Vansh Bhardwaj

Austin, TX | scorpio.vansh@gmail.com | (512) 460-9515 | github.com/VanshBhardwaj1945 | linkedin.com/in/vanshbhardwaj1945

Experience

Midcontinent Independent System Operator (MISO)
Security Engineer Co-op (Incoming) Aug – Dec, 2027

- TBD - Incoming security engineering co-op.

Cloudflare
Security Engineer Intern, Enterprise IAM June – Aug, 2026

- Automated access governance, least-privilege enforcement, and access reviews across the company's SaaS estate.
- Eliminated configuration drift by replacing a hardcoded app-to-access-group map with live Cloudflare Access API lookups, automatically detecting renamed and decommissioned apps the static list missed.
- Automated inactive access detection to enforce least privilege: a scheduled Cloudflare Worker pulls login telemetry via the Cloudflare Access API and flags users with dormant SaaS access for review and deprovisioning.
- Authored access-control policy-as-code in Rego/OPA (with OPAL) and built an excess-access detection algorithm to surface entitlements beyond a user's need.
- Built the Python/Bash data layer behind a JSON REST API, with caching to cut redundant API calls and read-only scoping across multiple isolated accounts.
- Followed GitOps practices — access via merge request, short-lived credentials over hardcoded secrets — and contributed to threat modeling in security design reviews.
- Built a multi-agent AI development workflow (Architect/Analyst/Engineer/Security roles with persistent memory and a dashboard) to accelerate long-running projects.

Pitney Bowes
Software Engineer Intern June - July 2024

- Built a full-stack AI chatbot on Azure: a chat UI frontend and a Python backend integrating the Azure OpenAI Service via token-based API auth; collaborated through GitHub branches and PRs.
- Provisioned cloud infrastructure (VMs, virtual networks, load balancers, storage) and managed API tokens/keys securely.
- Built Docker images and deployed containerized services to a Kubernetes cluster; tested CI/CD in GitHub Actions and reviewed Terraform IaC.
- Supported backend teams on databases/query flows ad auth-token patterns.

Projects & Labs

FlowSec — CI/CD Pipeline Security Scanner .
Python · PyGithub · PyYAML · MITRE ATT&CK · OWASP CI/CD Top 10 · Claude API · Gitleaks May – June, 2026

- Built a 9-stage automated CI/CD pipeline using Jenkins for a live deployed Python Flask/SocketIO application, integrating security scanning, container deployment, and post-deploy verification into a fully automated delivery workflow.
- Built a live Grafana observability dashboard connected to Azure Log Analytics via KQL, monitoring request volume over time, health check frequency, and recent container logs across three real-time panels.
- Implemented Ansible post-deploy verification with 7 structured reliability tasks: port availability checks, HTTP health endpoint validation, response time threshold assertions, and JSON field verification run automatically after every deployment.
- Provisioned and managed all Azure infrastructure (Container Registry, Container Apps, Log Analytics Workspace) with modular Terraform, maintaining configuration as code with documented drift reconciliation.

Click Arena — DevSecOps Pipeline
Jenkins · Docker · Terraform · Ansible · SonarQube · Snyk · Trivy · Gitleaks · Cloudflare Worker · Azure Container Apps · Grafana Apr 2026

- Engineered a production-grade DevSecOps pipeline on Azure with a security gate at every stage and a Cloudflare edge layer, using a live multiplayer app as the deployable.
- Built a Jenkins pipeline-as-code chaining Gitleaks → SonarQube (SAST) → Snyk (SCA) → Docker build → Trivy (container scan) → Azure Container Registry → Azure Container Apps → Ansible verification → smoke test, fail-closed at each stage.
- Remediated real SAST findings — SonarQube flagged a CSRF misconfiguration in the SocketIO handshake plus 5 hotspots; fixed and documented.
- Enforced shift-left secret hygiene with Gitleaks pre-commit hooks plus a pipeline stage, and gated images on HIGH/CRITICAL CVEs via Trivy.
- Implemented an edge security layer in a Cloudflare Worker — API-key (X-API-Key) auth, HTTP security-header injection, and a 5-minute cron audit of allow/block rates.
- Provisioned the full Azure stack as code (Terraform) with Azure Monitor + Grafana observability dashboards.

Cloudflare Security Hardening
Cloudflare WAF · Access (Zero Trust) · Workers · Bot Protection · Page Shield · Terraform · OWASP Apr 2026

Performed a 6-phase security hardening of a live production site, managed entirely as Terraform IaC — WAF, Zero Trust access, edge Workers, rate limiting, and bot defense.

- Practiced detection-first hardening: analyzed live edge telemetry, identified an AWS EC2 recon bot (via whois) and anomalous POST probing, and wrote targeted blocking rules.
- Authored default-deny WAF rules covering SQLi, XSS, and path traversal, scanner User-Agents (sqlmap/nikto/nmap), and non-GET methods — manual OWASP Top 10 coverage.
- Enforced Zero Trust via Cloudflare Access (email OTP) on an /admin origin with no native auth, and rate-limited the API (4 req/10s/IP) to prevent abuse and Cosmos DB exhaustion.
- Deployed a Cloudflare Worker injecting six HTTP security headers (CSP, HSTS, X-Frame-Options, etc.), plus Bot Fight Mode, AI-bot blocking, and Page Shield for Magecart/supply-chain monitoring.

Cloud-Native Resume Platform
Azure Functions · Cosmos DB · Front Door · Storage · Cloudflare DNS/DNSSEC · Terraform · GitHub Actions · Pytest Feb 2026

- Built a serverless, fully-IaC web app on Azure with a CI/CD-tested API behind Cloudflare DNS.
- Architected separated layers — Azure Storage static frontend behind Front Door (CDN/TLS), Python Azure Functions REST API, Cosmos DB backend — with Cloudflare DNS + DNSSEC.
- Provisioned all infrastructure as modular Terraform with documented drift reconciliation.
- Built GitHub Actions CI/CD running Pytest on every push to block failing deploys.

Virtual Network Sandbox & Application Layer DoS Detection
VirtualBox · VMware · pfSense · iptables · Splunk (SIEM) · Nmap · Wireshark · tcpdump · Apache Feb 2026

- Engineered a segmented sandbox network using VirtualBox and VMware with Ubuntu Server, Windows, and Kali Linux instances and enforced traffic controls with pfSense.
- Administered Ubuntu Server instances from the command line, configured networking and services, and used Nmap, Wireshark, and tcpdump for packet capture and traffic analysis.
- Conducted controlled application layer DoS testing, measured service impact, ingested telemetry into Splunk, and produced detection playbooks documenting incident timeline, evidence, and remediation steps.

Azure Hands-on Labs

Entra ID · Azure RBAC · Azure Policy · ARM templates · Bicep · VMs/VMSS · NSG · VNet peering (In progress)

- Completed AZ-104 labs across identity, governance, networking, and IaC.
- Configured Azure RBAC, management groups, and service principals with least-privilege role assignments.
- Authored Azure Policy for tag enforcement, allowed SKUs, and baseline governance.
- Built VNet peering, route tables, and NSGs; deployed VMs/VMSS via ARM templates and Bicep.

Certifications

- CompTIA Security+ (SY0-701) Jan 2026
- Microsoft Certified: Azure Fundamentals (AZ-900) Feb 2026
- Google Cybersecurity Professional Certificate Aug 2025
- Microsoft Certified: Azure Administrator (AZ-104) Expected Aug 2026

Education

Bachelor of Science Degree, Computer Science - Texas State University

**Minor in Business Administration *Cybersecurity focus* Aug 27th. 2023 – (Expected) Dec 13th, 2027

****Relevant Coursework:*** *CS Systems and Security, Operating Systems, Assembly Language, Computer Architecture, Data Structures, Data Oriented Programming*

Technical Skills

- **Languages**: Python, Bash, PowerShell, JavaScript, C++, Java, HTML/CSS
- **Identity & Access (IAM):** IAM/IGA, access reviews & certification, least privilege, Zero Trust, zombie/inactive-access detection, deprovisioning, excess-access & entitlement analysis, RBAC, SSO, OAuth 2.0 / OIDC, policy-as-code (OPA/Rego, OPAL), Cloudflare Access, Microsoft Entra ID, service principals, secrets management
- **Cloud (Azure):** Functions, Container Apps, Container Registry, Cosmos DB, Front Door, Storage, Log Analytics, Azure Monitor, Application Insights, Azure CLI
- **Infrastructure as Code:** Terraform, ARM templates, Bicep, Ansible
- **CI/CD & DevOps:** GitHub Actions, GitLab CI, Jenkins, Azure DevOps, Docker, Kubernetes, pre-commit hooks, Pytest
- **Security Scanning (SAST/SCA/secrets/container):** SonarQube, Snyk, Trivy, Gitleaks, Bandit, pip-audit
- **Edge & Web Security:** Cloudflare (WAF, Access, Workers, Workers KV, Bot Protection, Page Shield, Access API), security headers, rate limiting, API-key middleware
- **Detection & Monitoring:** Splunk (SIEM), Grafana, Azure Monitor, structured logging; Nmap, Wireshark, tcpdump
- **Network & Firewall:** pfSense, iptables, Network Security Groups, network segmentation, TCP/IP, DNS, HTTP/HTTPS
- **AI & Agentic Engineering:** agentic & prompt engineering, multi-agent workflows, MCP (Model Context Protocol) servers, LLM API integration (Anthropic Claude API), AI-assisted development (OpenCode, Windsurf, Claude)
- **Frameworks & Standards**: OWASP Top 10, OWASP CI/CD Top 10, MITRE ATT&CK
- **Databases**: Cosmos DB, MySQL, PostgreSQL
- **Operating Systems:** Linux (Ubuntu, Kali), Windows / Windows Server, macOS