DANIEL LODI

New York, NY 10016 | dlodi@mail.yu.edu | (929) 751-9887 | LinkedIn

SUMMARY

A proactive cybersecurity and project management professional with practical experience in threat detection, incident response, and vulnerability management. Proven success reducing cyber incidents by 40% through optimizing SIEM platforms. I hold a CompTIA Security+ certification and currently pursuing a MS. in Cybersecurity.

EDUCATION

Yeshiva University, Katz School of Science and Health — New York, NY
Master of Science in Cybersecurity — Expected May 2027

Post-Graduate Diploma, Project Planning & Management — Kampala, Uganda
First Class. — Mar 2025

Makerere University — Kampala, Uganda
Bachelor of Science in Software Engineering — May 2015

PROFESSIONAL EXPERIENCE

Lead Digital Security Analyst — May 2023 – July 2025
Definite Creations LTD, Kampala, Uganda

- Led a team to achieve a 40% reduction in security incidents by optimizing SIEM platforms (Splunk, QRadar) with optimized log correlation for real-time threat detection.
- Mitigated cyber risks with layered security controls (Intrusion Prevention System, End-point Detection and Response), cutting breach pathways by 25% and enhancing incident response by 75% (NIST-aligned).
- Developed and implemented new threat detection logic that increased malware identification accuracy by 20% using Splunk tools.
- Coordinated remediation efforts during security incidents, resulting in faster resolution by 40% compared to previous protocols

Co-Founder & Project Manager — May 2020 – May 2023
Definite Creations LTD, Kampala, Uganda

- Led a 7 member cross-functional team to deliver 15+ web and mobile applications, completing projects on average 15% ahead of schedule and within budget.
- Delivered secure digital infrastructure for SMB's and NGOs by designing cloud-hosted systems with encryption, and backup controls.
- Built a digital agency from the ground up, growing the team to 8 and increasing client base by 70% over 5 years, delivering digital solutions across Uganda and the East African region.

Manager, Information Systems — July 2017 – March 2020
Uganda Energy Credit Capitalisation Company, Kampala, Uganda

- Delivered IT training and capacity-building, boosting staff digital proficiency by 30% and reducing external IT support costs by 25%
- Performed threat detection and remediation on 200+ endpoints using Wazuh endpoint security and network monitoring tools, preventing breaches and enhancing response efficiency.

- Coordinated assessment of system vulnerabilities , leading to the implementation of safeguard measures across multiple platforms

PROJECTS

Enterprise Security Monitoring and Threat Detection using Wazuh SIEM Fall 2025

- Deployed and configured a Wazuh-based SIEM and EDR environment on VirtualBox (Ubuntu 22.04 + Windows 10 agent) to enable enterprise-grade security monitoring, log analysis, and real-time threat detection; integrating File Integrity Monitoring, vulnerability detection, and MITRE ATT&CK-based rule mapping.
- Simulated and analyzed real-world attack scenarios (brute-force and PowerShell misuse) to generate actionable alerts and CVE vulnerability reports, demonstrating proficiency in SOC operations, security event correlation, and dashboard visualization using Wazuh v4.14.0 and Sysmon.

Deloitte Cybersecurity Management Forage Simulation Spring 2025

- Analyzed 100+ security logs during a data breach, mapped findings to NIST CSF, and strengthened simulated threat detection.
- Implemented RBAC aligned with ISO 27001, reducing unauthorized access by 70% and enhancing system resilience.

Network Analysis with WireShark Spring 2025

- Captured and analyzed real-time network traffic to detect anomalies, unauthorized access, and suspicious connections.
- Generated PCAP reports and extracted indicators of compromise (IOCs) for further investigation. https://github.com/lodidannie/Network-Forensics-Investigation

Vulnerability Management with Nessus Fall 2025

- Performed vulnerability assessments using Nessus in a home lab, analyzing CVSS scores to identify, categorize, and prioritize security risks across systems.
- Documented findings and recommended risk-based remediation strategies, aligning with security best practices and governance frameworks to improve overall security posture.

SKILLS & CERTIFICATIONS

Skills: Threat Detection, Vulnerability Assessment, Incident Response, Network Security, Security Architecture, Risk Management, Penetration Testing, Ethical Hacking, SIEM (Security Information and Event Management), Firewalls, Zero Trust Architecture

Certifications:

- CompTIA Security+ Oct 2025
- ISC2 – Certified in Cybersecurity July 2025

Programming: PHP, MySQL, Python, Javascript, HTML, CSS, WordPress, Drupal.
Tools: Metasploit, Burpsuit, Nessus, WireShark, Splunk, Wazuh, MS Project, Cyberbit, Canva, MS Office Suite