Mursaleen Sakoskar

613-869-3845 | **mursaleensakoskar@gmail.com** | **LinkedIn** | **GitHub** | **Portfolio Website**

Technical Skills

- **Programming:** Python, Go, Bash, PowerShell, C/C++, Java, JavaScript, React, Dart
- **Security Tools:** Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark
- **SIEM & Monitoring:** Splunk Enterprise, ELK Stack, AWS GuardDuty
- **DevSecOps & Automation:** Jenkins, GitHub Actions, Terraform, Ansible, Docker, Kubernetes
- **Data & Logging:** PostgreSQL, Redis, Elasticsearch, Kafka
- **IT Infrastructure & Networking:** Windows Server, Linux Administration, Active Directory, DNS, DHCP, TCP/IP, VPN, VMware

Certifications

- AWS Cloud Practitioner Essentials
- Fortinet Certified Associate Cybersecurity
- IBM Cybersecurity Fundamentals
- Cisco Certified Ethical Hacker (CEH)
- Splunk: Intro to Splunk
- Forage Cybersecurity Simulations (Mastercard, AIG, CommBank)
- Google Cybersecurity Professional Certificate (In Progress)
- CompTIA Security+ (Expected September 2025)

Education

B.Sc. Computer Science, Cybersecurity Specialization; Minor in Statistics *Expected May 2026*
Carleton University, Ottawa, Canada

Experience

Security Operations (Intern) May 2025 – Present
iMatter Global Solutions LLP

- Helped in connecting **AWS CloudTrail** to **Splunk**, shadowed a senior analyst to fine tune login anomaly correlation rules, and wrote a **Python script** that emails the SOC whenever **IAM lockouts** spike.
- Scheduled and analyzed weekly **Nessus scans**, drove **high-severity CVE tickets** from open to closure, and handled daily **phishing triage** (header checks, sandbox tests, sender blocks).
- Added an **OWASP ZAP baseline scan** to the CI pipeline for an internal test portal, filtered false positives with a senior analyst, and filed confirmed issues for developers.

App Developer (Co-op) May 2025 – Present
MVerse Technology Solutions

- Designed and developed a **Flutter/Firebase** mobile application with a **security-first** approach, implementing **OAuth2** authentication, encrypted local data storage, and onboarding **100+ active users**.
- Architected and integrated **REST** and **gRPC APIs** using **FastAPI** and **Node.js**, backed by **PostgreSQL** and **Redis**, enabling sub-200ms real-time data synchronization across services.
- Automated end-to-end **CI/CD pipelines** using **GitHub Actions** and **Jenkins**, adding unit tests with **pytest**, UI tests with **XCTest**, and integration tests in **Appium**.

IT Security Support (Intern) May 2024 – Sept 2024
iMatter Global Solutions LLP

- Captured lab traffic with **Wireshark**, pinpointed a misconfigured DNS server, recommended cache resets, and confirmed faster load times after the fix.
- Ran weekly **Nmap sweeps** of lab hosts, documented exposed ports, helped shut down two legacy services, and re-scanned to verify closure.
- Maintained the team's **asset inventory** (hostnames, patch status, AV dates) and wrote a short **phishing-response cheat sheet** now used in intern onboarding.

Software Tester & Coordinator (Co-op) May 2024 – August 2024
MVerse Technology Solutions

- Collaborated with **U.S.-based company Om Research** as their **software partner**, diagnosing and resolving issues in AI/ML learning models and **data pipelines** to streamline workflows and reduce downtime.
- Conducted **regression, functional, and non-functional testing** to validate model stability, accuracy, bias, fairness, and robustness across updates.
- Documented **test results** and maintained detailed performance records while providing feedback on testability and model improvements.

Projects

Splunk Multi-Cloud Threat Analysis Platform (GitHub link) Dec 2024 – June 2025
AWS, Terraform, Ansible, Splunk, Docker, Python

- Automated provisioning of a multi-account AWS lab environment with **Terraform** and **Ansible**, including **VPCs**, **EC2**, **CloudTrail**, and **Phantom SOAR** integration.
- Executed and replayed **MITRE ATT&CK** techniques via **Python** and **Boto3**, achieving 85% detection accuracy in Splunk with no false positives.
- Containerized the **HTTP Event Collector** pipeline and deployed on **EKS**, delivering a live Splunk dashboard for SOC analysts.

Emergency Mesh Network System (GitHub link) Feb 2025 – Apr 2025
C, Embedded, Raspberry Pi

- Implemented a decentralized mesh network in **C** with **distance-vector routing**, **auto-discovery**, and **signal-quality metrics** for device messaging.
- Developed a **hardware abstraction layer** for simulation (UDP) and Pi (WiringPi, SPI, UART), featuring offline map tiles and GPS integration.
- Secured communications with **MACs**, **XOR encryption**, and **adaptive RF scanning**, ensuring resilience against node failures.