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
- 专业排名前 50%，GPA: 3.85 / 5，连续两年获得校级奖学金

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15%，GPA: 3.34 / 5 平均成绩: 83.35

工作经验

奇安信（郑州）安全技术有限公司 驻场实习生 安全服务BG 2026/06 - 至今

- 在奇安信期间，学习资产指纹识别、端口/目录扫描、漏洞验证、报告编写与复测流程；使用Nmap、nuclei进行探测，通过Burp Suite、sqlmap验证SQL注入、XSS、文件上传、未授权访问和RCE等Web风险，使用Wireshark复核HTTP/TCP流量，并学习用Python/Shell整理批量探测结果和简单PoC。
- 随后被派驻至豫信电科，使用“一道墙”和天眼对35个统建政务信息系统进行告警值守。按业务及资产组筛选融合告警和多源关联告警，核对XFF、源/目的IP、请求体、响应体、状态码及前后访问记录等；依据登录结果、未认证端点回显和上传文件后续访问，成功通报项目组并跟踪修复弱口令，SpringBoot未授权访问，Swagger敏感信息泄露漏洞，ElasticSearch未授权访问等高危风险漏洞，确认风险后提交攻击IP封禁。
- 实习期间，值守范围累计监测44,108条恶意攻击告警，日均约2,005条、单日峰值3,956条；持续输出安全运行日报，维护8个项目/平台的28项安全问题记录，覆盖11类风险，及时防止政府资产受损。

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

- 主导招投标与政府采购信息数据采集系统的开发与迭代。面向全国各级公共资源交易、政府采购类站点开展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，完成公告标题、项目编号、采购单位、中标单位、中标金额、发布时间、公告类型等核心字段的结构化抽取与标准化映射，搭建可复用的字段解析规则体系。
- 基于 Python 技术栈，融合 Requests、BeautifulSoup 与 Selenium 实现动静态页面分层采集，针对性适配各类反爬策略；落地多线程并发采集、分布式 URL 去重、智能异常重试、请求频率动态调控等机制，配套全链路日志监控、数据清洗与入库校验流程，数据统一存储。
- 任职期间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强化系统并发能力与运行稳定性，降低采集中断率，替代人工检索与录入模式，有效缩减人力成本。

项目经历

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。

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 - 至今

- **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。

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、pgvector、Elasticsearch、OpenTelemetry、Langfuse 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。

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。

政府采购信息爬虫智能体 核心开发者 2025/07 - 2026/01

- 基于 Python、Requests/Scrapy、BeautifulSoup、Selenium、SQLite/JSON/MySQL 和扣子平台，开发政府采购信息智能采集 Agent，面向招投标公告、政府采购公告和中标结果页面，自动完成目标 URL 解析、页面结构识别、字段抽取、数据清洗和结构化存储。
- 实现增量抓取、URL 去重、异常重试、日志监控、结果持久化和导出查询能力，支持抽取项目编号、采购单位、中标单位、中标金额、发布时间、公告类型等核心字段；通过规则化解析与交互式采集流程降低人工检索和复制成本，提升采购情报收集效率与数据一致性。

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。

抖音用户浏览行为数据分析与挖掘 核心开发者 2023/02 - 2023/07

- 基于 Python、pandas、pyecharts 和 scikit-learn，完成海量浏览行为数据的采集、清洗、特征工程及训练/测试集构建。项目采用K-means 实现用户分群，并构建二分类模型预测关键行为，结合交互式 pyecharts 可视化大屏输出分析结果与模型评估报告，为业务决策提供数据支撑。

工作以外经历

河南理工大学丨大数据2002班 组织委员 2020/09 - 2024/06

负责班级与学院活动全流程策划跟进与执行，负责班级党支部党费催收，青年大学习安排等任务，组织安全知识宣讲与应急演练，提升团队凝聚力

计算机青年协会 外联部干事 2020/09 - 2022/06

参与校园大型志愿（电脑维修和清理，冬季志愿捐衣等）与维洁活动的组织与执行，负责人员安排与流程分配；参与志愿活动策划比赛与学校院校专业纪录片拍摄任务，具备活动协调与团队协作能力

河南理工大学贴吧 副吧务 2021/06 - 2022/06

负责社区内容审核、违规信息处理与互动氛围维护，保障线上交流环境积极健康，提升社区信息传播质量与讨论秩序

东软集团股份有限公司丨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，统筹任务分工与项目推进。基于 pandas 完成数据清洗、缺失值填补、一致性校验与特征工程，采用 scikit-learn 构建随机森林、线性回归、SVM 三类模型，通过交叉验证完成模型选型与序列化。实现前端特征录入、实时预测与多维可视化报告，主导结项答辩与系统功能演示

专业证书

CET4

专业技能

- **安全攻防与运营**：熟练使用一道墙、奇安信天眼、SOC、NDR、全流量态势感知等安全运营平台；可围绕源目 IP、XFF、访问流向、Payload、响应状态与资产上下文构建完整证据链，精准区分误报、攻击尝试与漏洞利用事件；掌握 SQL 注入、XSS、SSRF、文件上传、命令执行、未授权访问、弱口令等常见 Web 风险的验证与处置流程，熟悉 OWASP Top 10 与 MITRE ATT&CK 攻防框架。
- **安全自动化与 AI 应用**：具备 Agentic SOC 落地实践经验，可基于 LangGraph/LangChain、MCP、RAG 与工具调用机制，设计带审批门禁的安全运营自动化工作流，实现告警核查、日志检索、SOP 匹配与研判报告生成的标准化、自动化处理。
- **后端与全栈开发**：熟练使用 Python、Requests、BeautifulSoup、Scrapy、Selenium、pandas、scikit-learn 等工具库，可独立完成数据采集清洗、结构化解析、任务调度、异常重试与自动化脚本开发；掌握 FastAPI/Flask 框架，可完成 RESTful 接口开发与 Webhook 服务接入；熟悉 PHP 语言与 WordPress 二次开发，具备自定义主题、插件开发与全栈项目交付能力。
- **数据存储与数仓能力**：熟练使用 MySQL、SQLite 进行表结构设计、索引优化与事务开发；具备 Hadoop 集群部署、HDFS 分布式存储、Hive 数仓建模、离线统计与可视化查询的完整项目经验。
- **工程化与运维部署**：熟悉 Linux 系统操作与 Apache 服务配置，可独立完成环境搭建、接口联调、日志排查、服务监控与日常运维；掌握 Git 版本控制、Docker 容器化、VMware 虚拟化与网络配置，能够快速搭建各类开发测试环境。

自我评价

性格开朗大方，处事沉稳不内耗，热爱羽毛球、慢跑与音乐。工作中踏实严谨，学习能力强，乐于钻研技术，具备良好的团队协作意识与执行力。