Cuong Nguyen

Technological Polymath - Security & Embedded AI Engineer

cu5t05.com cu5t05inbox@gmail.com linkedin.com/in/cu5t05

Specialties

Cybersecurity: Cloud (AWS/Azure/GCP), IAM/Zero Trust (Okta/Entra), SSO/SAML/OIDC, WAF/CDN, KMS/Secrets (KMS/Key Vault/Vault), SIEM (Splunk/ELK), EDR (CrowdStrike), SOC 2, ISO 27001, NIST CSF, Incident Response.

DevSecOps & IaC: Terraform, Policy-as-Code, CI/CD (GitHub Actions/GitLab/Jenkins), supply-chain (SBOM, cosign), SAST/DAST, container security (Trivy/Falco).

Cloud & K8s: AWS (VPC/IAM/S3/CloudFront/Lambda/API GW/RDS), EKS/AKS/GKE, networking, org/multi-account, cost optimization.

AI & Agents: Pipelines, RAG (retrieval/embeddings), vector stores, model serving, guardrails, ML observability, local/offline (llama.cpp/ Ollama).

Observability & SRE: OpenTelemetry, Prometheus/Grafana, Datadog, logs/traces/metrics, SLOs, MTTR/RPO/RTO, alerting, disaster recovery.

Automation: Python, Bash, PowerShell, Ansible, APIs, config management.

Experience

Security & Embedded AI Engineer - Contractor

2020 - Present - New York, NY & Remote

Architected secure on-prem, cloud, and hybrid systems across platforms (AWS, Proxmox, Kubernetes, pfSense) with Zero Trust and controls aligned to SOC 2, ISO 27001, and NIST CSF.

Automated provisioning and ops with Proxmox CLI, Terraform (IaC), and Ansible (idempotent roles, drift detection, change audits).

Designed and deployed embedded, offline AI for air-gapped and intermittent networks, packaging models and guardrails for reliable edge operation.

Implemented DevSecOps pipelines (GitHub Actions) with SAST/DAST, SBOM signing, secrets/KMS, and policy-as-code for reproducible, gated releases.

Built observability and IR readiness (OpenTelemetry to Prometheus/Grafana/Datadog, SIEM); defined SLIs/SLOs and runbooks to accelerate MTTA/MTTR.

AV/IT Engineer - Contractor

2015 - 2020 - New York, NY & Touring

Delivered interactive AV/IT systems and full-stack web apps (frontend/backend/DB) for installations, logistics, and content workflows.

Built networking IaC (VLANs, ACLs, DHCP/DNS) for segmented stage networks with rollback and disaster-recovery playbooks (RPO/RTO baselines).

Implemented show control/lighting (DMX/Art-Net) with fault-tolerant rigs; standardized runbooks and drills achieving sub-2-minute MTTR in simulations.

Led staff training and knowledge transfer (onboarding, SOPs, playbooks) to improve handoffs and ensure consistent show readiness.

Managed production web presence (TLS, CDN/WAF, patching, backups) to measurably improve latency and uptime.

Projects

Embedded AI Cross-Chain Payment Orchestrator: Multi-hop route, split, and timing optimization across allowlisted bridges/DEXs; uses MCP + market-data connectors for quotes/state; enforces policy/risk limits; executes payments to minimize fees, slippage, and MEV with full decision logging.

AWS SSH Agent Hijacking - Bastion Host Risk: Simulated identity bypass via SSH agent/port forwarding; recommended replacing bastions with Session Manager and cert-based SSH to eliminate bastion exposure.

Automated AWS Security Lab - Terraform & CLI: Repeatable EDR/IR drills (GuardDuty to Lambda to containment), enabling automated detection/response testing.

Hybrid Security Research Lab - Proxmox, Tailscale, LLaMA.cpp: Built a hardened remote-access Proxmox cluster (key-only SSH, no root/password logins) hosting multi-VM environments for secure dev, blockchain simulation (Anvil/Besu), federated auth labs (Windows Server - AWS), and security monitoring (pfSense, Snort, Splunk), plus GPU-accelerated offline AI agentic workflows using Python-wheeled LLaMA.cpp.

Education

Goucher College - B.A.

2010-2014

Area of study: Applied Computer Science & Information Technologies in the Arts (systems, software, and digital media applications)

Honors & Awards

1st Place - Bloomberg Hackathon Cybersecurity CTF

Honors in the Major

The Phi Beta Kappa Brooke Peirce Award in Fine Arts