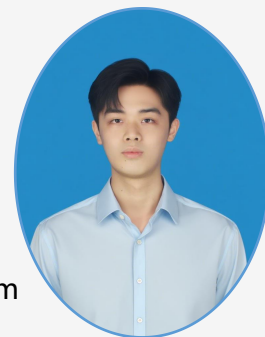


姓名：张天威 个人博客：<https://www.ztwresume.bond>



25 岁

广东省深圳市

13064278098

zhangtianweiismj@163.com

教育背景

2019.09-2023.07

北部湾大学

计算机科学与技术（全日制本科）

工作经历

2023.03-2024.12

上海天机科技股份有限公司

网络安全运维

- 服务对象主要为政府、学校、商场等大型客户，主导完成 20+ 个项目的交付工作，涵盖网络搭建、安全防护及数据容灾等领域，提供贴合客户需求的解决方案
- 负责项目售后、代运维支持工作，及时响应并解决客户提出的技术问题，保障系统、网络稳定运行
- 结合客户实际需求，策划并组织各层级人员的信息安全培训，提升团队安全意识和基础防护能力

2025.01-2025.07

鼎驰科技发展有限公司

运维工程师

- 参与金元证券云计算部门云平台运维，协助完成漏洞修复、服务器基础维护及平台升级工作，保障保障金融级系统稳定性
- 建立并维护 IT 资产台账，涵盖服务器、网络设备等资产信息，同时提供桌面运维支持，保障办公设备正常使用
- 收集并整理日常运维数据（如资源使用情况、故障记录等），定期形成报告，为平台优化提供参考

2025.08-2026.08

深圳智慧林网络科技有限公司

网络安全运维

- 负责公司官网服务器及数据库运维与网站上线部署，运用 AI 工具实现官网运行状态智能监控告警
- 负责公司网络安全防护与基线加固，参与视频监控安防服务器研发，支撑公司安防业务落地

项目经验

2022.07-2022.7

广西教育护网

- 在授权的渗透测试中独立完成。前期通过主动信息收集和被动信息收集对网站信息手工和工具自动批量打点后，根据收集的信息进行工具漏洞探测并配合 burp、goboy 等工具进行手工验证，最后挖掘到目录遍历漏洞一个，SQL 注入漏洞一个、逻辑漏洞两个并制作渗透测试报告与修复建议上交。

2023.03-2023.03

深圳市军民融合安全部署部署项目

- 路由部署深信服防火墙代替出口设备，单臂部署 ssl vpn、串接部署上网行为管理 AC，达到国家二级等保测评要求。

2023.04-2023.04

深圳市无线电监测管理站组网存储项目

- 服务器安全隔离方案落地，主备部署上网行为控制、主备部署防火墙、旁路部署 EDR、vpn，把服务器规划在一个安全的纯内网环境，达到国家二级等保测评要求。

2023.03-2024.07

深圳市无线电监测管理站网络安全维保项目

- 负责站内办公网络与网络安全的维护，协助站内解决网络技术问题，以及站内设备的更新上架，对客户所有信息系统用户、角色、权限合理性审核与校正；出现网络攻击或安全事件时帮助客户恢复系统及调查取证。

2023.06-2023.06

深圳市标准技术研究院深蓝护网行动

- 前期模拟组织多次次模拟演练（涵盖勒索病毒、供应链攻击、数据泄露场景），并策划组织客户各层级人员信息安全培训，同时输出相应应急预案文档，中期在完成基线加固的同时部署蜜罐，在值守期间对出现的 0day 漏洞进行临时修复或设置相应网络安全策略，并成功溯源多个攻击者 VPS 同时并进行封禁以及事件记录。

2023.09-2023.09 深圳环境监察支队深信服 VPN 项目

- 使用深信服 BBC 集中安全管理平台，将 30+分支 VPN 设备接入 BBC 集中安全管理平台，再通过策略模板统一下发实现批量配置与网络安全管控，保证网络传输安全与私密。

2024.03.2024.03 深圳市无线电监测管理站信锐 SFG 网关部署项目

主导重新规划站内各站点子网，使用 SFG 网管统一管控各站点分支出口交换机设备，实现流量的负载均衡，以及流量日志的审计，极大提高了站内运维管理效率，同时并回收政务网 ip 资源。

2023.03-2024.07 深圳市标准技术研究院网络安全维保项目

- 负责院里网络与网络安全的维护，参与网络安全方案的制订与实施，协助护网项目开展，以及设备的更换上架。

2024.06-2024.7 深圳市文化馆国家级护网行动

- 完成前期资产梳理与基线加固：排查服务器、网络设备等 IT 资产，识别弱口令、未授权访问等高危漏洞，同时
- 制定分优先级修复方案，96 小时内完成 28 个高危漏洞闭环修复，低危漏洞整改率 90%，同步更新安全基线配置、防火墙策略优化、日志审计规则完善等，攻防演练期间，所值守单位实现 0 失分。

2024.03-2024.3 无委大厦 17 楼信锐无线网络改造

- 主导无线改造方案设计，结合建筑结构，规划部署无线 AP 30 台，采用 AC 集中控制器，实现统一管理，通过 PoE 交换机供电简化布线，覆盖面积从原 60% 提升至 99%，强化无线安全机制对接企业 AD 域实现员工账号统一认证，设置物联网设备 MAC 地址白名单，有效防范无线入侵，符合等保二级接入安全要求。

2024.07-2024.12 中国移动项目国际业务运营分析平台运维项目

- 负责项目系统底层 linux 安全运维工作，mysql 数据库的查询与备份
- 查看监控系统 prometheus、dashboard 容器运行情况，查看应用运行日志信息，ELK 等
- 负责项目系统的容量评估、故障演练、服务降级、异常熔断、监控告警等工作，同时收集、编写、汇报日常运维中的各项数据与演练报告。

2025.03-2025.3 PXE 无人值守批量自动化部署项目

- 搭建 DHCP+TFTP+HTTP 服务架构，编写 Kickstart 自动化应答脚本，实现 CentOS 7 系统全程无人值守安装，实现 50 台物理服务器的批量操作系统部署。

2025.04-2025.4 证券机房搬迁项目

- 前期梳理服务器、网络设备等 it 资产，编写相应迁移方案，将业务中断时间控制到最小，并对业务配置与业务数据进行相应备份，校验数据完整性，最终零数据丢失完成搬迁

2025.09-2026.09 公司官网 AI 智能监控平台建设项目

项目背景：官网此前依赖人工巡检与事后报障，故障发现滞后、告警噪音大、定位耗时长；项目目标是构建覆盖外部访问体验与内部资源水位的智能监控体系，实现故障提前发现、告警降噪与快速定位。

整体技术架构与选型

- **数据采集层**：Blackbox Exporter 做 HTTPS 拨测，采集状态码、首包与全页耗时、证书剩余天数；Node Exporter 采集服务器 CPU、内存、磁盘 IO 与连接数；MySQL Exporter 采集连接数、慢查询与主从延迟；Filebeat 采集 Nginx 访问日志与应用日志。指标 30 秒一轮，拨测 1 分钟一轮。
- **传输与存储层**：Prometheus 定时拉取指标写入本地 TSDB，保留 90 天；日志经 Filebeat→Logstash 清洗后入 Elasticsearch，按天建索引并保留 30 天。全栈以 Docker Compose 部署，监控数据本地留存、仅外发告警摘要，兼顾成本与数据合规。
- **分析推理层**：Grafana 负责可视化与阈值告警；自研 Python 服务定时聚合 Prometheus 与 ES 的窗口数据，调用 DeepSeek 大模型 API 完成日志聚类、异常语义判定与根因初判，结果回写 ES 并生成结构化结论。
- **告警通知与可视化层**：Alertmanager 按 P0/P1/P2 分级路由，分别采用电话短信、企业微信机器人与日报汇总；Grafana 大盘统一展示可用性、P95 耗时、错误率与证书到期倒计时，实现一屏看全局。

监控方法与 AI 应用场景

- **监控指标**：覆盖可用性、响应耗时、错误率、证书与域名到期、首页关键字校验，并叠加服务器与数据库资源水位，形成“外部体验+内部资源”双视角。
- **探测策略**：拨测频率 1 分钟，深圳、上海、北京三地节点与多运营商线路交叉验证，剔除单点网络抖动造成的误报；连续 2 个周期失败才触发告警，证书与域名按 30/7/1 天分级提醒。
- **异常判定**：静态阈值（可用性<99.9%、P95>1.5s）与动态基线（同比环比偏离超 3σ）双轨并行，并对持续劣化趋势提前预警，解决“只看阈值、不看趋势”导致的漏报。
- **AI 职责**：①日志与告警聚类降噪，同类告警合并为一条事件并给出置信度；②异常检测与趋势预测，识别流量突增、爬虫与 CC 攻击苗头；③根因辅助定位，关联发布记录与依赖拓扑给出 TOP3 可能原因；④自动生成值班摘要与处置建议。

项目价值

- **业务成果**：上线 6 个月累计提前发现 12 起潜在故障（证书到期、磁盘水位告急、慢查询堆积等），均在用户可感知前完成处置；官网年可用性 99.95%，告警量下降约 70%，平均修复时长（MTTR）由 45 分钟降至 12 分钟。

个人技能

- 熟悉网络安全设备配置、防火墙、交换机、网络审计、设备高可用性、设备流量管理等。
- 熟悉 Linux、Windows、国产操作系统的基本命令/工具、常规服务、文件结构等。
- 熟练 Zabbix、nagios 监控，监控服务集群各种基本性能指标，保障服务器
- 熟悉常见开源软件如 Nginx、Tomcat 的配置与维护以及安全加固。
- 熟练使用 nessus，awvs 等工具，并能修复系统和服务的漏洞。
- 能够对国外资料进行简单翻译，并且能做一定的学习研究。
- 熟练 Prometheus、Grafana、ELK 监控栈搭建与维护，独立完成采集、接入与大盘配置
- 熟练运用 DeepSeek、ChatGPT 等大模型辅助运维：日志聚类降噪、异常语义判定与根因定位
- 熟悉 Python 运维自动化：监控数据拉取、告警聚合、企业微信机器人告警推送与日报生成
- 熟悉 WEB 安全相关知识，OWASP TOP10 漏洞原理。

荣誉证书

- 华为认证 HCIP-Security 证书
- CET-4 证书
- 深信服认证 SSTP 证书