Thong Huynh

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

SUMMARY

IT professional with certifications in **AZ-104**, **AZ-500**, **RHCSA**, and **RHCE**, skilled in cloud security, automation, and **SIEM** solutions. Experience in **Azure**, **Ansible**, and **Red Hat** environments, designing and building secure, scalable infrastructures. Proficient in system monitoring, vulnerability management, and system administration with a focus on operational efficiency.

WORK EXPERIENCE

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

- Configured Azure Network Security Groups and Microsoft Defender for Cloud, ensuring NIST 800-53 compliance
- Integrated Azure Monitor to provide real-time visibility into cloud infrastructure performance and security
- Supported in troubleshooting **SSH**, **firewalls**, and **Azure** deployments, focusing on secure cloud configurations
- Built and managed a **SIEM** system in Azure, centralizing logging, monitoring, and alerts for incident detection
- Developed dashboards to track security alerts and exploits, enhancing threat detection and response times
- Successfully reduced security incidents by 71% through optimizing **NSG**s and cloud security configurations
- Developed **KQL** queries to extract actionable insights from logs, identifying incidents over defined 24-hour periods

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 services
- Ran custom lines to establish connections for various services, tailoring installations to meet specific customer needs
- Demonstrated strong **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

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

The Cyber Streetracker

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

Project Fishy Phiishing

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

Qualys Quest Analysis

- Established a virtual environment for **Qualys** vulnerability assessments, analyzing outdated applications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

CERTIFICATIONS

Red Hat Certified Engineer **RHCE** | Sep 2024
Red Hat Certified System Administrator **RHCSA** | Jul 2024
CompTIA - **A+** | **Security+** | **CySA+** | 2023
Microsoft Azure Administrator Associate **AZ-104** | Feb 2024
Microsoft Azure Security Engineer Associate **AZ-500** | Apr 2024
ITIL® v4 Foundation | Jan 2024

SKILLS

SIEM | Azure | Vulnerability Management | Technical Analysis | System Administration | EDR | Ansible | Linux(RHEL) | DNS
Windows | Networking | Virtualization | System Monitoring | CI/CD | LVM | IAM | IaC | Elastic | Firewall | Bash | Python
Zeek | GitHub | SSL/TLS | OAuth2.0 | Phishing Analysis | Incident Response | Cloud Security | Automation | High Availability