

年龄：24

联系电话：15093344287

邮箱：zyh183160@163.com

地址：河南省郑州市

政治面貌：共青团员

Github：sutaon

周宇航



教育经历

郑州大学 网络空间安全·统招硕士

2024/09 - 2027/06

- 主修课程：高级网络安全技术、计算系统安全、软件安全、高级计算机网络、网络安全等
- GPA:3.85/5 平均成绩:84.70，连续两年获得郑州大学校级奖学金

河南理工大学 数据科学与大数据技术·统招本科

2020/09 - 2024/06

- 主修课程：数据结构、数据库系统、计算机网络、操作系统、Linux原理与应用、Java程序设计、数据爬取、机器学习、分布式数据库、Python数据分析、线性代数、多元统计分析等
- 专业排名前20%，GPA:3.34/5 平均成绩:83.35，河南理工大学优秀学生通讯员，CET4

工作经验

奇安信安全技术(南京)有限公司 安全实习生 安全服务BG

2026/06 - 2026/09

- 安全技能实训**：系统学习资产指纹识别、端口/目录扫描、漏洞验证及报告编写与复测流程；熟练使用 Nmap、Nuclei 进行资产探测，通过 Burp Suite、sqlmap 验证 SQL 注入、XSS、文件上传、未授权访问及 RCE 等 Web 漏洞，结合 Wireshark 复核 HTTP/TCP 流量，并使用 Python/Shell 编写批量探测脚本及简易 PoC。
- 驻场安全运营(豫信电科)**：依托"一道墙"及天眼平台，对 35 个统建政务系统开展告警值守，按业务/资产组筛选融合告警与多源关联告警，结合源/目的 IP、请求/响应体及访问链进行研判；发现并通报弱口令、SpringBoot 未授权访问、Swagger 敏感信息泄露等高危漏洞，跟踪修复闭环并提交攻击 IP 封禁；协助第三方公司对多个政府上线项目开展"两高一弱"账号和密码资源池排查及安全设备等保密评工作。
- 运营成果**：累计监测恶意攻击告警 44,108 条（日均约 2,005 条，峰值 3,956 条/日），持续输出安全运行日报，维护 8 个项目/平台共 28 项安全问题记录，覆盖 11 类风险类型，有效保障政务资产安全。

北京剑鱼信息技术有限公司河南分公司 爬虫开发工程师 数据研发部

2025/06 - 2025/09

- 系统设计与自动化采集脚本开发**：主导招投标与政府采购信息采集系统开发与迭代，面向全国各级公共资源交易及政府采购站点，完成页面结构分析与动态加载机制识别，抽象统一的 XPath/CSS/正则解析规则，实现核心字段结构化抽取与标准化映射；基于 Python 融合 Requests、BeautifulSoup 与 Selenium 实现动静态分层采集，落地多线程并发、分布式去重、智能重试、频率调控及全链路日志监控与入库校验流程。
- 运营成果**：日均上线迭代爬虫任务 50+，采集成功率稳定在 96% 以上；通过架构与流程优化提升系统并发能力与运行稳定性，替代人工检索与录入模式，有效缩减人力成本。

百度贴吧 垂类内容运营 校园组

2022/05 - 2022/08

- 实习内容**：负责百度贴吧校园垂类内容运营，细分校园板块内容赛道；开展日常内容巡检，按规范处置违规信息，联动高校吧主维护社区秩序；策划校园主题活动，联动同类院校开展联名活动；挖掘推荐优质 UGC 内容，统计运营指标并输出周度复盘；协助开展吧主管理、规则宣导等事务。
- 运营成果**：累计处置违规内容 100 余条；落地 2 场校园主题活动及院校联名活动，累计评论超 1500 次，板块热度稳居同类院校前列，日均互动量提升 35%；挖掘推荐优质内容 10 余篇。

项目经历

Agentic SOC Assistant | AI 安全运营自动化助手 负责人

2026/06 - 至今

[sutaon/agentic-soc-assistant](#)

- 项目概述**：Agentic SOC 智能告警研判系统 (v0.3.0) 面向政企与 SOC 安全运营场景打造，基于 LangGraph 构建 Agentic 告警研判工作流，将告警标准化、调查规划、受限工具调用、RAG 证据检索、风险判定、人工审批及报告生成串联为可测试、可追溯的状态化流程，同时提供 CLI、MCP stdio、FastAPI 与 Docker 等多形态运行入口。

- **技术栈**：以 Python 3.11/3.12 为开发基础，核心采用 LangGraph、MCP 1.x、Pydantic v2、FastAPI 搭建研判服务内核，配套 Pytest、Ruff、Docker Compose、GitHub Actions 实现工程化测试与 CI 持续交付；预留本地 OpenAI-compatible 模型、Elasticsearch、OpenTelemetry 等扩展接口，支持检索、观测与推理能力的平滑升级。
- **核心功能**：通过 MCP Server 开放资产查询、漏洞情报、已知漏洞检索、日志检索、SOP 检索五类只读安全工具，以 Schema 白名单、重试机制约束 Agent 调用行为，全程留存工具执行 ID 与脱敏查询指纹；实现 CISA KEV 公开情报安全同步与可审计离线快照管理，内置情报过期检测机制；设计 EvidenceGate 证据门禁，将研判结论与证据 ID 强绑定，通过多源日志关联、实体事件校验精准区分攻击确认、证据不足与误判场景，对高风险处置动作保留人工审批门槛，同时支持规则引擎与本地大模型双模式降级切换。
- **项目成效**：已覆盖 7 个基准研判场景，包含基础回归场景与真实公开情报典型路径；在基准测试集中，检索召回、工具调用、引用有效性、结论准确性及情报溯源等核心指标全部达标，无事实偏离问题；通过 45 项单元测试与多环境 CI 门禁验证，整套研判工作流实现可运行、可追溯、可评估与容器化部署。

河南省数字政府“一道墙”安全支撑平台告警监测与研判项目

项目成员

2026/07 - 2026/09

- **项目概述**：依托河南省数字政府“一道墙”安全运营支撑平台，面向政务信创云 35 个统建政务信息系统开展常态化安全运营，覆盖流量攻击检测、防御验证与告警研判全流程，构建“监测 - 研判 - 处置 - 整改”的安全运营闭环，保障政务系统网络安全稳定运行。
- **技术栈**：融合奇安信天眼、SOC、NDR、WAF/IDS、全流量态势感知等平台能力，采用 WAF/NDR 多源告警关联、全流量回溯、漏洞利用链分析、攻击成功性验证、协议行为分析、误报归因与白名单策略等技术，构建完整攻击证据链，支撑精准风险研判。
- **核心功能**：覆盖漏洞扫描、弱口令爆破、未授权访问、Web 注入、命令执行、WebShell 通信、异常外联等攻击场景；可精准区分真实攻击、漏洞暴露、已阻断攻击、平台误报、扫描仿真流量与正常业务访问，输出风险通报、封禁加白、整改复测等标准化处置建议，配套漏洞闭环管理与检测规则迭代优化能力。
- **项目成效**：日均监测处置恶意攻击告警 2,005 条，通过标准化研判流程与告警分级机制，大幅降低误报漏报与人工复核成本；缩短风险响应时长与漏洞暴露窗口，保障省级平台重大活动期间零重大安全事故，推动漏洞全链路闭环落地，为数字政府安全体系建设提供数据化决策支撑。

流量攻击告警自动研判 Skill

创作者

2026/07 - 至今

sutaon/triaging-traffic-attack-alerts

- **项目概述**：面向政务服务平台及政企安全运营中心，设计适配一道墙、天眼、SOC/WAF/NDR 等多类安全平台的流量攻击告警智能研判 Skill，将零散孤立的告警转化为覆盖攻击意图识别、漏洞可利用性评估、成功证据验证、业务合法性检查、影响定级、通报决策的结构化研判流程，辅助一线安全人员高效开展高频告警初筛与复核工作。
- **技术栈**：基于 Codex Skill 框架进行开发，采用 Python、JSON、Markdown/YAML 实现研判规则与逻辑编排；融合 HTTP/WAF 日志分析、应用与数据库审计、EDR 主机日志、OOB 回连验证等技术手段，对接 CISA KEV、FIRST EPSS、NVD CVE API 实时漏洞情报，依托 GitHub Actions 实现工程化迭代与能力落地。
- **核心功能**：搭建四级攻击判定体系，结合请求响应、多源日志、资产暴露面、历史处置记录等维度形成完整证据链，全面覆盖弱口令、未授权访问、注入攻击、WebShell、组件暴露及扫描器仿真流量等攻击场景；接入实时漏洞情报评估处置优先级，严格区分通用漏洞评级与本地实际利用结果，自动输出分类研判结论及配套证据、处置口径与修复建议。
- **项目成效**：经脱敏历史告警样本回放验证，辅助研判准确率达 90% 以上，可稳定区分攻击成功、误报、扫描探测等多类场景；落地政企告警初筛场景后统一通报标准，有效降低孤立字段判定导致的误通报，同时优化扫描器告警处置逻辑，精准识别资产暴露风险；经高危漏洞场景演练可实现攻击结果精确分级，支持重复告警聚合提升复盘效率；核心 Skill 体量缩减 56% 并拆分为按需加载模块，触发效率与可扩展性显著提升。

基于Hive的烟草管控系统分布式存储平台设计

核心开发者

2024/01 - 2024/06

- **项目概述**：面向烟草零售登记与专卖监管需求，主导研发基于 Hadoop/Hive 的扫码登记与监管分析原型平台，打通数据采集、分布式入仓、查询分析与可视化全流程，为商品流向追溯和监管决策提供数据支撑。
- **技术栈**：以 Hadoop 2.9.2 为底层架构，依托 HDFS、Hive 3.1.2 构建分布式存储与数仓能力；使用 Python 实现二维码解析、数据校验与入仓调度，结合 PHP、前端可视化组件及 VMware 集群环境完成全栈落地。
- **核心功能**：主搭建 1 主 2 从 Hadoop 集群，按零售商维度规划 HDFS 目录与 Hive 表结构；构建图片上传、二维码解析、SHA-256 去重、WebHDFS 上传、Hive 入仓的自动化数据链路；实现扫码明细查询、多维度统计看板与用户角色

分流功能。

- **项目成效：**完成端到端原型验证，验证了 Hadoop 方案在烟草监管场景的落地可行性；通过摘要校验拦截重复扫码记录，保障数据一致性；形成零售登记、监管分析的业务闭环，为后续功能扩展奠定技术基础，且实现论文支撑。

个人博客搭建与美化

核心开发者

2023/12 - 至今

haveyouself.fun

- **项目概述：**独立开发基于 WordPress 的个人博客与会员社交平台，自研响应式主题与会员业务插件，整合内容创作、会员体系、社交互动与项目展示模块，实现三级权限体系，已部署至阿里云 Linux 服务器稳定运行。
- **技术栈：**基于 WordPress 与 PHP 扩展业务能力，依托 MariaDB 设计自定义业务表与索引优化；采用原生 JavaScript 实现无刷新前端交互，配套响应式布局；完成服务器部署、安全加固与自动化测试体系搭建。
- **核心功能：**基于 WordPress 与 PHP 扩展业务能力，依托 MariaDB 设计自定义业务表与索引优化；采用原生 JavaScript 实现无刷新前端交互，配套响应式布局；完成服务器部署、安全加固与自动化测试体系搭建。
- **项目成效：**完成从主题开发到公网部署的全链路闭环，将单一博客扩展为内容 + 社交一体化平台；优化数据模型保障并发一致性，核心服务运行稳定，建立自动化测试体系支撑功能迭代。

学生成绩预测分析系统

核心开发者

2023/12 - 2024/01

- 基于 Python、pandas、scikit-learn、Matplotlib、Seaborn 和 HTML 前端交互，完成学生成绩预测系统的设计与实现。项目覆盖数据清洗、缺失值填补、一致性校验、独热编码、特征工程和可视化探索等完整流程；构建随机森林、线性回归、SVM 三类模型，并通过交叉验证进行效果对比，选择最优模型后进行序列化保存。系统提供简洁的 HTML 交互界面，支持用户实时输入特征并展示预测结果和多维度可视化报告，提升了成绩预测的可用性和分析效率。

工作以外经历

郑州大学 信安3-6班计算机网络实验课

助教

2026/03 - 2026/06

任本科《计算机网络》实验代课助教，带教 11 个实验：用 Wireshark 完成 IP/TCP/UDP/HTTP 等协议抓包分析，用 Packet Tracer 指导 VLAN 与静态、RIP/OSPF 路由配置，辅导 Socket 编程，负责答疑与报告批改。

河南理工大学 大数据2002班

组织委员

2020/09 - 2024/06

统筹班级与学院各类活动全流程策划、跟进及落地执行；承担班级党支部党费收缴、青年大学习统筹安排等党务工作；牵头组织安全知识宣讲与应急演练，强化安全防范意识，有效提升团队凝聚力与协作能力。

河南理工大学 计算机青年协会

外联部干事

2020/09 - 2022/06

参与组织执行校园大型志愿活动（含电脑维修清理、冬季爱心捐衣等）与校园维洁工作，统筹人员分工与流程安排；参与志愿策划比赛及院校专业纪录片拍摄，具备优秀的活动协调与团队协作能力。

东软集团股份有限公司 数据分析与机器学习实训

小组组长

2023/12 - 2024/02

带领6人小组完成学生成绩预测系统全流程研发，统筹分工与项目推进。基于pandas完成数据清洗与特征工程，采用scikit-learn构建随机森林等模型，交叉验证选型，实现前端录入、实时预测与可视化，主导结项答辩与系统演示。

专业技能

- **网络安全渗透：**会 Nmap、Wireshark 等攻防工具；精通 OWASP Top10 漏洞验证；熟悉 SOC/WAF/ 天眼平台，具备告警研判、攻击链分析与漏洞闭环能力。
- **AI Agent：**熟悉 LangGraph/LangChain 搭建 Agent 工作流；掌握 MCP 工具接入、RAG 检索；可通过 Python 实现安全告警自动化研判落地。
- **后端开发：**熟练 Python，熟悉 FastAPI/Flask；掌握 Linux、Docker、CI/CD；熟练 pandas、scikit-learn 数据建模，熟悉 MySQL 及 Hadoop 架构。

自我评价

具备网络安全、后端开发与数据建模的复合技术能力，擅长安全自动化工具与 AI Agent 工作流的落地实现，做事严谨细致，秉持闭环思维，能快速学习新技术并结合业务场景落地应用，具备良好的团队协作与执行力。日常热爱羽毛球、慢跑与音乐，坚持规律运动，习惯在运动中梳理思路、调节状态，始终以沉稳积极的态度应对工作与生活。