Neel Soni

Guelph, ON N1L 0J2 | sonineelp@gmail.com | (647) 919-8283 | linkedin.com/in/sonineelp

Professional Summary

Master's student in Cybersecurity and Threat Intelligence with strong academic foundation and practical experience in penetration testing, malware detection, digital forensics, secure communication, and Artificial Intelligence. Utilize industry tools such as Metasploit, Wireshark, and SIEM platforms, with a strong inclination towards applied research. Collaborated on group research, led technical initiatives, and participated in hands-on labs simulating real-world attacks. Dedicated to protecting systems and proactively mitigating emerging cyber threats.

Education

Master of Cybersecurity and Threat Intelligence
University of Guelph, Guelph, ON — Expected Jan 2026

Graduate Certificate in Information Security Management
Fanshawe College, London, ON — Dec 2024
GPA: 3.59

Bachelor of Technology in Computer Science and Engineering
Navrachana University, Vadodara, Gujarat, India — May 2021

Technical Projects

ArXiv Paper Summarizer using Multi-Agent AI System — Jun 2025 – Jul 2025

- Developed a multi-agent research assistant using Microsoft's AutoGen framework to automate literature reviews from arXiv.
- Designed two specialized agents: a search agent for querying arXiv using FunctionTool and a summarizer agent for generating structured Markdown-based reviews.
- Implemented coordination through a RoundRobinGroupChat to allow agents to communicate and divide responsibilities effectively.
- Built using Python libraries including autogen, arxiv, dotenv, openai, and asyncio for deployment.
- Demonstrated modular, task-driven AI agent orchestration with applications in intelligent assistants and autonomous research tools.

Hybrid Malware Detection with Explainable AI (SHAP) — May 2025 – Jun 2025

- Developed a malware classification system by combining static (EMBER) and dynamic (CIC-MalMem) features into a hybrid dataset of ~850,000 samples and 2,400+ dimensions.
- Applied PCA to reduce dimensionality while preserving 98% variance, and used SMOTE to address class imbalance.
- Trained models including XGBoost, LightGBM, and MLP; XGBoost achieved 96.1% accuracy and 0.991 ROC AUC with hyperparameter tuning.
- Used SHAP for post-hoc explainability to identify the most influential features and interpret PCA components.

- Visualized feature contributions through SHAP summary, bar, and force plots for transparent model behavior.

Exploit Development and Vulnerability Assessment Jan 2025 – Apr 2025

- Exploited buffer overflow vulnerabilities in user programs using custom payloads for local privilege escalation.
- Employed gdb for analyzing call stacks and memory to craft return-to-libc and shellcode-based attacks.
- Conducted vulnerability scanning using OpenVAS and Nessus, and scripted fingerprinting using Nmap NSE.
- Used Metasploit to automate post-exploitation tasks such as credential dumping and persistence.

Cryptographic Libraries and Secure Communications Feb 2025 – Mar 2025

- Designed secure message exchange protocols using OpenSSL, demonstrating symmetric and asymmetric encryption.
- Developed Python implementations for AES in ECB, CBC, and GCM modes, analyzing implications for confidentiality and integrity.
- Performed RSA key generation, encryption/decryption, and signature validation.
- Investigated vulnerabilities from key reuse, improper padding, and insecure stream cipher configurations.

Web Application Security Testing (SEED Labs) Jan 2025 – Apr 2025

- Performed black-box and white-box testing on intentionally vulnerable apps using SEED Labs.
- Identified and exploited XSS to steal cookies, CSRF to force unauthorized state changes, and SQLi to bypass authentication.
- Crafted PoC payloads using curl, Burp Suite, and browser-based JavaScript injections.
- Suggested mitigation strategies such as content security policy, CSRF tokens, and input validation.

Publications

OpCode-Based Malware Classification Using Machine Learning and Deep Learning Techniques
Neel Soni, Varij Saini, Rudraksh Gupta
arXiv preprint: arXiv:2504.13408, April 2025

Research Projects

APT Analysis and AI-Based Detection for Cyber Threat Intelligence (Group Project) Jan 2025 – Mar 2025
*CIS*6530 - Threat Intel & Risk Analysis | University of Guelph*

- Researched 40+ state-sponsored Advanced Persistent Threat (APT) groups.
- Developed structured TTP profiles using OpenCTI for threat modeling.
- Collected malicious payloads, reverse-engineered samples using GHIDRA, and extracted opcode-level features.
- Engineered machine learning models (SVM, KNN, Decision Tree) on 1-gram and 2-gram opcode sequence analysis.

- Implemented a CNN model based on academic literature and compared performance with traditional models.
- Evaluated results using accuracy, precision, recall, F1-score, and confusion matrices, with comprehensive visualization.

Analyzing Penetration Testing Practices for Autonomous Vehicles – A Qualitative Meta-Synthesis
Capstone Project | Fanshawe College | Sept 2024 – Dec 2024

- Systematically reviewed research literature from 2010 to 2023 from IEEE Xplore, ScienceDirect, and other repositories.
- Identified recurring vulnerabilities in autonomous vehicle systems including sensor spoofing, V2X protocol attacks, and software logic errors.
- Applied thematic coding methodology to extract patterns and gaps in penetration testing approaches across different studies.
- Highlighted inconsistencies in tools and evaluation techniques, emphasizing the need for standardized penetration testing frameworks for AVs.
- Proposed a unified model leveraging AI-based adaptive fuzzing and behavioral anomaly detection for real-time AV system assessment.

Skills

Cybersecurity: Penetration Testing, Threat Intelligence, Vulnerability Assessment, SIEM (Splunk, Elastic), YARA, IDS/IPS, Network Scanning, Log Analysis, Metasploit, Burp Suite, Nmap, OpenVAS, Nessus, Wireshark

Programming & Tools: Python, Bash, Regex, JavaScript, Git, GHIDRA, Linux (Kali, Ubuntu), Windows, Mac OS, Data Science (Keras, TensorFlow), Azure, AWS, GCP, Prompt Engineering (LLMs)

Soft Skills: Technical Writing, Public Speaking, Team Leadership, Mentorship, Problem-Solving, Collaboration, Adaptability, Eager to learn

Work Experience

Sales Associate, *Sai Krupa Jewellers, Vadodara, India* Jul 2021 – Mar 2024

- Delivered customer service, managed billing, and maintained store operations.

Web Developer – Freelance, *Various Clients (India)* 2021 – 2023

- Developed and maintained websites for various clients including healthcare and consulting firms.
- Improved page load speed by 40%, and managed secure payment integration.
- Performed cross-browser testing, SEO optimization, and performance monitoring.

Volunteer Leadership & Community Involvement

Chapter Leader, OWASP WWW Chapter – University of Guelph Apr 2025 – Present

- Co-leads chapter operations; organizes workshops, CTFs, speaker sessions, and training events.
- Encourages peer collaboration, secure coding practices, and real-world skill-building on campus.

Telemedicine Camp Volunteer, A.P. Panchakarma Clinic 2020 – 2021

- Set up digital infrastructure and assisted patients with onboarding and device troubleshooting.

- Helped ensure smooth scheduling and connectivity for virtual consultations.

Festival Organizer, Innuvate University Festival, Navrachana University 2019 – 2020

- Managed stage setup, volunteer scheduling, and audio-visual coordination for multiple events.
- Resolved technical issues and ensured real-time event flow with cross-team coordination.