Thong Huynh

Nashville, Tennessee • thuynh808@streetrack.org

Cloud Resume • LinkedIn • GitHub

SUMMARY

Cloud and Security Infrastructure Engineer with a hands-on mindset, skilled in Linux, AWS, Azure, and automation tools like Ansible and Terraform. Built secure, STIG-compliant systems and real-world projects. Backed by years of fieldwork in farming and construction, bringing strong work ethic and problem-solving skills.

Explore my interactive Cloud Resume at streetrack.org

TECHNICAL SKILLS

- **Cloud**: AWS (EC2, VPC, S3, IAM, ECR, ECS, API Gateway), Azure (Sentinel, Defender, Cosmos DB)
- **Infrastructure**: Ansible, Terraform, GitHub Actions, STIG Hardening, Bash, Python, CI/CD
- **Security**: SIEM (Elastic, Sentinel), Incident Response, IAM, NIST 800-53, OAuth2.0, Vulnerability Management
- **Systems**: RHEL, Rocky Linux, Windows, HAProxy, Prometheus, Grafana, Apache, Zeek, LVM, Networking
- **Tools & Equipment**: Power tools, Drywall Tools, Framing Equipment, Heavy Machinery (Bulldozers, Excavators)

WORK EXPERIENCE

Log(N) Pacific *Lynnwood, WA (Remote)*
Cyber Security Support Engineer 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

Self-Employed
Fruit Farm Manager Jun 2020 – May 2025

- Oversaw all operations of a **12-acre** tropical fruit farm with hundreds of trees including lychee, soursop, and others
- Managed pruning, fertilization, harvesting, and packing of fruit for sale to local vendors
- Maintained irrigation systems, equipment, and scheduled harvest cycles for year-round productivity

Self-Employed / Contract Work *Hilo, Hawaii*
Construction Laborer – Tile Installation May 2022 – Feb 2024

- Measured, cut, and set tiles for kitchens, bathrooms, and flooring projects under the guidance of a veteran installer
- Mixed mortar, prepared surfaces, and assisted with grouting and final finishing for residential clients

Self-Employed / Contract Work *Hilo, Hawaii*
Dozer Operator Jan 2016 – Feb 2022

- Operated D6 dozer and heavy equipment across **500+** acres
- Conducted precision earthmoving for irrigation channels, orchard plots, and roadbeds
- Maintained and repaired machinery, ensured safety compliance, and coordinated with landowners

Self-Employed *Hilo, Hawaii*
Farmer (Ginger & Potatoes) Dec 2012 – Dec 2020

- Cultivated and harvested ginger and potatoes for sale across Hawai‘i Island
- Handled soil preparation, crop rotation, irrigation, and manual labor for large seasonal yields

Self-Employed / Contract Work *Hilo, Hawaii*
Builder & Drywall Installer 2013 – 2014

- Framed warehouse structures, set wall studs, and installed drywall panels
- Performed mudding, taping, and finishing tasks with attention to timeline and quality

RA Sushi Houston, Texas
Sushi Chef 2008 - 2012

- Prepared high-quality sushi and sashimi dishes, ensuring freshness and presentation excellence
- Interacted with customers, providing a positive dining experience and accommodating special requests

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

Elastic Labs *(SIEM/Ansible Automation)*

- Built an automated **Elastic** Stack **SIEM** lab across **RHEL** and **Windows** VMs using **Ansible**
- Integrated network telemetry and endpoint logs (**Sysmon**) with **MITRE**-based detection rules and dashboards
- Simulated **brute-force** attacks to validate alerting pipeline and confirmed log correlation for **SSH** and **RDP** events

Security Onion SOC Workshop *(Malware Analysis)*

- Created a virtual SOC with **Security Onion**, **Zeek**, **Suricata**, and **Wireshark** for network forensics
- Investigated **75+ IDS alerts** from a malicious **PCAP** file uncovering Oski stealer activity and **data exfiltration**
- Correlated threat intelligence with **AbuseIPDB** and **VirusTotal**, and delivered a full **incident report**

Azure SOC Honeynet *(Cloud Security)*

- Deployed a mini honeynet in **Azure** with **Microsoft Sentinel**, collecting **5+ log types** across 3 VMs which detected **253 incidents** and **1,000+ malicious flows** in 24 hours using custom **KQL** attack maps
- Implemented **NSG hardening**, **private endpoints**, and **firewall** rules resulting in reducing incidents from **253** to **0** and **malicious** traffic from **1,094** to **0** in the 24-hour post-hardening period

Project Fishy Phiisshing *(Email Analysis)*

- Automated the collection of **100+ phishing** email samples using a **Python** script and analyzed them in a **Kali Linux** VM with Thunderbird, **VirusTotal**, **Talos**, and **PhishTool**
- Investigated spoofed headers, malware attachments, and credential harvesting; delivered **2 SOC-style incident reports** with technical findings and **10+ mitigation** recommendations

ScanOps *(Image Vulnerability Scanning)*

- Built a **CI/CD** pipeline using **GitHub Actions**, **Trivy**, and **AWS ECR/S3** to automatically **scan**, **tag**, and **promote** or **quarantine** Docker images across 3 environments
- Generated **SBOMs** for 4 sample apps, scanned for **400+ CVEs**, and triggered **Slack** alerts for **CRITICAL/HIGH** findings ensuring only secure images reached production

Breach Tracker *(Automated Breach Intelligence)*

- Deployed a secure, auto-scaling breach data **API** using **Flask**, **ECS Fargate**, **ECR**, **API Gateway**, **internal ALB,** and **private subnets** across 2 availability zones via **Terraform** (**76+ resources**)
- Automated full-stack setup with **Ansible**, including **container** build, **ECR** push, and **S3-hosted dashboard**, serving sorted breach data from Have I Been Pwned

CVE Data Lake *(Vulnerability Intelligence)*

- Automated ingestion and analysis of **1,000+ CVE** records using **AWS S3**, **Glue**, and **Athena**
- Generated **8+ JSON** reports from **SQL** queries to support **SOC** workflows and **vulnerability** trend analysis

STIG-Hardened *(Ansible, RHEL, Compliance)*

- Automated **DISA STIG** hardening and validation for **RHEL 9** using **Ansible** and **SCC** across a multi-VM lab
- Improved system compliance from **35.4%** to **82.18%** by remediating over **40+** security findings (**CAT I & II**)

HA-WebTrack *(System Monitoring)*

- Deployed a **high-availability** web server cluster with **HAProxy** load balancing, **Prometheus**, and **Grafana** for **real-time monitoring**
- Simulated production **stress** by generating traffic with **Apache Benchmark**; verified **auto-failover** and **recovery**

CERTIFICATIONS

- **Microsoft Certified: Azure AI Fundamentals (AI-900)** - Apr 2025
- **AWS Certified Solutions Architect Associate (SAA-C03)** - Jan 2025
- **Red Hat Certified Engineer (RHCE)** - Sep 2024
- **Red Hat Certified System Administrator (RHCSA)** - Jul 2024
- **Microsoft Azure Security Engineer Associate (AZ-500)** - Apr 2024
- **Microsoft Azure Administrator Associate (AZ-104)** - Feb 2024
- **ITIL v4 Foundation** - Jan 2024
- **CompTIA CySA+** - Nov 2023
- **CompTIA Security+** - Jun 2023
- **CompTIA Network+** - Oct 2025
- **Cisco CCNA** - Oct 2025

EDUCATION

- **Bachelor of Science in Information Technology -** WGU *(In Progress)*