Fatima Al-Rashid

Senior Security Analyst, Incident Response | Security Analyst

fatima.alrashid@email.example • (416) 555-0151

PROFESSIONAL SUMMARY

Cybersecurity analyst with six years in incident response and threat detection for financial services. Leads investigations from first alert to containment and lessons learned, tunes detections in Microsoft Sentinel and Defender, and works with infrastructure teams on fixes that stick. GIAC GCIH certified and holds Government of Canada Secret clearance.

PROFESSIONAL EXPERIENCE

Senior Security Analyst, Incident Response *Apr 2023 — Present*

Bayfront Trust Financial · Toronto, ON

- Led 30 security investigations including a business email compromise, coordinating containment with IT, legal and privacy teams and writing executive summaries.
- Built 25 KQL detections in Sentinel for identity and cloud attacks, tuning each with test data to keep false positives manageable for the SOC.
- Ran quarterly threat hunts based on current threat intelligence, finding an unmanaged server with exposed remote access that infrastructure then retired.
- Wrote and tested the ransomware response playbook with tabletop exercises for IT, communications and executives.

Security Analyst *Jun 2020 — Mar 2023*

Lakeshore Insurance Group · Mississauga, ON

- Monitored SIEM alerts and EDR telemetry for 2,500 endpoints, handling escalations and producing weekly incident reports for the security manager.
- Managed monthly vulnerability scans in Tenable and tracked critical fixes with system owners, shortening the time critical findings stayed open.
- Delivered phishing simulation campaigns and short training for staff, in English and French for the Quebec office.

EDUCATION

Bachelor of Technology, Information Security — Lakeshore Polytechnic University *2020*

SKILLS

Technical: Incident response, Microsoft Sentinel, Microsoft Defender XDR, KQL, Threat hunting, Digital forensics, Malware triage, Azure and Entra ID, MITRE ATT&CK, Vulnerability management, Python, French and English

Certifications: GIAC Certified Incident Handler (GCIH) · Microsoft Certified: Security Operations Analyst Associate · CompTIA Security+