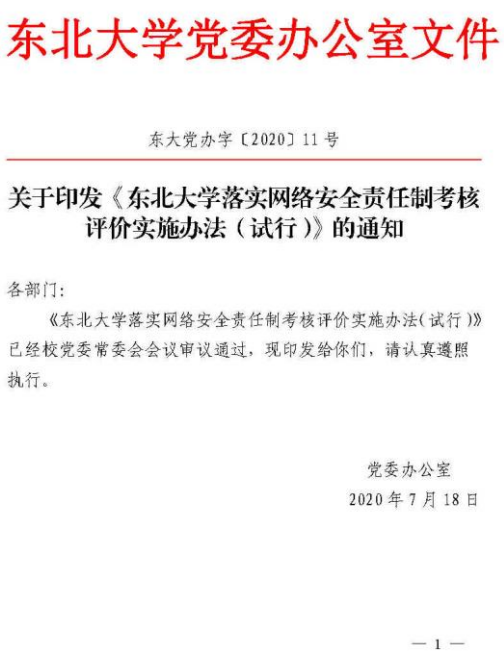
各部门：

《东北大学网络安全管理办法（试行）》已经校党委常委会会议审议通过，现印发给你们，请认真遵照执行。

中共东北大学委员会

2020年7月18日

—1—



东北大学党委办公室文件

东大党办字〔2020〕11号

关于印发《东北大学落实网络安全责任制考核评价实施办法（试行）》的通知

各部门：

《东北大学落实网络安全责任制考核评价实施办法（试行）》已经校党委常委会会议审议通过，现印发给你们，请认真遵照执行。

党委办公室

2020年7月18日

— 1 —

东 北 大 学 文 件

东大校字〔2020〕67号

关于印发《东北大学信息化项目建设管理办法（试行）》的通知

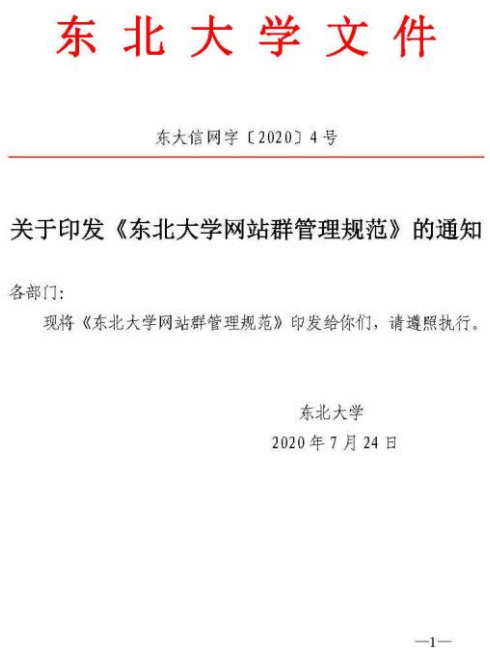
各部门：

《东北大学信息化项目建设管理办法（试行）》已经2020年第十四次校长办公会议审议通过。现印发给你们，请遵照执行。

东北大学

2020年7月17日

—1—



东 北 大 学 文 件

东大信网字〔2020〕4号

关于印发《东北大学网站群管理规范》的通知

各部门：

现将《东北大学网站群管理规范》印发给你们，请遵照执行。

东北大学

2020年7月24日

—1—

信息化建设和网络安全工作阶段性成果

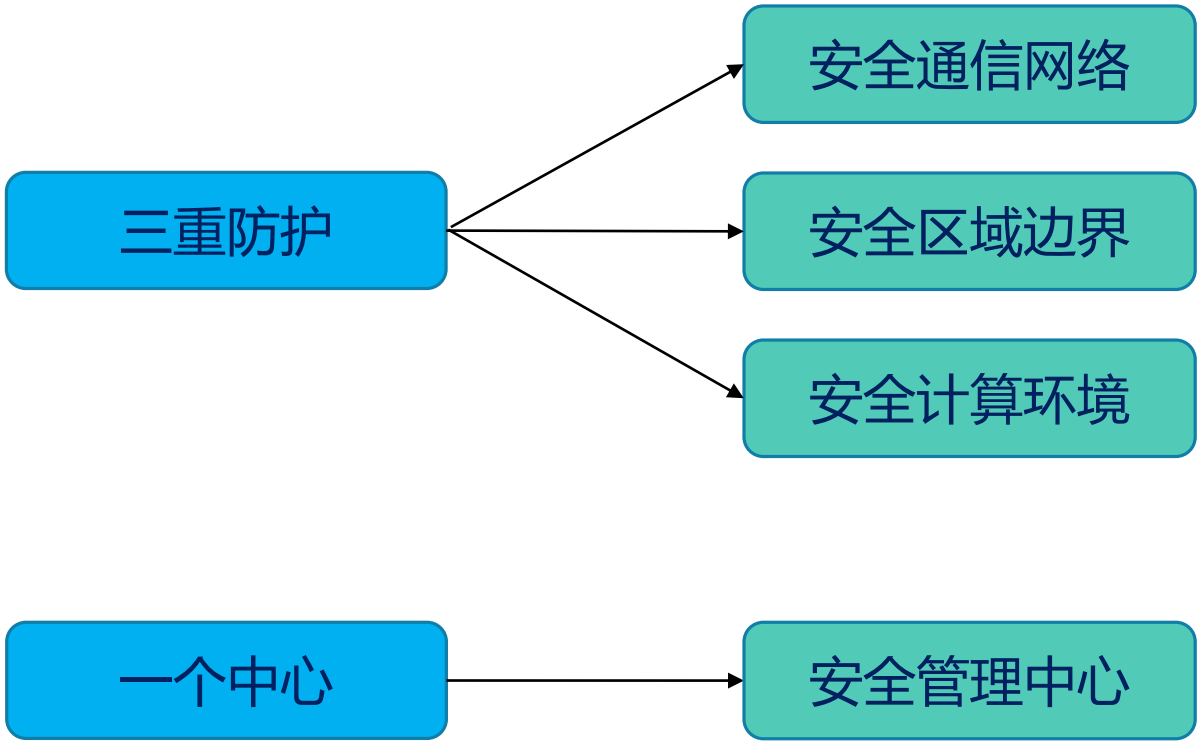
- “网络安全和信息化是一体之两翼、驱动之双轮”
  - “软硬”兼施：主动提供技术支撑，强化网络安全管理，整体推动统筹进程。
  - 稳步推进：制度保障、统筹管理、协调推进的信息化建设和网络安全工作。

统筹建设、集中管控，对学校校园网络网络安全防护体系和能力提出更高要求。

日常时期和重要时期网络安全保障需求

日常时期和重要时期网络安全保障需求

- 网络安全等级保护2.0要求



网络结构、网络带宽、网络传输、可信验证

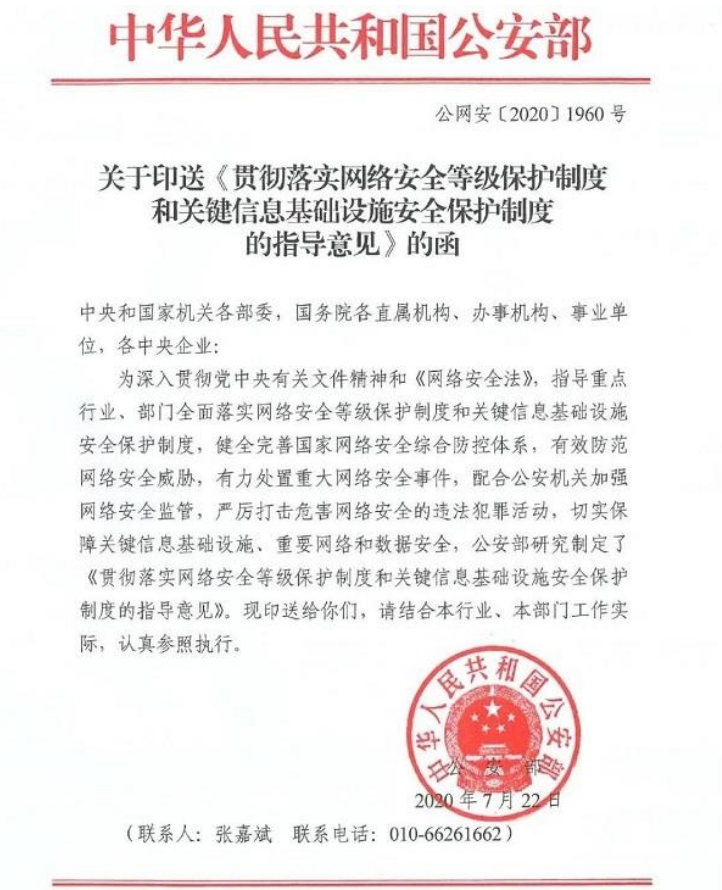
边界防护、访问控制、入侵防范、安全审计、恶意代码防范、可信验证

身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证；数据完整性、保密性、数据备份恢复、个人信息保护等

安全管理、系统管理、安全审计、集中管控

日常时期和重要时期网络安全保障需求

- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》
  - 新目标：构建国家网络安全综合防控体系
  - 新理念：实战化、体系化、常态化
  - 新举措：动态防御、主动防御、纵深防御、精准防御、整体防控、联防联控
  - 新高度：国家网络安全综合防御能力和水平上升一个新高度



中华人民共和国公安部

公网安〔2020〕1960号

关于印送《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的函

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各中央企业：

为深入贯彻党中央有关文件精神和《网络安全法》，指导重点行业、部门全面落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，配合公安机关加强网络安全监管，严厉打击危害网络安全的违法犯罪活动，切实保障关键信息基础设施、重要网络和数据安全，公安部研究制定了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》。现印送给你们，请结合本行业、本部门工作实际，认真参照执行。

2020年7月22日

（联系人：张嘉斌　联系电话：010-66261662）

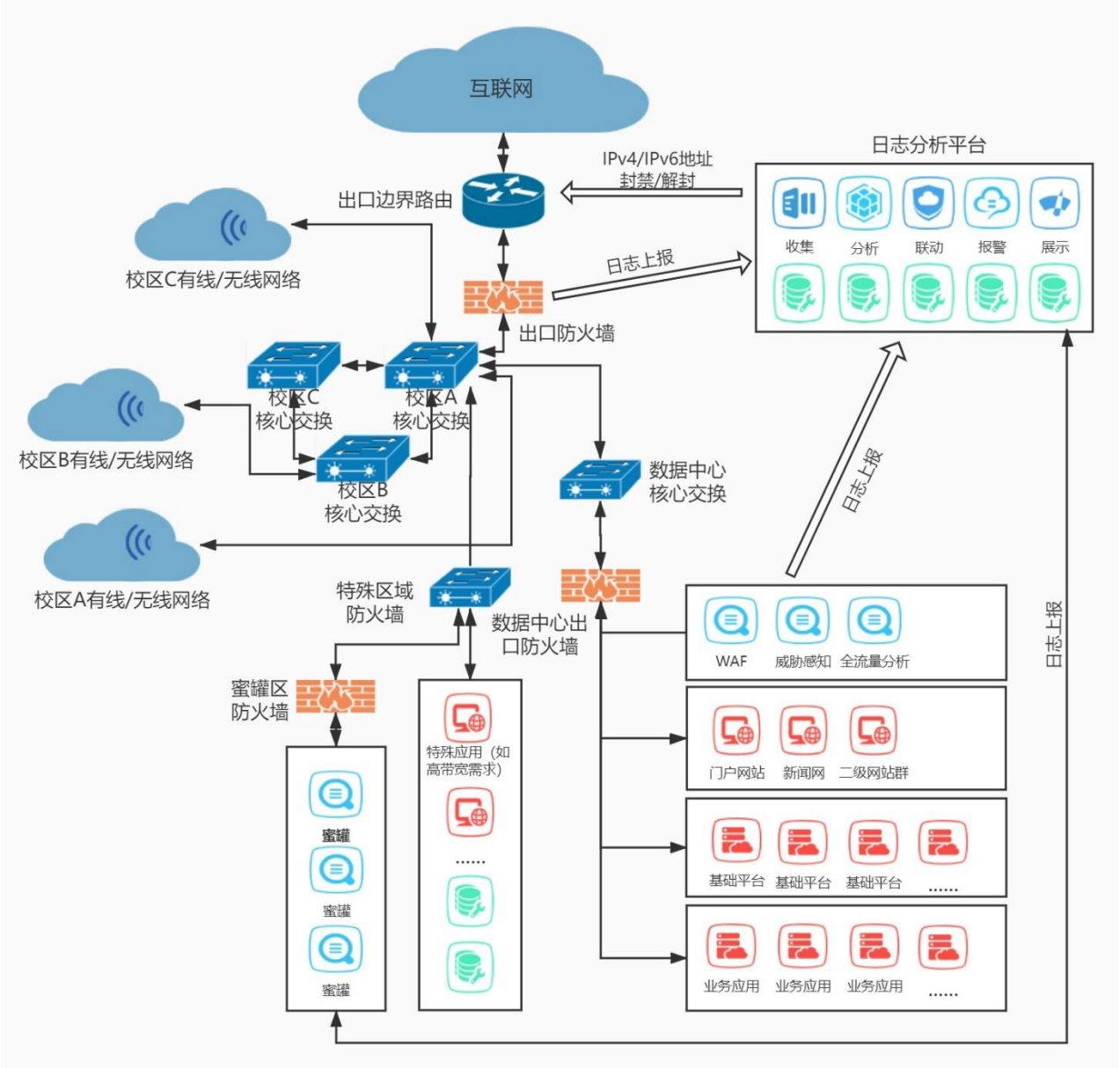
日常时期和重要时期网络安全保障需求

- 日常时期网络安全保障需求
  - 合理化部署网络安全防护手段
  - 层次化开展安全威胁信息收集
  - 效率化分析研判网络安全威胁
  - 制式化实践网络安全威胁阻断
  - 柔性化保障信息服务稳定运行

日常时期和重要时期网络安全保障需求

- 重要时期网络安全保障需求
  - 在网络安全重要保障时期、攻防演练期间等重要时期，网络安全保障要求将有明显提高，特别是攻防演练期间有针对性的网络安全威胁会显著增加，为保障网络安全合规和满足政策要求，需要在日常时期安全防护要求基础上，进一步提升网络安全保障要求。
    - 适度优先保证网络安全保障水平，降低信息服务便捷水平。
    - 尽可能提高安全威胁监测范围和内容，尽量避免漏报。
    - 组织团队值守和研判安全威胁，尽早处置响应疑似安全威胁。
    - 组织团队及时溯源疑似安全威胁，主动开展安全防护措施。
    - 及时准备应急响应处置流程和预案，发生疑似安全事件及时研判、处置和上报，并最小化影响范围。

校园网络威胁监测与处置体系规划与实践

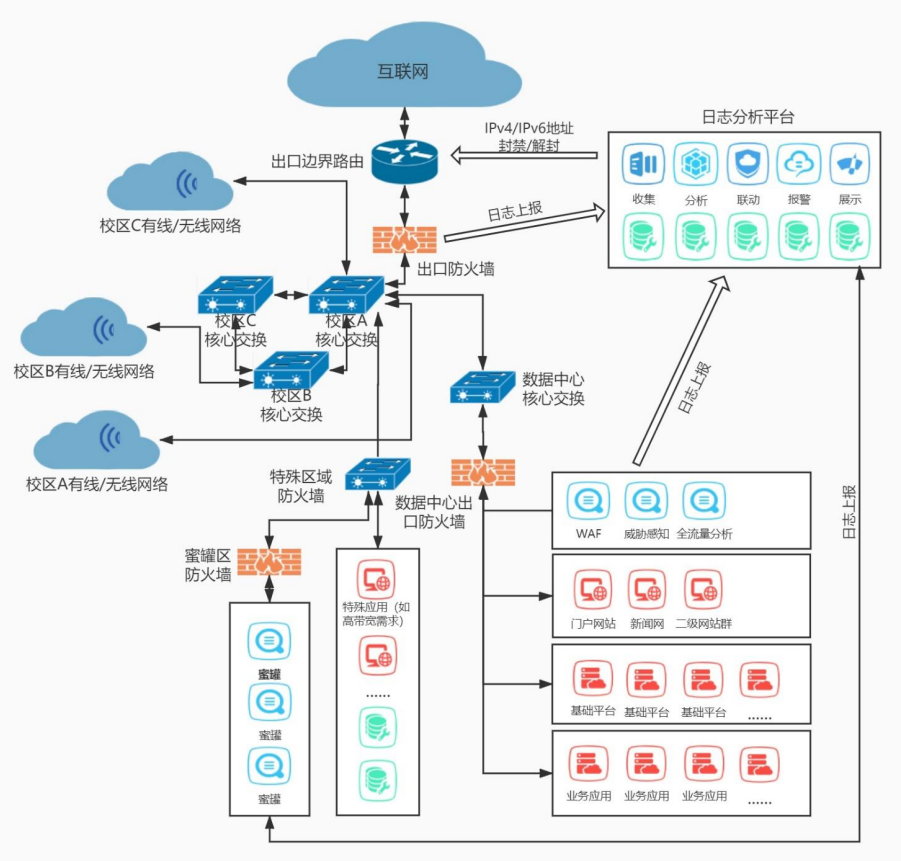

互联网
IPv4/IPv6地址
封禁/解封
日志分析平台
出口边界路由
收集
分析
联动
报警
展示
校区C有线/无线网络
日志上报
出口防火墙
校区C
核心交换
校区A
核心交换
校区B有线/无线网络
校区B
核心交换
数据中心
核心交换
日志上报
校区A有线/无线网络
特殊区域
防火墙
数据中心出
口防火墙
WAF
威胁感知
全流量分析
蜜罐区
防火墙
特殊应用（如
高带宽需求）
门户网站
新闻网
二级网站群
蜜罐
蜜罐
蜜罐
.....
基础平台
基础平台
基础平台
.....
业务应用
业务应用
业务应用
.....
日志上报

校园网络威胁监测与处置体系规划与实践

- 校园网络威胁监测与处置体系
  - 校园网络具有多校区统一互联网出口、环形多校区主干网络、服务集中运行于数据中心等特征。
  - 通过**全网部署IPv4/IPv6双栈网络设备、合理部署网络安全相关设备、集中搭建日志分析平台、主动**采用添加“**黑洞路由**”封禁和删除“黑洞路由”解封威胁相关IPv4/IPv6地址等方式实现对校园网络相关安全威胁的全方面监测、分析、预警和高效阻断、处置；
  - 同时在分析研判安全威胁时先根据日志来源进行初筛，之后**根据日志来源不同和当前安全态势水平（日常或重要）**对具体安全威胁设置不同的权重，**研判是否进行阻断或阻断时间**，在力争保障网络安全的同时降低对正常应用服务的影响。

校园网络威胁监测与处置体系规划与实践

- 校园网络威胁监测与处置体系
  - 部署IPv4/IPv6双栈
  - 按等保等级分区
  - 多渠道监测
  - 分层次分析
  - 高效率处置
  - 偏柔性恢复
  - 重持续防护



校园网络威胁监测与处置体系规划与实践

- 校园网络威胁监测与处置体系
  - 常态化获取高质量的安全威胁情报，及时进行阻断（时长自动设置和手工设置，根据威胁评价阻断时间1~15 天，重要时期阻断时间上限会增加到30 天。

一周内阻断IPv4、IPv6地址数量情况

类型	周一	周二	周三	周四	周五	周六	周日
IPv4	145	125	142	124	249	119	154
IPv6	13	5	8	9	7	9	21

校园网络威胁监测与处置体系规划与实践

- 后续持续改进和提升
  - 在提高日志分析研判准确度上，应该在记录误报情况的基础上，增加对准确度的评价，以改进分析研判机制提高准确度；
  - 在保障网络安全防护水平基础上，增加其他有效的威胁阻断机制，提供必要的信息提示和投诉渠道给被误报的源地址用户，持续改善机制柔性处理水平；
  - 此外改进简单加权累加后比对阈值的威胁水平判断机制，建立必要的威胁水平模型，提高监测与处置体系的科学性和可验证性，逐步摆脱基于运维人员经验人为设置安全威胁水平带来的准确性偏离。

结束语

结束语

- 网络安全工作涉及学校网络和信息化规划、建设、运维等各个方面；
- 网络安全人才来自学校网络建设与运维、系统设计与开发、服务部署与运维等各条“战线”；
- 网络安全能力来源于理论学习、动手实践（攻防演练、CTF……）、沟通交流；
- 网络安全工作的成绩体现在服务师生，保障服务质量和数据安全，减少网络安全事件发生。

致谢

- 感谢东北大学信息化建设与网络安全办公室网络、信息化和安全管理、运维一线的各位同事！
- 感谢兄弟高校同仁们和众多网络安全领域领先厂商在各渠道的信息分享和深入交流！
- 感谢教育系统网络安全保障专业人员（ECSP）培训课程。
- 做好大家理念、技术和经验的收集者和搬运工，希望此次分享能对各位同仁做好网络安全相关工作有所帮助。

教育网络信息安全

感谢聆听，多多交流

变化是永恒的！

网络安全工作永远在路上...

自我介绍

王宇

东北大学信息化建设与网络安全办公室

目前主要参与东北大学网络安全体系建设与日常管理

电子邮件：wangy@mail.neu.edu.cn

QQ：10662877

微信：wangyuneu

个人主页：http://faculty.neu.edu.cn/wangy/

办公电话：024-83687240-8002