# Neel Upadhyay

647-224-2484 • neelmu12@gmail.com • LinkedIn • GitHub • Brampton, Ontario

## SUMMARY

Software Engineering student (Cybersecurity Stream) at York University with hands-on experience in SIEM deployment, threat detection, vulnerability assessment, and cryptographic security controls. Proven ability to execute end-to-end security assessments — penetration testing, incident analysis, and risk remediation documentation — aligned with NIST CSF and MITRE ATT&CK, with strong awareness of compliance and risk management requirements in regulated financial environments.

## TECHNICAL SKILLS

**Languages:** Python, Java, C/C++, SQL, Bash, Verilog
**Security Tools:** Wireshark, Nmap, Hydra, John the Ripper, Metasploit, SQLMap, Kali Linux, OpenSSL, GPG
**SIEM & Detection:** Splunk, ELK Stack, SOC Analysis, Threat Hunting, MITRE ATT&CK, Network Traffic Analysis
**Cryptography:** AES-128 (hardware), Double Ratchet / Signal Protocol, KDF Chains, OpenSSL, GPG
**Cloud & DevOps:** AWS EC2, Docker, REST APIs, WebSockets
**Platforms & Tools:** Jira, Confluence, Git, Linux/Unix, Kali Linux, WSL, Bash Scripting
**Frameworks:** NIST CSF, MITRE ATT&CK, Vulnerability Assessment, Threat Intelligence, Malware Analysis
**Certifications:** Google Cybersecurity Certificate (2025), CompTIA Security+ (2026), AWS Cloud Practitioner (2026), Java HackerRank (2024), Blue Team Level 1 (2026)

## WORK EXPERIENCE

**TJX Companies — Mississauga, ON** **Sept 2024 – Dec 2024**
**Real Estate Market Analyst Co-op**

- Automated data validation and reporting workflows in Python, improving data accuracy by 15% — strengthening data integrity practices relevant to compliance reporting environments.
- Analyzed multi-source market datasets (population, competitor, demographics) to produce risk-assessed trade area expansion recommendations for senior stakeholders.
- Designed Excel dashboards consolidating store-level KPIs, enabling data-driven retention and relocation decisions across the real estate portfolio.

**Manefa Contracting Inc. — Brampton, ON** **June 2021 – Aug 2022**
**Software Developer Intern**

- Built a Java application with SQL backend to automate material cost tracking, reducing manual entry errors by 60% and enforcing data integrity controls across project records.
- Developed real-time Excel dashboards for project forecasting, improving operational efficiency by 30% and enabling proactive risk identification for project managers.

## PROJECTS

**Cybersecurity Home Lab — SIEM & Threat Detection | Splunk, ELK Stack, Nmap, Hydra, MITRE ATT&CK** **2025 – 2026**

- Deployed Splunk and ELK Stack to ingest Windows/Linux logs; simulated adversarial activity (Nmap reconnaissance, SSH brute-force, credential stuffing) on controlled lab targets.
- Mapped attacker behavior to MITRE ATT&CK TTPs (Reconnaissance, Credential Access, Lateral Movement) via timeline correlation and custom detection rules — replicating enterprise SOC analyst workflows.

**Web Application Penetration Test & Remediation | SQLMap, Python, SQL, Parameterized Queries** **2025 – 2026**

- Conducted a structured penetration test against a personal full-stack application using SQLMap, identifying blind and error-based SQL injection vulnerabilities in live query execution paths.
- Remediated all findings with parameterized queries and input validation; documented the full attack-and-fix cycle in a formal penetration test report aligned with industry standards.

**Double Ratchet Secure Messaging Protocol | Python, Diffie-Hellman, KDF Chains, AES** **2025 – 2026**

- Implemented Signal's Double Ratchet protocol from scratch, combining DH key exchange with KDF chains to derive unique ephemeral session keys per message — enforcing forward secrecy and break-in recovery.
- Validated forward secrecy guarantees through key compromise scenarios, confirming past sessions remained protected and future sessions recovered automatically after each ratchet step.

**AES-128 Hardware Encryption — FPGA | Verilog, DE10-Lite FPGA, RTL Design** **2025 – 2026**

- Implemented AES-128 encryption/decryption at the RTL level in Verilog on a DE10-Lite FPGA, including SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations.
- Architected modular security hardware — ALU, key-expansion module, RAM storage, and FSM controller — with switch-based I/O for plaintext input, key generation, and memory addressing.

**Wireshark Network Traffic Analysis | Wireshark, TCP/IP, DNS, HTTP, ARP** **2025 – 2026**

- Captured and dissected live traffic to detect unencrypted credentials, ARP spoofing indicators, and anomalous sessions via deep packet inspection across TCP, DNS, and HTTP layers.
- Built detection intuition for anomaly-based network analysis, directly applicable to SIEM alert-tuning, threat hunting, and incident triage workflows in enterprise security operations.

## EDUCATION

**Lassonde School of Engineering — York University** **Sept 2022 – Dec 2026**
Honours Bachelor of Engineering, Software Engineering | Cybersecurity Stream