Justin Bowen

Justin Bowen
Dallas, TX
https://justin.vet | justin.bowen.1337@gmail.com | github.com/penguinztech | linkedin.com/in/justinbowendfw/

PROFESSIONAL SUMMARY

Technology and Information Security Leader with 20+ years of experience spanning all facets of the technology stack. A proven technical and people leader across the full spectrum of Information Security (Blue, Red, GRC, and beyond), Network Engineering, Helpdesk Operations, and Program Definition. As an award-winning programmer since 2004, I frequently contribute to open source projects to drive technical innovation. Seeking a Senior Individual Contributor or Senior Management role where I can apply my comprehensive background in building secure, scalable systems and leading high-performing technical organizations.

CORE COMPETENCIES

- **Certifications:** GCWN, GPEN, GCIH, GCFA, GXPN, Security+, A+, Network+, Project+, Cloud+, Certified Kubernetes Administrator (CKA), Linux Professional (LPIC)
- **Technical Leadership:** Infrastructure Security (18 yrs), Incident Response (13 yrs), Threat Detection (13 yrs), Cloud Security (5 yrs), Application Security (5 yrs)
- **Software Development:** Python (18 yrs), Go (7 yrs), Bash (20 yrs), Perl(2 yrs), x86 Assembly(3 yrs), PHP(3 yrs), Rust (1 yr), and JavaScript (12 yrs)
- **Strategic Operations:** Security Orchestration, Automation, and Response (SOAR), Zero Trust Architecture, AI Security Strategy, DevSecOps
- **Industry Contributions:** Cloud Security Alliance (CSA) author and contributor for AI and Zero Trust Security
- **Leadership Experience:** 3 years as a Manager and 6 years as a Senior Manager.

PROFESSIONAL EXPERIENCE

Head of Information Security / Founding Security Engineer | Raya App, Inc. | April 2025 – June 2026

- Established a comprehensive information security program from inception, covering all domains and governance frameworks from a technical and program leadership perspective.
- Implemented AI security controls through hooks, proxies, and local client configurations to ensure secure model adoption.
- Deployed and optimized EDR, NDR, CDR, CNAPP, and MDR solutions alongside a modern Mobile Device Management (MDM) suite.
- Authored and enacted 23+ security policies and standards to formalize organizational security posture.
- Optimized CI/CD pipelines by integrating security automation, AI, and IaC (Terraform / Ansible), services , significantly reducing production vulnerabilities and security gaps.
- Directed Application and API security improvements, enhancing the resilience of core product offerings.
- Led incident response workstreams, achieving successful resolution of critical incidents within hours of detection.
- Collaborated with the Cloud Security Alliance (CSA) on AI Security documentation and steered internal AI strategy across business units.
- Documented and executed a strategy for migrating to centralized SSO for streamlined login and role assignments.

- Built a self-service AI suite integrating 15+ linters and security scanners, automating localized security reviews and development workflows and reducing late stage security blockers.

Staff Security Engineer & Technical Lead Manager | Uber Technologies Inc | April 2020 – March 2025

- Directed global network security operations for Uber and its subsidiaries, managing 12+ concurrent technical projects.
- Architected and led execution against 5-year security roadmap encompassing cloud and physical network infrastructure company-wide.
- Created a security performance testing framework that reduced endpoint-related support tickets by 50%.
- Developed a serverless detection system that proactively intercepted over 1,000 malicious files.
- Spearheaded infrastructure redesigns to enhance platform resilience and mitigate large-scale attack vectors.
- Deployed enterprise-scale Zero Trust and SASE solutions including Zscaler and iBoss.

Senior Manager (NCOIC) - Cyber Security Training | TX Air National Guard | 2022 – 2023

- Rebuilt training program from near zero
- Prepared 30 person team which successfully completed cyber security quick reaction force missions
- Managed training programs and 1:1 training for 30 technical leads

Senior Manager (NCOIC) & Technical Lead | WA Air National Guard | 2020 – 2022

- Rebuilt the Weapons and Tactics (WepTac) program; operational oversight and technical audits.
- Identified and remediated 10+ critical technical discrepancies through rigorous internal auditing.
- Managed and trained a 30-person security blue team to defend against nation-state Advanced Persistent Threats (APTs).
- Rebuild deployments and usage with IaC /CaC (Ansible)

Manager, Technical Security Services | Protiviti Consulting | May 2018 – April 2020

- Directed incident response and proactive threat hunting engagements for specialized client environments as well automation and orchestration across multiple domains.
- Designed and implemented enterprise security architectures for large-scale cloud migrations.
- Standardized company-wide monitoring and automation workflows to improve operational efficiency.

Technical Manager, Red Team | Washington Air National Guard | 2017 – 2020

- Established the unit's inaugural Red Team and provided training to security personnel across the USAF.
- Executed dozens of threat detection engagements, authoring over 100 custom detection rules.
- Led high-impact Purple Team exercises to validate and improve defense-in-depth strategies.

SKILLS

- **Cloud & Infrastructure:** AWS, GCP, Azure, OCI, Vultr, OpenStack, Kubernetes (K8s), Cloud-Native Security, Multi-Cloud Governance
- **Artificial Intelligence:** AI Security, LLM Security, AI Governance, AI Model Adoption, Ollama, llama.cpp, Claude, Gemini, ChatGPT/OpenAI, Mistral, AI Sandboxing, AI Cluster hardening, guardrails
- **Networking:** Networking, TCP/IP, SASE, SSE, DMVPN, PKI, Wireguard, IPSEC, Cisco, Juniper, Arista, Firewalls, envoy proxy, cilium, and network policies, eBPF, Micro-segmentation, Software-Defined Networking (SDN), Identity-Aware Proxy (IAP)
- **Systems Security:** EDR (e.g.: CrowdStrike, SentinelOne), MDM (Iru, FleetDM), Mac OS, Linux, and Windows
- **Programming & Scripting:** Python, Go, Bash, Perl*, x86 Assembly, PHP, JavaScript / NodeJS *, Ruby *, Crystal *, and Rust *

- **Automation & Security Tools:** Ansible, Terraform / OpenTofu, n8n, Apache NiFi, UiPath, Splunk, ELK, LogRhythm, Zscaler, iBoss, Crowdstrike, Wiz, EDR, NDR, CDR, CNAPP, MDR, Security Observability
- **Threat Intelligence, Detection, & Response:** Threat Intelligence, Incident Response, Threat Hunting, Logging & Visibility, Regex, Snort, Splunk, ELK, LogRhythm, FireEye, Purple Teaming
- **Product Security:** RASP, Approov, AppDome, Cloudflare, bot prevention, REST API protection, gRPC API Protection, and GraphQL API Protection
- **Identity & Access Management:** Okta, SSO, SAML, OIDC, OAuth2, SPIFFE/SPIRE, JWTs, Authentication Proxies, Envoy Proxies
- **DevSecOps:** GitHub Actions, GitLab CI/CD, Wiz, Socket.dev, Snyk, Software Supply Chain Security
- **Governance, Risk, & Compliance (GRC):** Zero Trust, NIST, ISO27001, PCIv4, HIPAA, NYDFS, CSA STAR, SOC2, and experience in writing policies, standards, and guidelines.

EDUCATION

- **Western Governors University** | Bachelor of Science in Network Engineering and Security
- **Regis University** | Bachelors of Science - Computer Science | Minor in Psychology
- **United States Air Force** | Associates in Science - Cyber Defense Operations

Additional Work History

- Network Security Engineer | Alaska Airlines | 2017 – 2018
- Blue Team Lead | REI | 2015 – 2017
- Cyber Security Technical Lead | WA ANG Cyber Protection Team | 2015 – 2017
- Enterprise Network Security Lead and Auditor | USAF Reserves, INOSC– West | 2012 – 2015
- Enterprise Security Engineer 2 | Amazon Inc. | 2014 – 2015
- Senior Threat Network Security Engineer | Trustwave, Inc. | 2013 – 2014
- Enterprise System Security Engineer | L3 Stratis | 2012 – 2013
- Lead Enterprise Network Security Engineer | U.S. Air Force Active Duty | 2007 – 2012
- Forum Support Moderator | Awardspace Web Hosting | 2006 – 2007

Professional references available upon request.