

# THONG HUYNH

Nashville, Tennessee

thuynh808@streettrack.org

[linkedin.com/in/thuynh808](https://www.linkedin.com/in/thuynh808)

<https://www.streettrack.org>

## EXPERIENCE

### Log(N) Pacific

Cyber Security Support Engineer (Intern)

5/1/2024 – 3/31/2025

Lynnwood, WA (Remote)

- Implemented **Azure security controls** including Private Endpoints, Network Security Groups (NSGs), and Defender for Cloud, resulting in **100% elimination of security incidents** and an **80% reduction in security events**
- Supported and troubleshooted **Azure Sentinel, Virtual Machines, Azure Monitor, Log Analytics, and Entra ID**, effectively resolving **5-7 infrastructure and security issues per week** across Linux and Windows environments
- Investigated and resolved recurring issues involving VM sizing and access, **SSH/RDP connectivity, SQL authentication, log ingestion failures, Syslog telemetry, NSG rule misconfigurations, MFA procedures, and identity access**
- Built **KQL-driven dashboards** to analyze authentication failures, network traffic, security events, and **Sentinel** incidents

WorldCom Cable (Comcast Contractor)

10/1/2006 – 12/31/2008

Cable Technician

Houston, TX

- Installed residential cable, internet, and voice services, completing **500+ service installations** with consistent uptime
- Diagnosed connectivity issues, ran custom cabling, and restored service through systematic troubleshooting

### Self-Employed Contractor

1/1/2009 – 4/1/2024

Heavy Equipment Operator & Farm Manager

Hilo, HI

- Operated and maintained heavy equipment, construction tools, and agricultural systems in contract roles
- Managed safety-critical, physically demanding work while meeting schedules, quality standards, and customer requirements
- Built discipline, problem-solving ability, and operational reliability through years of hands-on responsibility

## PROJECTS

### Enterprise Observability Platform - IT Capstone

- Delivered a centralized observability platform for a **Layer-3 collapsed-core OSPF network**, consolidating telemetry from 3 Cisco Layer-3 switches, a perimeter firewall, and Linux servers into unified dashboards
- Implemented a full monitoring and logging stack using **Prometheus, Grafana, Loki, Grafana Alloy, SNMP, and Syslog**, enabling correlated **metrics and logs** in a unified visibility plane
- Built a repeatable onboarding workflow using **Ansible automation**, standardizing deployment/configuration so future nodes can be added consistently as the environment scales
- Validated functionality through simulated **load testing** and **failover scenarios** to confirm real-time telemetry ingestion

**Portfolio:** <https://www.streettrack.org>

**GitHub:** <https://github.com/thuynh808>

## CERTIFICATIONS

Red Hat Certified Engineer (**RHCE**) | Red Hat Certified System Administrator (**RHCSA**)

Cisco Certified Network Associate (**CCNA**) | AWS Certified Solutions Architect – Associate (**SAA-C03**)

Microsoft Azure Administrator Associate (**AZ-104**) | Microsoft Azure Security Engineer Associate (**AZ-500**)

Additional Certifications: CompTIA A+, Network+, Security+, CySA+ | ITIL v4 Foundation

## EDUCATION

B.S. Information Technology - Western Governors University

## SKILLS

**Cloud Platforms:** Microsoft Azure, Amazon Web Services (AWS)

**Infrastructure & Compute:** Azure Virtual Machines, VNets, VM Scale Sets, Azure Storage, AWS EC2, ECS, S3

**Operating Systems:** Linux (RHEL, Rocky Linux, Ubuntu), Windows Server

**Security & SIEM:** Microsoft Sentinel, Azure Monitor, Log Analytics, Defender for Cloud, Elastic Stack, Zeek

**Monitoring & Observability:** Prometheus, Grafana, Loki, SNMP, Syslog

**Automation & IaC:** Ansible, Terraform, GitHub Actions, Bash, Python

**Networking:** TCP/IP, DNS, VLANs, 802.1Q trunking, OSPF, STP, EtherChannel, NSGs, Firewalls, Routing

**Telemetry & Analysis:** Windows SecurityEvent, Linux Syslog, KQL, dashboards, workbooks, attack maps