熊熙辰 (Xichen Xiong / Seren)

(+86) 13242933626 | g759472683@gmail.com | blog.csdn.net/qq_49714982 | 深圳 / 可赴沪

求职意向

高级 AI 安全研究员 | 35-45K · 16 薪 | 上海

期望在具备攻防安全深度的团队中，将一线渗透测试经验与企业级 AI 落地安全架构能力结合,聚焦 AI 落地安全 / Agent 安全 / 大模型风险评估方向。

专业简介

2 年世界 500 强电子制造企业甲方安全工程师经验,深度参与企业 AI 落地安全体系建设。自主设计并主导落地「AI 吸烟区 2.0」实体隔离企业 AI 落地方案,在等保合规框架下为 100+ 开发者打通 GPT-4 / Claude 等外部大模型的安全使用通道,累计零数据泄露事件。同时具备扎实的一线攻防能力:主导 12 个业务系统深度渗透测试,累计发现 27 个 Critical/High 级别漏洞并 100% 完成修复;自研 Python 安全基线审计系统,实现全资产审计效率提升 60%。CISP 持证,河南金盾信安杯 CTF 二等奖(Web + MISC)。

核心能力

领域	能力
AI 落地安全架构	实体隔离 / 网闸光闸 / DLP / 数据脱敏 / 单向文件摆渡 / 全量审计
AI Agent & Workflow	Hermes Agent 开发 / MCP 协议 / RAG / Skill / 工具调用 / Prompt 工程
AI 风险评估	Prompt 注入检测 / 输出幻觉验证 / 工具调用异常排查 / 提示词审计
渗透测试	OWASP Top 10 全覆盖 / Burp Suite / Nmap / SQLMap / Metasploit
Python 安全开发	自动化扫描 / 漏洞扫描器 / 基线审计 / 工具集成 / FastAPI
合规体系	ISO 27001 / ISO 22301 / 等保 2.0 / 数据出境合规

工作经历

鹏鼎控股 (Avaryholding) — 信息安全工程师(甲方安全团队)

深圳 | 2024.04 – 至今

1. AI 落地安全架构(核心亮点)

自主设计并主导落地公司首个 「AI 吸烟区 2.0」实体隔离企业 AI 落地方案,在保障核心业务系统(OA / 数据库)与外网物理隔离的前提下,为 100+ 开发者打通 GPT-4 / Claude 等外部大模型的安全使用通道。该架构通过等保 2.0 测评及 ISO 27001 双重审计,累计运行 6+ 个月零数据泄露事件,现已被集团 3 个 BU 复用为标杆架构。

2. Web 深度渗透测试

- 主导 12 个业务系统(OA / SCM / HRM 等)深度渗透测试,覆盖 18 类攻击向量(SQLi / XSS / CSRF / SSRF / 文件上传 / 逻辑漏洞)
- 累计发现 11 个 Critical + 16 个 High 漏洞,100% 完成修复闭环
- 建立"漏洞分级 → 修复跟踪 → 复测闭环"流程,将高危漏洞修复周期从 14 天压缩至 7 天

3. Python 安全开发

- 主导企业安全基线审计系统 Python 智能化升级:自动化漏洞扫描 + 风险自动分级 + 修复建议生成
- 内置 120+ 合规规则,全资产审计效率提升 60%
- 整合企业 230+ 资产(8 大类)的风险评估模型,覆盖技术 / 管理 / 流程三个维度

4. 攻防体系建设

- 制定年度渗透测试计划 + 季度复测机制
- 主导 Q4 2024 两次利用事件后的"企业 Web 安全防护升级"专项,发现 32 个风险点全部整改
- Q2 2025 起零利用事件,安全事件响应效率提升 80%

5. ISO 双体系认证

- 参与 ISO 27001(ISMS)+ ISO 22301(BCMS)双体系认证,主导编写 4 份内部安全策略文档
- 公司首次认证即零不符合项通过,获得 2 个千万级国际客户投标资质

关键项目经历

项目一　「AI 吸烟区 2.0」实体隔离企业 AI 落地安全方案

角色: 首席架构师 + 主导实施 | 周期: 2025

项目背景: 公司 100+ 工程师迫切需要使用 GPT-4 / Claude 提升研发效率,但核心业务系统(OA / 核心数据库)严禁直连外网,且等保合规要求数据不出域。传统方案(VPN + 代理网关)在 2024 年两次内部安全审计中被否决。

架构方案 — 自主设计 5 层实体隔离 AI 落地架构:

```
│   └─ 安全代理网关(白名单 API + DLP)      │
├──────────────────────────────────────────┤
│ Layer 2: 物理隔离设备(网闸/光闸)单向文件摆渡 + 审批 │
├──────────────────────────────────────────┤
│ Layer 1: 正式内网生产区(OA / 核心业务)禁止直连吸烟区 │
└──────────────────────────────────────────┘
```

关键技术创新: - 物理隔离: 网闸 / 光闸实现单向文件摆渡,仅允许脱敏数据 / 审核结果通过 - 混合 LLM 编排: AI Agent 编排引擎动态调度外部 GPT-4 + 内部 LLM,按数据敏感度分级 - MCP/Skill/RAG 工具链: IDE 插件 / Agent 工具支持标准 MCP 协议调用,降低开发者接入门槛 - DLP + 脱敏视图: 准生产数据脱敏后用于 AI 调试,真实数据严格不出域 - Dogfooding Agent: 自动化安全扫描 + 误用检测,持续验证 AI 输出安全性

项目成果: - 100+ 开发者安全使用 GPT-4 / Claude,零数据泄露事件(运行 6+ 个月) - 通过等保 2.0 + ISO 27001 双合规审计 - 成为集团标杆架构,被 3 个 BU 复用落地 - 估算每年节省 200+ 工时(开发者 AI 提效)+ 规避 ≥ 500 万潜在数据泄露损失

项目二 企业 Web 安全防护升级专项

角色: 项目负责人 | 周期: 2025.03 – 2025.07

公司 Q4 2024 因 WAF 防护不足发生 2 起利用事件。主导全 12 个对外站点深度渗透测试,覆盖 18 类攻击向量,识别 32 个风险点并制定定向修复方案。同步开发 Python 自动化扫描模块嵌入安全基线审计系统,建立"年度渗透测试 + 季度复测"长效机制。

成果: Q2 2025 起零利用事件,安全事件响应效率提升 80%,方法论被集团采纳为最佳实践。

项目三 ISO 27001 + ISO 22301 双体系认证

角色: 安全模块核心 | 周期: 2024.09 – 2024.12

完成企业 230+ 资产安全分级盘点,组织全员风险评估识别 17 项中高风险(修复率 98%)。在所有安全条款的现场审计中完成答辩,首次认证即零不符合项通过,为公司赢得 2 个千万级国际客户投标资质。

教育背景

郑州科技学院 — 电气工程及其自动化(统招本科) | 2018.09 – 2022.06

证书与奖项

证书/奖项	颁发机构	时间
河南金盾信安杯 CTF 二等奖(Web + MISC)	金盾信安杯组委会	–
CISP 注册信息安全专业人员	中国信息安全测评中心	2024
IELTS 6.5(单项不低于 6.0)	British Council	2023
全国大学生信息安全竞赛 省级三等奖	全国大学生信息安全竞赛组委会	2022

技术栈

AI 安全架构: 实体隔离 / 网闸 / 光闸 / DLP / 数据脱敏 / 单向文件摆渡 / 全量日志审计 / 录屏审计 AI 风险评估: Prompt 注入检测 / 输出幻觉验证 / 工具调用异常排查 / 提示词审计 / RAG 风险评估 Agent 框架: Hermes Agent(深度实践)/ MCP / RAG / Skill / Tool Calling / LangChain(熟悉)/ LlamaIndex(熟悉)/ AutoGen(熟悉) 渗透测试: Burp Suite Pro / Nmap / AWVS / SQLMap / Kali Linux / Metasploit / Cobalt Strike(基础) Web 安全: SQLi / XSS / CSRF / SSRF / 文件上传 / 命令注入 / 逻辑漏洞 / 反序列化(OWASP Top 10) 编程语言: Python(安全自动化 + AI 工具开发 + 脚本)/ Shell / 基础 Go 基础设施: Docker / Kubernetes(基础)/ GPU 集群 / VDI / Nginx / Linux 系统 合规体系: ISO 27001 / ISO 22301 / 等保 2.0 / GDPR(基础) 语言能力: 中文(母语)/ 英语(IELTS 6.5 — 可阅读英文技术文档与国际协作)

附加亮点

- CSDN 技术博客: blog.csdn.net/qq_49714982 — 持续输出渗透测试与 AI 安全实践文章
- 甲方视角: 区别于乙方渗透测试工程师,具备完整的漏洞发现 → 修复 → 复测闭环落地能力
- AI Native: 深度使用 Hermes Agent 完成日常安全工作,具备 AI Native 工作流构建能力
- 国际化: IELTS 6.5 英语能力,可与国际团队直接协作(集团内部多个国际客户对接经验)

求职信(Cover Letter)与面试高频问题清单,可按需生成。