

Idus Erediauwa

23 Menahan Street, New York, NY | (917) 683-2814 | Email: iduseredia@gmail.com |
Web: [linkedin.com/in/iduseredia](https://www.linkedin.com/in/iduseredia) | Portfolio: github.com/iduredia97

PROFESSIONAL SUMMARY

Dedicated analyst passionate about strengthening information security by leveraging penetration testing, incident response, and SIEM analysis to detect and mitigate threats. I'm bringing a multidisciplinary academic background, specializing in Data-driven Analysis, Identity Access Management (IAM), Governance Risk & Compliance (GRC), Networking, Security Operations and System Administration. Proficient in proactively identifying and neutralizing cyber threats to protect organizations and individuals from financial harm. Guided by a strong commitment to ethical standards and problem-solving, I strive to help organizations achieve their security goals by safeguarding networks, implementing secure IT infrastructure, and mitigating risks effectively. Currently strengthening expertise with CompTIA Security+ to reinforce risk management and security operations expertise.

EDUCATION

Bachelor of Science (BSc) | Finance

Lancaster University, UK | July 2019

- **Honors & Awards:** Dean's List (2019); Economics Honor Society; Teaching Fellow Award
- **Relevant Coursework:** Mathematics, Statistics, Data Analytics, Financial Analysis and Modelling, Economics, Accounting Information Systems (AIS)

CERTIFICATIONS & PROFESSIONAL TRAINING

- CompTIA Security+ (In Progress, expected 09/25)
- Splunk SIEM Bootcamp (ThinkCloudly, 2025)
- IBM: Introduction to Cybersecurity Tools & Cyber Attacks (2024)
- Northwestern University Cybersecurity Bootcamp (2023–2024)
- Google Cybersecurity Professional Certificate (2023)

PROFESSIONAL EXPERIENCE

I currently have 6 years of experience in customer support. I've worked at institutions such as the NYC Department of Education, Sapphital Learning Technologies, New York Medical Clinic and Unilever. My most recent relevant technology experiences are below.

Company: New York Medical Clinic

Title: IT Analyst

Brooklyn, NY | Nov 2023 – Sept 2025

- Maintained, managed, and secured electronic health record (EHR) systems and other critical clinical software and hardware, ensuring HIPAA compliance and reliable system operations
- Supported the rollout of role-based access controls (RBAC) in EHR and billing systems, ensuring least-privilege access in compliance with HIPAA
- Processed 200–300 identity lifecycle requests daily (onboarding, transfers, deprovisioning) using Entra ID (Azure AD), Broadridge IDM, and CyberArk.
- Assisted with refining IAM policies and procedures to align with NIST CSF and HIPAA requirements, improving compliance posture by 35%
- Built and maintained dashboards tracking IAM KPIs such as provisioning times and ticket closure rates, helping identify and resolve access control issues
- Participated in HIPAA and internal audits, collecting and presenting IAM evidence and contributing to a 100% remediation rate in the 2024 audit cycle
- Delivered cybersecurity awareness sessions (including phishing simulation results) that led to a 22% improvement in staff phishing resistance
- Documented IAM security control findings and collaborated with leadership on improvements in account hygiene and RBAC coverage
- Maintained confidentiality when provisioning access to sensitive systems, following strict data classification and custodianship protocols
- Provided staff training and ongoing support on software and IT systems, improving workflow efficiency and proper system utilization
- Compiled, organized, and secured patient and financial data, ensuring data accuracy, accessibility, and privacy protection
- Analyzed clinic workflows and system data to identify improvements, enhancing patient care and operational effectiveness
- Monitored cyber operations and website systems, actively pursuing cybersecurity skills to strengthen data protection and digital infrastructure security

Company: Sapphital Learning Group

Title: Business Analyst (IT) / System Administrator

New Castle, Delaware | Sept 2020 – Present

- Delivered Tier 1 and Tier 2 technical support for 200+ end users across the architectural design and product management teams, resolving 95% of tickets within SLA
- Managed support workflows using Jira Service desk, logging and tracking tickets with detailed root cause documentation
- Installed, configured, and troubleshoot high-demand software and hardware, diagnosing and resolving technical issues, recommending software solutions, and coordinating with vendors to maintain system uptime and operational efficiency
- Developed internal KPIs and performance dashboards using Jira insights and Excel, achieving a 20% rise in employee satisfaction with support services through targeted improvements

Company: Sapphital Learning Group

Title: IT Analyst: Graduate Scheme (DevOps Pathway)

New Castle, Delaware | Sept 2019 – Aug 2020

- Gained rotational experience in IT support, systems administration, and business analysis
- Contributed to GRC implementation and IAM exposure during DevOps projects

Company: Tata

Title: Cybersecurity SOC Analyst

(Simulated on Forge) | July 2025

- Collaborated with a Cybersecurity Consulting team to deliver comprehensive documentation and presentations, showcasing the ability to communicate complex technical concepts effectively
- Acquired expertise in IAM principles, cybersecurity best practices, and strategic alignment with business objectives

Company: AIG

Title: Cybersecurity Analyst

(Simulated on Forge) | July 2025

- Completed a cybersecurity threat analysis simulation for the Cyber Defense Unit, staying updated on CISA publications
- Researched and understood reported vulnerabilities, showcasing analytical skills in cybersecurity
- Drafted clear and concise emails to guide teams on vulnerability remediation
- Utilized Python skills to write a script for ethical hacking, avoiding ransom payments by bruteforcing decryption keys

Company: Mastercard

Title: Cybersecurity Analyst

(Simulated on Forge) | July 2025

- Served as an analyst on Mastercard's Security Awareness Team
- Helped identify and report security threats, including phishing
- Analyzed and identified areas of the business that needed more robust security training and implemented training courses and procedures for the team

PROJECTS

Project: **SIEM Implementation & Log Analysis**

Source: github.com/iduredia97/Security-Audit

Platforms Used: Splunk, Windows Server, Ubuntu Server — Built homelab for centralized log collection and AD security event analysis.

Project: **Network Design & Security Integration**

Source: github.com/iduredia97/Merged-Whisper-Security-Network-Design-Security-Integration

Platforms Used: Windows Server, pfSense, Splunk — Designed enterprise network with integrated monitoring and layered defenses.

Project: **SOC Automation (SOAR, Workflows, Case Management)**

Source: github.com/iduredia97/SOC-Automation-Lab

Platforms Used: Shuffle SOAR, TheHive, Cortex — Automated triage, enriched threat intel, and streamlined incident workflows.

Project: **Incident Response & Threat Analysis**

Source: github.com/iduredia97/Incident-Report-Analysis

Platforms Used: Splunk, Windows Event Viewer, PowerShell — Investigated suspicious activity and documented incident response.

Project: **Network Traffic Monitoring**

Source: github.com/iduredia97/Detection-Lab

Platforms Used: Wireshark, Kali Linux, Splunk — Simulated cyberattacks to validate IDS/IPS rules and improve detection accuracy

KEY SKILLS AND TECHNICAL COMPETENCIES

- **Identity & Access Management (IAM):** RBAC, SoD enforcement, identity lifecycle automation, least privilege access; tools: Active Directory, Entra ID (Azure AD), CyberArk, SailPoint, RSA SecureID, Broadridge IDM
- **Governance, Risk & Compliance (GRC):** Alignment with NIST CSF, NERC CIP, PCI DSS, ISO/IEC 27001, HIPAA, GDPR, ISA/IEC 62443, CIS Controls
- **Vulnerability & Threat Management:** Nessus, Rapid7, OpenVAS, Wireshark, Suricata, Metasploit, SQLmap, Burp Suite, tcpdump; risk analysis, ethical hacking, incident response, IDS/IPS, threat hunting, network forensics
- **Cloud & On-Premises Security:** Secure architecture, policy implementation, and monitoring using Microsoft Sentinel, Defender for Identity
- **Security Awareness & Audit Readiness:** Phishing campaign metrics, compliance mapping, audit interviews, evidence collection, access reviews, exception tracking
- **Cybersecurity Metrics & Reporting:** SLA fulfillment, KPI tracking, and security breach trends visualization via ServiceNow; executive and regulator reporting, translating technical insights into business context
- **Workflow Automation & Ticketing:** ServiceNow, JIRA, PowerShell scripting for access workflows, compliance tracking, and operational efficiency
- **Programming & Scripting:** Python, SQL, Bash, Java, JavaScript, Kotlin, Swift, R Studio
- **Operating Systems:** Linux (Ubuntu, Kali), Windows (Desktop & Server), macOS

REFERENCES

*Available Upon Request