Thong Huynh

thuynh808@streetrack.org | github.com/thuynh808 | linkedin.com/in/thuynh808 | streetrack.org

EXPERIENCE

LogN Pacific Jan 2026 - Present

Cybersecurity Analyst (Internship)

Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations, contributing to a 100% reduction in critical, 90% in high, and 76% in medium vulnerabilities for the server team
- Performed vulnerability assessments and risk prioritization using Tenable across Windows and Linux environments
- Executed secure configurations and compliance audits (DISA STIG) with Tenable to meet industry standards
- Automated remediation processes and STIG implementations using PowerShell to address critical vulnerabilities

Security Operations:

- Performed threat hunting with EDR, detecting IoCs from brute force attacks, data exfiltration, and ransomware
- Designed, tested, and published advanced threat hunting scenarios for incident response tabletop exercises
- Developed custom detection rules in Microsoft Defender for Endpoint to automate isolation and investigation
- Reduced brute force incidents by 100% by implementing inbound NSG/firewall rules to limit Internet exposure
- Created Microsoft Sentinel dashboards to monitor logon failures and malicious traffic using threat intelligence
- Experienced with KQL (similar to SQL/SPL) which I used to query logs within the SIEM and EDR platform

LogN Pacific May 2024 - Mar 2025

Cyber Security Support Engineer (Internship)

Platform Security Support

- Implemented Azure security controls including Private Endpoints, Network Security Groups (NSGs), and Defender for Cloud, resulting in 87% elimination of security incidents and an 80% reduction in security events
- Supported and troubleshot 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

PROJECTS

Designed and implemented hands-on cybersecurity, cloud, and infrastructure projects, including vulnerability management workflows, threat hunting scenarios, SIEM engineering, cloud security architecture, automation, and compliance hardening.

Portfolio Website: https://www.streetrack.org

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)
CompTIA A+, Network+, Security+, CySA+ | ITIL v4 Foundation

EDUCATION

BS Information Technology - Western Governors University

ADDITIONAL SKILLS AND TECHNOLOGIES

Endpoint Detection and Response (EDR), Vulnerability Management, Risk Prioritization, Vulnerability Remediation, Firewall & NSG, Microsoft Azure, Amazon Web Services (AWS), Azure Virtual Machines, VNets, VM Scale Sets, Azure Storage, AWS EC2, ECS, S3, Microsoft Sentinel, Azure Monitor, Log Analytics, Defender for Cloud, Elastic SIEM, Zeek, Prometheus, Grafana, Loki, SNMP, Syslog. Ansible, Terraform, GitHub Actions, PowerShell, Bash, Python, Linux (RHEL, Rocky Linux, Ubuntu), Windows Server, TCP/IP, DNS, VLANs, 802.1Q Trunking, OSPF, STP, EtherChannel, Routing, NIST 800-53, NIST 800-61, PCI-DSS, HIPAA, GDPR, Windows SecurityEvent, Linux Syslog, KQL, SQL, Dashboards, Troubleshooting