**EDUCATION**

**Seneca Polytechnic**  **Graduation: 2025**

Diploma in Computer Programming (CPA)

* **Database Management System (C++):** Designed and implemented a command-line interface for adding, removing, editing, and managing an existing database using C++ programming.
* **Interactive Web Application:** Developed a dynamic, small-scale database using HTML, CSS, and JavaScript to display data interactively with a cohesive user interface.
* **Portfolio Website:** Built a personal portfolio website from scratch to showcase education, skills, and projects using HTML, CSS, and JavaScript.
* **Software Development Concepts:** Demonstrated knowledge of software development lifecycle by creating use case diagrams using Visual Paradigm for system modeling

**TECHNICAL SKILLS**

**Cybersecurity Skills:** SIEM (Splunk, Chronicle), Network Security & Firewalls, Incident Response & Threat Analysis, Log Analysis & Packet Analysis (Wireshark), Cyber Threat Intelligence (CTI) frameworks

**Programming Languages:** JavaScript, Java, C/ C++, Python

**Frameworks and Databases:** React, React.js, Node.js, Next.js, MySQL, MongoDB

**Web Development:** HTML, CSS, XML

**Tools & Platforms:** Git, Wireshark, Nmap, Linux (Kali)

**RELEVANT CERTIFICATION**

**Google CyberSecurity Certificate (***Issued by Google, Coursera***)** **03/2025**

* Gained hands-on experience in security operations, incident response, and risk management.
* Developed practical skills in threat detection, mitigation, and log analysis.

**CompTia Sec+ Certification (In Progress)** **04/2025**

* Studying **network security, cryptography, risk management, and security operations**.
* Gaining hands-on experience with **threat detection, incident response, and security best practices**.

**PROJECTS**

**Automated System Diagnostics Tool (PowerShell/Bash/Python)**  **2025**

* Created a script that checks system health, monitors CPU/memory usage, and detects issues.
* Includes automated logs and troubleshooting suggestions.
* Skills: PowerShell, Bash, Python, Windows/Linux troubleshooting

**Network Traffic Analysis with Wireshark and tcpdump 2025**

* Used **Wireshark** to capture and analyze **500+ network packets** for suspicious activity.
* Identified and mitigated a simulated **malware infection** by tracing unusual traffic patterns and isolating affected systems.
* Skills: Wireshark, Network Security, Incident Response

**Vulnerability Assessment & Risk Mitigation 2025**

* Used **Nmap** to scan a test environment for security vulnerabilities.
* Assessed **risk levels** and proposed security **hardening measures** based on **CIS benchmarks**.

**Incident Investigation using SIEM (Splunk/Chronicle SIEM) 2025**

* Investigated a simulated phishing attack using **Splunk SIEM**, analyzing **50+ log entries** to detect malicious activity.
* Identified **Indicators of Compromise (IoCs)**, such as suspicious IP addresses and unauthorized login attempts.
* Documented findings and proposed mitigation strategies, reducing future risk by **30% in a simulated test environment**.

**Personal Online Portfolio**  **2025**

* Created an online portfolio showcasing personal projects, technical skills, and interests using HTML, CSS, and JavaScript. The portfolio offers detailed insights into my capabilities, serving as a dynamic representation of my professional background and achievements.
* GitHub Link: https://github.com/UnclElmino/unclelmino.github.io