THONG HUYNH

Hilo, Hawaii | Thuynh808@streetrack.org | https://github.com/Thuynh808 | https://linkedin.com/in/thuynh808

SIEM | Azure | Vulnerability Management |Technical Analysis | System Administration | EDR | TryHackMe Top 5% Ansible | Linux(RHEL) | Networking | Virtualization | System Monitoring | CI/CD | LVM | IAM |

Transitioning into IT with a solid foundation in network security, incident response, and system administration

RELEVANT PROJECTS

AZURE CLOUD RESUME - https://www.streetrack.org

- 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

HA-WebTrack - https://github.com/Thuynh808/HA-WebTrack

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

Security Onion SOC Workshop - https://github.com/Thuynh808/Security-Onion-SOC-Workshop

- Leveraging the SIEM, imported a malicious PCAP file and executed incident response procedures to fortify network defenses
- Generated detailed incident reports, enhancing understanding of security threats and improving future incident response

The Cyber Streetracker - https://github.com/Thuynh808/TheCyberStreetracker

- Built a web app integrating real-time cybersecurity news and a CVE search tool using OAuth 2.0 for secure authentication
- Deployed with Azure Front Door and Web Application Firewall for security and availability

Azure Live Traffic SOC Honeynet - https://github.com/Thuynh808/Cloud-SOC

- 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, significantly improving honeynet security posture

Active Directory Lab - https://github.com/Thuynh808/Active-Directory-Lab

- Implemented a corporate Active Directory environment, configuring DC, DHCP, and DNS for seamless user authentication
- Automated user creation using Python scripts, enhancing efficiency and reducing manual errors

Project Fishy Phishing - https://github.com/Thuynh808/Fishy-Phiisshing

- Leveraged Python and GitHub API to automate phishing sample retrieval, strengthening threat intelligence capabilities
- Conducted in-depth analysis of phishing emails, documenting findings in comprehensive reports for cybersecurity awareness

Qualys Quest Analysis - https://github.com/Thuynh808/Qualys-Quest-Analysis

- Established a virtual environment for Qualys vulnerability assessments, systematically analyzing outdated applications
- Implemented a continuous vulnerability management cycle, generating trend reports to document & improve remediation process

PROFESSIONAL EXPERIENCE

Cyber Security Support Engineer (Intern) **Log(N) Pacific - Lynnwood, WA (Remote) | May 2024 – Present**

- **Cloud Security:** Configured Network Security Groups, and Defender for Cloud, ensuring NIST 800-53 compliance
- **Support & Troubleshooting:** Assisted students and troubleshooted infrastructure configurations with Microsoft Azure services

Agriculture Management & Operations Specialist **Self-employed - Hilo, Hawaii | Dec 2012 – Present**

- **Operations Management:** Orchestrated farm activities, cultivation, and harvesting processes to optimize yield and quality
- **Heavy Machinery Operator:** cleared forestry and fields with dozers and tractors for land preparation and cultivation

Cable Technician **WorldCom Cable - Houston, Texas | Jun 2006 – Jun 2008**

- **Installation Expertise:** Installed and maintained over 500 cable systems in residential homes, ensuring reliable service
- **Custom Line Installation:** Expertly ran custom lines to establish internet, phone, and television connections
- **Technical Proficiency:** Demonstrated technical proficiency in troubleshooting and resolving cable-related issues

CERTIFICATION & EDUCATION

- **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
- **Microsoft Azure Fundamentals AZ-900 |** Feb 2024
- **ITIL® v4 Foundation | AXELOS Global Best Practice |** Jan 2024
- **CompTIA - A+ | Security+ | CySA+ |** 2023