JULIAN SILVA-ERAZO

New York, NY | julian.silva@jjay.cuny.edu | 929-710-8090 | linkedin.com/in/julian-silvaerazo | github.com/Julznyc12

EDUCATION

John Jay College of Criminal Justice

B.S. Computer Science & Information Security

Expected Graduation: December 2026 | GPA: 3.3

Relevant Coursework: Digital Forensics, Network Security, Computer Security, Cryptography, Linux Administration, Incident Response

DFIR & TECHNICAL SKILLS

Digital Forensics: Windows Registry Analysis, Registry Explorer, Windows Prefetch, Jump Lists, Browser Forensics, Cloud Forensics, SQLite Viewer, Timeline Reconstruction

Incident Response: Alert Triage, IOC Identification, Threat Hunting, Log Analysis, Security Event Investigation

Security Tools: Splunk, Suricata, Wireshark, Nmap, tcpdump, VirtualBox

Systems: Active Directory, Linux, Ubuntu, LDAP, Kerberos, RADIUS, Group Policy (GPO)

Programming: Python, Bash, SQL, C/C++

Automation & AI: n8n, Hugging Face, Groq LLMs, Random Forest, Isolation Forest

Certifications: CompTIA Security+ (In Progress), CodePath CYB102

EXPERIENCE

Security Automation Engineer Intern

John Jay College | Feb 2026 – Present

- Developed AI-assisted security workflows using n8n and Hugging Face models to process and classify security alerts
- Designed SOC-style enrichment pipelines using severity scoring and confidence-based alert classification
- Implemented state-tracking logic to prevent duplicate processing across automated investigations

Security Analyst Trainee

CodePath CYB102 | May 2025 – Aug 2025

- Conducted alert triage and traffic analysis using Splunk and Wireshark in SOC-style environments
- Investigated DDoS and brute-force attack scenarios while identifying indicators of compromise (IOCs)
- Performed packet inspection and log analysis to identify anomalous network activity

PROJECTS

AI-Powered Intrusion Detection System

Python, Suricata, Splunk | Feb 2026 – Present

- Developed a hybrid intrusion detection system combining Suricata monitoring with machine learning-based attack detection
- Built Python pipelines to parse Suricata eve.json logs and extract IP addresses, signatures, severity levels, and attack activity
- Investigated IDS alerts and reconstructed attack behavior through Splunk-based log analysis and traffic monitoring
- Designed Splunk dashboards to monitor 1,000+ security events and identify suspicious network behavior
- Conducted DDoS simulations using Apache Bench while monitoring system activity through Splunk, tcpdump, and htop
- Implemented Random Forest and Isolation Forest models to support malicious traffic classification and anomaly detection

Digital Forensics & Artifact Analysis Labs

Windows & Browser Forensics | Jan 2026 – Present

- Performed forensic analysis of Windows artifacts including Prefetch files, Jump Lists, Registry hives, and browser databases
- Used Registry Explorer and SQLite Viewer to reconstruct user activity, browser history, and forensic timelines
- Conducted timeline reconstruction and artifact correlation during simulated DFIR investigations involving removable media activity
- Analyzed browser and cloud-based artifacts to support investigative workflows and evidence reconstruction

Threat Intelligence Automation Pipeline

n8n, Hugging Face, Groq LLM | Mar 2026 – Present

- Designed a multi-model automation pipeline for threat intelligence enrichment and alert classification
- Integrated Hugging Face models and Groq-hosted Llama 3 models into n8n workflows for automated security analysis
- Processed structured threat intelligence alerts and exported enriched results into Airtable dashboards for investigation tracking