

DONALD VU

Dallas, TX | donalddvu.com | linkedin.com/in/donalddvu | (682) 256-9869 | donalddvu@gmail.com

PROFESSIONAL SUMMARY:

Security+ certified Data & Operations Analyst pivoting into SOC. Hands-on labs in email header analysis (SPF/DKIM/DMARC), packet analysis (Wireshark/tcpdump), host/service discovery (Nmap), and SIEM investigations with Splunk & ELK/Kibana. 3+ years of Python/SQL/Tableau automation and clear documentation; comfortable investigating known-suspicious activity and identifying indicators across logs and emails.

CERTIFICATIONS

- CompTIA Security+, July 2025

SKILLS

- **Security:** Wireshark, tcpdump, Nmap, Splunk, ELK/Kibana
- **Email security:** Header analysis (From/Return-Path/Received), SPF/DKIM/DMARC, URL/attachment triage — tools: Google Messageheader, MXToolbox, CyberChef, VirusTotal, sha256sum
- **Systems:** Linux/bash; Windows (Event Viewer, UAC/BitLocker)
- **Frameworks:** MITRE ATT&CK, Cyber Kill Chain, Pyramid of Pain
- **Data/Tools:** SQL (BigQuery), Python (pandas), Excel VBA, Tableau/Power BI, Git, JIRA

PROJECTS

TryHackMe - SOC Analyst Training Labs

July 2025 - Present

- **Packets/Discovery:** Wireshark/tcpdump (ARP/TCP, HTTP); Nmap (-sV, -p) → basic misconfigs.
- **Email Threat Analysis (Phishing):** extracted raw headers (From/Reply-To/Return-Path/Received), verified SPF/DKIM/DMARC (Google Messageheader/MXToolbox), inspected/decoded URLs (CyberChef), and checked link/attachment reputation (e.g., VirusTotal); captured IOCs (domains/IPs/URLs/hashes) from known-suspicious emails.
- **SIEM — Monitoring & Detection:** scoped by index/sourcetype, extracted fields, and used stats/timechart/table + time/keyword/alert-signature filters to examine known-suspicious auth/VPN events and pinpoint the fields/values that raised suspicion.

WORK EXPERIENCE

CoreLogic

Irving, TX

Data Analyst

December 2023 - May 2025

- Built Python + SQL (BigQuery) + VBA automations for client process: streamlined queue triage, standardized notifications, and improved SLA tracking.
- Developed a multi-client constraints-based BigQuery tool to speed investigations and on-demand data pulls; authored runbooks for operations handoff.
- Developed Tableau dashboards used by cross-functional teams to monitor client servicing timelines, data request turnaround, and operational KPIs.
- Partnered with stakeholders to troubleshoot data issues and validate fixes; documented workflows to reduce repeat tickets.

Business Operations Analyst

August 2021 - December 2023

- Served as Subject Matter Expert for the Service Transfer Process, overseeing accurate onboarding and data migration of new client accounts.
- Led tool training and created internal documentation to help team members quickly adopt and understand reporting workflows.
- Delivered operational reports and created internal docs/training to standardize reporting workflows across the team.
- Identified process inefficiencies and implemented improvements that reduced turnaround times.

EDUCATION

University of Texas at Arlington

Arlington, TX

Bachelor of Science in Management in Information Systems

3.56 GPA

- Organizations/Awards: Sports Coordinator for Filipino Student Association (FSA), Dean's List