Sohail Ahmed Mohammed

SOC Operations & **Security Automation Specialist**
Location: Hyderabad, India | **Nationality:** Indian
Phone: +91-8801235561 | **Email:** mohammedsohailahmed18@gmail.com
linkedin.com/in/s0ha1l | msohail.pages.dev

PROFESSIONAL SUMMARY

Canadian-trained IT Security Analyst with over 4 years of experience specializing in **SOC Operations**, **Detection Engineering**, and **Security Automation**. Proven expertise in high-compliance North American health-tech environments (LifeLabs), managing complex security stacks including CrowdStrike, Exabeam, ExtraHop, Proof-Point,Forescout, and Qualys. Expert in building custom Python and PowerShell frameworks to automate threat hunting and vulnerability management, consistently reducing manual triage time by up to 95%.

CORE TECHNICAL EXPERTISE

- **Security Operations (SOC):** Alert Triage, Incident Response, Log Analysis, Anomaly Detection.
- **Detection & Automation:** SIEM Parser Development (DLP, UBA, WAF), Python Security Tooling, SOAR.
- **Threat Hunting:** Living off the Land (LotL), Process Impersonation, MITRE ATT&CK Mapping.
- **Vulnerability Management:** Enterprise-wide Scanning (Qualys), Risk Assessment, Remediation.
- **Tools:** CrowdStrike EDR, Exabeam SIEM, ExtraHop NDR, Infoblox DNS Security, Forescout NAC, Imperva WAF, Netskope CASB, Cloudflare WAF, Proofpoint Email Security, Microsoft Entra ID, Cyera DLP, ServiceNow, Qualys VMDR, Intune.

PROFESSIONAL EXPERIENCE

LifeLabs | Toronto, ON, Canada
IT Security Analyst (SOC Operations) Nov 2025 – Present

- Developed 5+ custom SIEM parsers for critical log sources (DLP, UBA, WAF), increasing detection fidelity and coverage by 30%.
- Engineered a Python-based framework to automate threat hunting for LotL and process impersonation, reducing manual triage time by 95%.
- Integrated multi-stage threat intelligence by automating SHA256 hash extraction for bulk enrichment via Virus-Total and OTX APIs.
- Led Forescout NAC hardware refresh, ensuring secure device onboarding and zero-trust access control.
- Implemented automated WAF log downloader and forwarder for SIEM using Python API integration.
- Collaborated with MSSP analysts to refine escalation workflows, reducing false-positive rates by 35%.
- Migrated 70+ certificates from external CA to internal CA, improving management efficiency and reducing costs.

IT Security Analyst Feb 2024 – Nov 2025

- Performed weekly Qualys vulnerability scans on network appliances, identifying 50+ critical vulnerabilities and reducing gaps by 30%.
- Completed 50+ software risk assessments and 40+ server vulnerability assessments prior to production rollout.
- Supported SOC 2 Type II audits for 2024 and 2025 by providing technical evidence and mapping controls.
- Resolved enterprise-wide Intune connectivity issues for 2,000+ endpoints, enabling critical OS upgrades and compliance.
- Developed Selenium-based Python tools to streamline vulnerability reporting, reducing manual triage time by 40%.

IT TVM Analyst (Co-op Student) May 2022 – Aug 2022

- Conducted 20+ vulnerability assessments, resulting in a 20% reduction in identified vulnerabilities.
- Performed device scanning on 4,000+ endpoints to ensure security patch compliance.

Buggy, INABUGGY | Toronto, ON, Canada
General Systems Manager May 2023 – Feb 2024

- Performed security reviews of business mobile applications, identifying and leading remediation of 12+ critical vulnerabilities.
- Engineered system health monitoring solutions using Python and Bash to reduce downtime via proactive alerting.

CERTIFICATIONS

- **GIAC GMON (SEC511):** Continuous Monitoring & Security Operations — Exp. Apr 2029
- **CompTIA Security+** — Exp. Jul 2027
- **ISC2 Certified in Cybersecurity (CC)** — Exp. Dec 2026

TECHNICAL PROJECTS

- **CrowdStrike Threat Hunt Analyzer:** Python script for automated LotL analysis and VirusTotal/OTX API integration.
- **VulScan API:** Cloudflare Workers/D1 RESTful API enriching CVE data with CISA KEV and Exploit-DB metadata.
- **IOC Scanner:** Full-stack web app for automated IOC enrichment across multiple threat feeds.
- **WAF Log Forwarder:** Python script to download logs from Imperva WAF and forwards them to SIEM using API.

EDUCATION

Post-Graduate Certificate in Information Systems Security — Barrie, ON, Canada
Georgian College | *GPA: 4.0/4.0 (Dean's Honors)*

Post-Graduate Certificate in Mobile Application Development — Toronto, ON, Canada
Canadore College | *GPA: 3.8/4.0*

Bachelor of Engineering in Computer Science — Hyderabad, India
Osmania University | *GPA: 3.5/4.0*

LANGUAGES

English: Fluent (IELTS 8) • **Urdu:** Native • **Hindi:** Native

SECURITY LABS, RESEARCH & TECHNICAL INTERESTS

- **Detection Engineering Lab:** Built a virtualized environment using HELK (Hunting ELK) and Sysmon to simulate adversary TTPs and develop custom Sigma rules.
- **Cloud Security Research:** Deploying serverless security tools on Cloudflare and Azure to automate IOC ingestion and reputation scoring.
- **CTF & Learning Platforms:** Active participant in TryHackMe and HackTheBox, focusing on SOC Analyst and Defensive Security pathways.
- **Security Automation:** Developing JavaScript bookmarklets and Python CLI tools to optimize daily SOC workflows and data enrichment.
- **Vulnerability Research:** Monitoring CISA KEV and NVD metadata to build automated CVE lookup tools for rapid response.
- **Threat Intelligence:** Documenting emerging threats and vulnerabilities and sharing them with the security community.