陈子昂 | 高级网络安全工程师 | 渗透测试与安全运营

中国,北京市,北京,北京市海淀区中关村南大街 5 号,100081
+86 138 1234 5678 • chen.ziang@securemail.cn • https://www.chenziang.dev
@chenziang-sec • @chenziang-sec • 知乎 @chenziang-sec

简介

资深网络安全工程师,拥有多年金融与互联网行业安全建设经验,擅长渗透测试、安全运营、云原生安全与零信任架构落地。

- 主导多家大型企业红蓝对抗、攻防演练与应急响应,累计发现并修复高危漏洞 200+ 个
- 熟悉等保 2.0、ISO 27001、GDPR 等合规要求,具备从 0 到 1 搭建安全管理体系的经验
- 熟练使用 Python、Go、Bash 编写安全工具,推动安全左移与 DevSecOps 流程建设
- 持有 CISSP、OSCP、CISP 等专业认证,具备良好的跨团队沟通与项目管理能力

教育背景

北京邮电大学 **https://www.bupt.edu.cn**

硕士,网络空间安全,成绩:3.8/4.0 2016 年 9 月–2019 年 6 月

- 研究方向为云原生安全与威胁检测,参与国家级网络安全重点实验室项目
- 发表 2 篇安全领域学术论文,获校级优秀研究生称号
- 担任信息安全竞赛战队队长,带队进入全国总决赛

课程:密码学与安全协议、网络攻防技术、操作系统安全、数据库安全、云安全与虚拟化、安全编程与代码审计

南京邮电大学 **https://www.njupt.edu.cn**

学士,信息安全,成绩:3.7/4.0 2012 年 9 月–2016 年 6 月

- 系统学习信息安全基础理论,完成网络攻防、密码学与系统安全等核心课程
- 参与校信息安全协会,组织校内 CTF 培训与安全沙龙

课程:计算机网络、信息安全导论、密码学基础、操作系统、数据结构与算法、Web 安全

工作经历

云盾网络安全科技有限公司 **https://www.yundunsec.com**

高级网络安全工程师 2023 年 7 月至今

- 负责金融云平台安全架构设计与落地,覆盖 IAM、数据加密、网络隔离与零信任接入
- 主导红蓝对抗与攻防演练,优化检测规则 300+ 条,将高危事件平均响应时间缩短 45%
- 推动 DevSecOps 建设,将 SAST、DAST、SCA 集成至 CI/CD 流水线,上线前漏洞修复率提升至 95%
- 建立安全运营中心(SOC)指标体系,定期输出威胁情报与风险报告,支撑管理层决策
- 指导 5 人安全团队,制定培训与演练计划,提升团队渗透测试与应急响应能力

关键字:零信任、云安全、红蓝对抗、DevSecOps、安全运营、应急响应

星河支付科技有限公司 **https://www.xinghepay.com**

安全运营工程师 2022 年 1 月–2023 年 6 月

- 负责支付业务安全监控与事件响应,日均处理安全告警 2000+ 条,误报率降低 30%
- 搭建基于 ELK 与 Suricata 的日志分析平台,实现异常登录、暴力破解与数据泄露场景的实时检测
- 参与等保 2.0 三级测评与整改,完成 60+ 项安全控制措施落地,顺利通过外部审计
- 编写 Python 自动化脚本,实现漏洞扫描、资产梳理与报告生成,节省每周 10 小时人工成本
- 组织季度安全意识培训与钓鱼演练,员工安全事件上报率提升 2 倍

关键字:SIEM、等保 2.0、ELK、Python、威胁检测、安全意识

北辰云计算有限公司 **https://www.beichencloud.com**

渗透测试工程师 2019 年 7 月–2021 年 12 月

- 负责 Web、移动 App 与 API 渗透测试，累计完成 120+ 个项目，发现高危漏洞 200+ 个
- 编写渗透测试报告与修复建议，协助研发团队完成漏洞复现、修复验证与回归测试
- 建设内部漏洞知识库与测试用例库，推动安全测试标准化，提升团队交付效率 25%
- 参与客户红队评估与社工演练，模拟 APT 攻击路径，帮助客户完善边界防护与检测能力

关键字：渗透测试、OWASP Top 10、Burp Suite、Metasploit、API 安全、红队评估

语言

中文：母语或双语水平　　**关键字**：普通话二级甲等

英语：完全专业水平　　**关键字**：CET-6、TOEIC 900、技术文档写作

专业技能

渗透测试与红队评估：专家　　**关键字**：Burp Suite、Metasploit、Nmap、OWASP Top 10、社会工程学

安全运营与事件响应：高级　　**关键字**：SIEM、Splunk、ELK、威胁情报、应急响应

云原生与基础设施安全：高级　　**关键字**：Kubernetes、Docker、容器安全、微隔离、零信任

安全开发与自动化：高级　　**关键字**：Python、Go、Bash、DevSecOps、代码审计

合规与风险管理：中级　　**关键字**：等保 2.0、ISO 27001、GDPR、风险评估、安全审计

荣誉

年度优秀安全工程师

云盾网络安全科技有限公司　　2024 年 12 月

表彰在云平台零信任安全架构落地与红蓝对抗演练中的突出贡献，推动高危事件响应效率提升 45%。

全国网络安全挑战赛二等奖

中国网络安全挑战赛组委会　　2018 年 11 月

作为战队核心成员参与 Web 安全与逆向工程赛项，在 300 余支队伍中进入全国前十。

证书

CISSP 国际注册信息系统安全专家　　**https://www.isc2.org**

ISC2　　2021 年 6 月

OSCP 认证渗透测试专家　　**https://www.offsec.com**

Offensive Security　　2020 年 3 月

CISP 注册信息安全专业人员　　**https://www.cisp.cn**

中国信息安全测评中心　　2020 年 9 月

出版刊物

《网络安全技术与应用》　　**https://www.cnki.net**

基于零信任架构的企业云原生安全实践　　2023 年 5 月

- 分析传统边界安全模型在云原生环境下面临的挑战
- 提出融合身份认证、微隔离与持续风险评估的零信任落地框架
- 结合金融行业案例验证方案在降低横向移动风险方面的效果

《信息安全研究》　　**https://www.cnki.net**

面向 API 资产的安全测试与风险治理方法　　2021 年 10 月

- 梳理 API 资产发现、权限校验与敏感数据暴露的常见风险
- 设计覆盖设计、开发、测试与运营阶段的 API 安全治理流程
- 给出自动化测试与持续监控的工程实践建议

引荐

李明远 **+86 139 0000 1234**
前技术总监 limingyuan@yundunsec.com
陈子昂在云平台安全架构与红蓝对抗项目中展现出扎实的技术功底和优秀的跨团队协作能力，能够独立负责复杂安全项目并推动落地。

项目

企业零信任访问平台 **https://www.yundunsec.com/projects/zero-trust**
面向多分支企业的统一身份认证与细粒度访问控制平台 2024 年 1 月–2024 年 11 月

- 负责身份代理、策略引擎与风险评分模块的安全设计
- 实现基于设备指纹、用户行为与上下文风险的动态访问控制
- 支撑 5000+ 员工远程办公场景，降低未授权访问风险 60%

关键字：零信任、身份认证、微隔离、风险评分

云原生安全审计系统 **https://www.yundunsec.com/projects/cloud-audit**
面向 Kubernetes 与容器环境的配置审计与运行时检测系统 2023 年 8 月–2023 年 12 月

- 集成 CIS Benchmark 与自定义策略，实现集群配置基线自动化检查
- 基于 eBPF 采集容器运行时行为，检测异常进程、文件与网络活动
- 将审计结果接入 CI/CD 与告警平台，推动 200+ 项配置风险闭环

关键字：Kubernetes、容器安全、eBPF、CIS Benchmark

红蓝对抗演练平台 **https://www.beichencloud.com/projects/red-blue**
支持自动化攻击编排与防御效果评估的攻防演练平台 2021 年 4 月–2021 年 12 月

- 设计攻击剧本编排、目标资产管理与演练复盘模块
- 集成 MITRE ATT&CK 战术图谱，量化检测覆盖与响应能力
- 支撑 10+ 场内部攻防演练，缩短演练环境准备时间 50%

关键字：红蓝对抗、MITRE ATT&CK、攻击编排、安全评估

兴趣爱好

网络安全研究：CTF 竞赛、漏洞挖掘、威胁情报

运动：马拉松、羽毛球、徒步

阅读与写作：技术博客、历史、科幻小说

志愿服务

中国网络安全志愿者联盟 **https://www.cybervolunteer.cn**
安全讲师 2020 年 3 月至今

- 参与社区网络安全公益培训，面向中小企业与高校学生普及安全开发与防护知识
- 编写 Web 安全入门课程与实验手册，累计培训学员 800+ 人次
- 组织漏洞披露与应急响应志愿活动，协助 20+ 家单位完成安全事件处置