Ashar S. Ahmed

Toronto, ON | ashar@aahmed.org | (647) 328-3346 | U.S. and Canadian Citizen
linkedin.com/in/asharahmed | github.com/asharahmed

February 25, 2025
Bespin Global Hiring Team
Re: Security Analyst, AI SOC Platform

Dear Hiring Team,

I'm applying for the Security Analyst role on the AI SOC Platform team. I've spent the last few years doing detection engineering and incident response at a small scale—building a SIEM, writing the rules, triaging the alerts, writing the playbooks—and I'd like to do that work somewhere it reaches more than a handful of endpoints.

At a healthcare practice where I serve as the sole security advisor, I stood up the entire security program: Wazuh for SIEM and log correlation, MDM and endpoint hardening across the fleet, MFA, DNS filtering, and the IR playbooks that tie it all together. I went from having no visibility to sub-one-hour MTTD. It's small in scale but I own every layer of it, which means I've had to get good at the full loop—onboarding log sources, writing and tuning detection logic, investigating alerts, and closing out findings. On my own time I run a homelab with 20+ containers (Prometheus, Grafana, Loki, CrowdSec, Wazuh) where I break and fix things constantly, which keeps the muscle memory fresh.

Before the security work, I spent a year at the Government of Canada building AWS infrastructure—IAM, S3, DynamoDB, CloudWatch, CloudTrail—with Terraform and Checkov for policy-as-code. I'm used to reading CloudTrail logs and tracing what happened in a cloud environment. I also wrote the security runbooks that got adopted across the org, which ended up earning me the Directors' General Award of Merit.

On the nice-to-have side: I write Python regularly for automation and data wrangling, I build detections with SQL and regex, and I work in Git and CI/CD pipelines daily. I've also been using AI tooling heavily in my security workflow—prompt engineering isn't a buzzword for me, it's just how I work now. Cert-wise, I hold the SSCP, passed the CISSP (Associate of ISC2), and have both the AWS Solutions Architect and Developer Associates, on top of an M.S. in Cybersecurity and a CS degree.

I'm a dual U.S.–Canadian citizen in Toronto, happy to work remotely in NA time zones. Would be glad to talk more about what I could bring to the platform team.

Thanks for reading.

Ashar S. Ahmed