Mohamed Elsaban

+1 519-400-0441 | mohamedelsaban@cmail.carleton.ca

Technical Skills

Cybersecurity & Intelligence Tools: OSINT Framework, theHarvester, Shodan, Hashcat, John the Ripper, Wireshark, Nmap, Burp Suite, Metasploit Framework, Kali Linux, **Splunk**, Suricata, Zeek
Languages: Python, Java, JavaScript, C/C++, HTML, CSS
Technologies: Node.js, Express.js, Flask, AWS Basics, Elastic Stack, PowerShell
Developer Tools: Git, Docker, MySQL, VS Code, IntelliJ, Microsoft Office suite, Jira Service Desk

Experience

Technical Solutions Lead Oct 2024 – Present
Office of Risk Management, Carleton University *Ottawa, ON*

- Collaborated with **cybersecurity leadership** to map log correlation patterns from risk notifications, reducing false positives by **15%**.
- Authored **incident notification runbooks** aligning Carleton's environment with NIST CSF, improving escalation clarity for future SOC integration.
- Engaged the **NIST Computer Security Division** for best practices, translating framework guidance into actionable monitoring requirements.
- Leveraged OSINT investigations to enrich alert context, supporting faster triage decisions.
- Handled sensitive data with discretion while supporting university-wide risk initiatives.

Communications Security Lead Jan 2024 – Present
CU On Orbit (Satellite Design Team) *Ottawa, ON*

- Led development of an **encryption and key-rotation schema** for LoRa telemetry, contributing detection use-cases for downlink anomalies.
- Simulated LoRa **signal interception** with SDR to create baseline vs. malicious traffic captures, later replayed in Wireshark for packet analysis labs.
- Produced incident response drill for lost-link scenario, defining alert thresholds and escalation paths for the future ground-station SOC.
- Authored a compliance report mapping satellite comms controls to **NIST 800-53 IR family**.

Projects

Carleton Email Spoofing Detection & DMARC Hardening Spring 2025
Security Case Study

- Identified p=none DMARC policy on `@carleton.ca` allowing spoofed phishing emails; demonstrated exploit to IT Services.
- Parsed **Exim** and O365 transport logs in Splunk to visualize spoofing attempts and propose detection queries.
- Drafted Suricata rules and SIEM search macros to raise Tier-1 alerts on future header anomalies, later adopted in pilot SOC dashboard.
- Authored mitigation plan moving policy to **p=reject** and enabling DKIM alignment; plan accepted for fall roll-out.

Intro SOC Triage Lab (Ongoing) Summer 2025
Independent Blue-Team Development

- Building home-lab using **Splunk Free**, Zeek, and Suricata generating synthetic attacks (Brute RDP, Phishing, DNS tunneling).
- Created Tier-1 playbook for alert triage: verify IOC, correlate MITRE technique, escalate severity.
- Achieved **mean investigation time ¡ 5 min** for 10 common alert scenarios.

Education

Carleton University Sep 2023 – Apr 2028
Bachelor of Computer Science Co-op (Cybersecurity) *Ottawa, ON*

- President's Scholarship

Relevant Coursework: Cryptography, Systems Programming, Web Applications, Incident Response Fundamentals, Data Structures, Discrete Math, Software Engineering