ANKIT BOSE

Cybersecurity Leader | Detection Engineering Architect | Purple Team Strategist

Toronto, Ontario, Canada • ankitbose6622@gmail.com • LinkedIn • GitHub

PROFESSIONAL SUMMARY

Cybersecurity leader with 9+ years of experience architecting enterprise detection engineering, adversary emulation, and automation programs across financial, pharmaceutical, and energy sectors. Builder of MITRE ATT&CK-aligned detection frameworks and detection-as-code pipelines delivering measurable uplift in signal quality (60% improvement) and response efficiency (40% MTTR reduction). Proven leader in scaling high-performance detection teams and driving SOC maturity transformation initiatives.

EXPERIENCE

Manager, Detection Engineering

2022 – Present

PwC Canada

- Architected enterprise-wide detection engineering framework aligned to MITRE ATT&CK across hybrid cloud, endpoint, and identity telemetry.
- Engineered 250+ high-fidelity detections across Microsoft Sentinel, Defender, Splunk, and Chronicle.
- Improved signal-to-noise ratio ~60% through behavioral logic refinement and telemetry normalization.
- Reduced MTTR by ~40% via SOAR automation and playbook orchestration across 10+ enterprise clients.
- Led structured purple team validation program covering 150+ ATT&CK techniques.
- Designed detection-as-code CI/CD pipeline: schema validation, KQL checks, Sigma conversion, and quality gates.
- Built executive ATT&CK coverage heatmaps and detection governance dashboards for C-suite reporting.
- Mentored and scaled multidisciplinary detection, response, and automation teams across three functional units.

Cybersecurity Consultant

2016 – 2022

PwC India

- Delivered SOC transformation engagements across financial and pharmaceutical clients, designing SIEM architectures and custom use-case libraries.
- Conducted threat hunting engagements uncovering stealth persistence and lateral movement activity.
- Acted as L3 escalation SME for SIEM and advanced analytics; led P1 incident investigations and cross-functional response coordination.

SKILLS

Detection Engineering	KQL, Sigma, Detection-as-Code, MITRE ATT&CK Modeling
Platforms	Microsoft Sentinel, Microsoft Defender, Splunk, Google Chronicle, ArcSight, ELK
Automation	SOAR (Sentinel, Chronicle), Playbook Engineering, Workflow Orchestration
Adversary Emulation	Atomic Red Team, Custom Simulation Frameworks
Security Leadership	Team Scaling, Detection Governance, SOC Maturity Uplift
Telemetry & Stack	Palo Alto, Check Point, Sysmon, Security Onion

PROGRAM IMPACT

10+ Enterprise Clients	**20+** Analysts Mentored	**500+** Detections Deployed	**150+** ATT&CK Techniques Validated	**Multi-Cloud** Azure & Hybrid Coverage