

AUNG B. MHN

CYBER SECURITY SOC ANALYST

(202) 213-1669 | aungmhn03@gmail.com | www.linkedin.com/in/aung-mhn-016ba6287

PROFESSIONAL SUMMARY

CompTIA Security+ certified Computer Engineering Technology graduate with hands-on security operations experience in a regulated banking environment. Investigate endpoint and email threats using Microsoft Defender and Rapid7 InsightIDR, including LEQL queries for log analysis and security investigations. Bring experience in phishing analysis, incident triage, security documentation, and PowerShell automation supporting visibility across 2,800+ enterprise assets.

CERTIFICATIONS

CompTIA Security+ | AWS Certified Cloud Practitioner

TECHNICAL SKILLS

Security tools & log analysis: Microsoft Defender, Rapid7 InsightIDR (SIEM), Rapid7 LEQL, Rapid7 InsightVM, Wireshark, Windows Event Logs, Sysmon, YARA

Security operations: Log analysis, incident triage and investigation, phishing analysis, threat hunting, LDAP reconnaissance detection, MITRE ATT&CK, DMARC

Systems & networking: Active Directory, Windows Server, Entra ID, DNS, DHCP, VPN, Linux

Scripting & automation: PowerShell, Python, REST APIs, SQL, Regex, Git

PROFESSIONAL EXPERIENCE

Technology & Security Operations Intern | STAR Financial Bank

May 2026 - Present

- Investigate endpoint and email threats using Microsoft Defender and Rapid7 InsightIDR, analyzing indicators of compromise and anomalous activity to support security triage.
- Use Rapid7 LEQL queries to search and analyze logs in support of security investigations.
- Analyze phishing campaigns, malicious URLs, email spoofing, and DMARC failures using DNS analysis and sandbox testing to identify threats.
- Create custom YARA detections and author operational runbooks and technical documentation to support security investigations and consistent analyst workflows.
- Develop PowerShell scripts and REST API integrations to reconcile inventory across 2,800+ enterprise assets; build vulnerability KPI reports and remediation tracking workflows.
- Analyzed network traffic using Wireshark to investigate potential distributed denial-of-service (DDoS) activity.
- Investigated security events using Windows Event Logs and Sysmon to identify suspicious activity.

Associate Banker | JPMorgan Chase

February 2024 - May 2026

- Investigated account and ledger discrepancies and escalated exceptions according to regulatory and internal control requirements.
- Processed an average of 80 customer transactions daily while adhering to KYC/AML requirements; maintained zero audit findings.

RELEVANT PROJECT

Active Directory Reconnaissance Detection | LDAP Activity Analysis

- Developed a detection for unusually high LDAP request volumes within short timeframes to flag potential automated enumeration against domain controllers.
- Developed a detection for workstation-originated LDAP activity associated with PowerShell, Command Prompt, Python, BloodHound, and SharpHound to flag potential Active Directory reconnaissance and attack path mapping.

EDUCATION

Purdue University | May 2026

B.S. Computer Engineering Technology | Minor in Information Technology