Anthony Bayate Jr.

Cranford, NJ |908-587-6782 | anthonybayate@outlook.com | linkedin.com/in/abayate/ | github.com/abayate

EDUCATION

Kean University | GPA: 3.83/4.0 — Union, NJ

Bachelor of Science in **Information Technology**; Concentration in **Cybersecurity** — **Expected May 2027**

- Extracurricular Activities: Tau Sigma National Honor Society, Vice President of Association for Computing Machinery (ACM), WiCyS, Center of Cybersecurity Member, NextGen Cyber Association Club Member, NJ SECON2025, Kean Hackathon 2025
- Relevant Coursework: Network Technology; Unix/Linux; Web Client-Side Programming; IT Data Structures (Java); CS Transfer Introduction (Secure Shell).

PROJECTS

Build and Maintain a Cybersecurity Home Lab | Virtualization, Kali Linux, Splunk Enterprise, Windows 10, Network Reconnaissance

- Configured a virtualized cybersecurity lab using Oracle VirtualBox with Kali Linux (attacker) and Windows 10 (target) on an internal network.
- Conducted network reconnaissance using Kali Linux to identify open ports on the Windows machine, leveraging Splunk Enterprise for real-time log monitoring and threat analysis.
- Demonstrated practical skills in penetration testing, network security, and log management

Secure Virtual Network Monitoring Lab | VMware Workstation, pfSense, Splunk Enterprise, Linux, Windows 10, SSH, Log Monitoring

- Engineered a segmented network environment with pfSense to control traffic and simulate perimeter security for internal systems.
- Created custom firewall rules enabling ICMP and SSH (port 22) communication, then validated rule enforcement through simulated attacks and secure logins.
- Installed and configured Splunk Enterprise to ingest and analyze over 1,000 syslog entries, successfully detecting and alerting on failed SSH logins and sudo activity within seconds.

AWS Cloud Security Operations (SOC) Simulation Lab | Amazon EC2, Amazon GuardDuty, AWS Security

- Built a cloud-based SOC lab replicating an enterprise security environment to simulate detection and response processes.
- Simulated over 350 threat events (SSH brute force, IAM reconnaissance, crypto mining), validating alerts in GuardDuty and Security Hub with 100% detection accuracy.
- Installed diagnostic tools (nmap, tcpdump, stress) and conducted tests that confirmed end-to-end visibility into attack behavior and system responses.

WORK EXPERIENCE

Bytehounds LLC — New York, NY

Junior Digital Forensics Incident Response (DFIR) Intern — **April 2024 – Present**

- Conduct forensic imaging and analysis of 15+ electronic devices using digital forensics tools such as Magnet Axiom, Cellebrite UFED 4PC, Cellebrite Physical Analyzer and Digital Collector, ensuring accurate and reliable evidence collection.
- Review account logins in support of many unauthorized access investigations by analyzing sign-in log data in Microsoft Excel, using IPinfo and MaxMind to geolocate IP addresses, detect suspicious activity (e.g., impossible travel), and document detailed forensic notes for future examiner review.
- Implement and utilize CrossTrax: Case Management Software, to manage 7-10 digital forensics cases monthly, streamlining case creation processes and reducing completion time by 90%.
- Collaborate closely with leadership in a startup environment to develop standard operating procedures (SOPs), explore automation opportunities, and implement more efficient solutions across various operational tasks and company processes.