NATHAN LE

(832) 486-0414

contact@nathanle.info · linkedin.com/in/nthnle · github.com/nthnle · nathanle.info

Senior Security Engineer with extensive multi-cloud security experience across AWS, Azure, and GCP, specializing in identity and access management, cloud security posture management, and threat detection and response.
Built scalable solutions to help secure large, multi-cloud enterprise environments spanning hundreds of accounts and subscriptions.

EXPERIENCE

November 2022 – Present

SENIOR SECURITY ENGINEER, SAGENT

- Own identity and access management (IAM) across >70 Azure subscriptions and GCP projects, including role assignments, access reviews, and enforcement of least-privilege principles
- Triage and remediate CSPM findings across multi-cloud environments to reduce misconfiguration risk
- Partner with engineering teams to embed cloud security best practices into Azure and GCP deployments
- Serve as point of contact for cloud security posture across Azure and GCP environments
- Conduct proactive threat hunting and incident investigations across environments
- Build and maintain SOAR playbooks to automate detection and response workflows
- Manage email security posture, including phishing detection, policy tuning, and threat remediation

August 2020 – November 2022

CLOUD SECURITY ENGINEER, S&P GLOBAL (FORMERLY IHS MARKIT)

- Managed organizational deployment of WAF/DNSFW/Shield to more than 250 accounts in AWS
- Ensured security best practices are in place during architectural reviews of a wide variety of application
- Engineered different security solutions based on given requirements
- Created and maintained automated pipelines to collect IOCs from threat intelligence platforms to be used in coordination with WAF/DNSFW/GuardDuty
- Automated data collection pipelines for a centralized graph database and other business intelligence reports that focus on security
- Deployed operational excellence monitoring solution to respond efficiently to job failure/outage
- Responded to Log4Shell/Spring4Shell vulnerabilities by creating a pipeline to extract IP addresses with suspicious indicators from WAF logs and then feed the IPs to a centrally managed WAF block list
- Became a point of contact for security queries and data quality
- Ensured the success of one of the largest mergers of 2020 by assisting the integration of two large organizations and the divestiture of several branches

EDUCATION

February 2020 – November 2020

DIVERSITY CYBER ACADEMY, SANS – ICMCP
GSEC | GCIH | GCFE

August 2017 – May 2020

B.S., COMPUTER INFORMATION SYSTEMS, UNIVERSITY OF HOUSTON
GPA 3.8 | Magna Cum Laude

SKILLS

- Bash, PowerShell, SQL, Python
- AWS, Azure, GCP, Infrastructure as Code, Containerization
- CI/CD, Scripting, Automation, Git
- Threat Hunting, Incident Response, SOAR

CERTIFICATIONS

- GSEC | GCIH | GCFE
- GIAC Advisory Board
- AWS Solutions Architect – Associate | Security Specialty
- Microsoft Certified: Azure Administrator Associate (AZ-104)

HONORS

- SANS - ICMCP: Diversity Cyber Academy Scholarship (2020)
- Chevron Student Scholarship (2019)
- Paul G. Smith, Jr. Scholarship Endowment (2018)
- UH Dean's List
- National Third Prize – MOSWC 2012
- National Consolation Prize – MOSWC 2011