Thong Huynh

Nashville, Tennessee • thuynh808@streetrack.org Azure Cloud Resume • LinkedIn • GitHub • THM Top 5%

SUMMARY

IT professional specializing in cloud security, automation, and system administration, with hands-on experience building secure, scalable infrastructures in **Azure**, **AWS**, and **Linux** environments. Skilled in **Ansible** and **Terraform**, with a focus on improving security posture and operational efficiency through automation and structured processes.

WORK EXPERIENCE

Log(N) Pacific *Lynnwood, WA (Remote)*
Cyber Security Support Engineer (Internship) May 2024 – Mar 2025

- Built and managed a **SIEM** in Azure, centralizing logging, monitoring, and alerts to enhance incident response
- Configured Azure **Network Security Groups** and **Microsoft Defender for Cloud**, ensuring NIST 800-53 compliance reducing security incidents by **71%**
- Developed **KQL** queries and dashboards to track security alerts, improving threat detection and response times
- Supported troubleshooting of **SSH**, **firewalls**, and Azure deployments, focusing on secure cloud configurations

WorldCom Cable (Comcast Contractor) *Houston, Texas*
Cable Technician Jun 2006 – Jun 2008

- Installed and maintained over **500 cable systems** in homes, ensuring reliable internet, phone, and television
- Ran custom lines to establish connections for various services and installations to meet specific customer needs
- Demonstrated **troubleshooting** skills, efficiently resolving issues to ensure uninterrupted service

PROJECTS

Azure Cloud Resume
- Engineered a cloud-based resume website with a live visitor counter, utilizing Azure Storage Static Website, Function APIs, Cosmos DB, and automated via **CI/CD** with **GitHub Action** workflows

Breach-Tracker
- Deployed a secure AWS breach tracker with **ECS Fargate, ECR, API Gateway, Terraform modules, and Ansible**, containerizing a Flask app that fetches data from Have I Been Pwned's Breaches API
- Architected a **multi-AZ VPC** with **public/private subnets**, **NAT Gateway**, and **Internal ALB** for scalable and private backend communication, following AWS security best practices

HA-WebTrack
- Designed a **high-availability** web server using **Ansible**, featuring system monitoring, and alerting via **Slack**
- Implemented performance testing with **Prometheus**, **Loki**, and **Grafana**, analyzing server load, traffic management, and failover response for comprehensive infrastructure monitoring

Azure Live Traffic SOC Honeynet
- Implemented a honeynet in **Azure**, integrating logs into Log Analytics for Microsoft Sentinel **SIEM**, enhancing security via metrics (Windows/Linux logs, alerts, incidents, malicious flows) following NIST SP 800-53 Rev 5
- Analyzed security pre/post control over 48 hours using Azure tools, improving honeynet security posture

Elastic Labs
- Simulated Elastic Stack environment using **Ansible** for automated deployment and management
- Configured **SIEM** system with **Elasticsearch, Kibana, Fleet, Zeek** integration, and Elastic Agents on RHEL

CVEDataLake
- Built an AWS CVE data lake with **S3, Glue, Athena** and **Ansible** for automated ingestion, storage, and analysis
- Generated **JSON reports via Python, SQL, and Ansible** for SOC dashboards, and vulnerability management

CERTIFICATIONS

AWS Certified Solutions Architect - Associate | Jan 2025
Microsoft **Azure** Security Engineer Associate | Apr 2024
Microsoft **Azure** Administrator Associate | Feb 2024
Red Hat Certified System Administrator **RHCSA** | Jul 2024
Red Hat Certified Engineer **RHCE** | Sep 2024
CompTIA **A+** | **Security+** | **CySA+** | 2023

SKILLS

Automation & DevOps: Terraform, Ansible, GitHub, CI/CD, Bash, Python, IaC
Security: SIEM, EDR, Incident Response, Vulnerability Management, Cloud Security, IAM, Firewall, OAuth2.0
Systems: Linux (RHEL), Windows, Virtualization, Networking, DNS, LVM, System Monitoring, High Availability