

# Mangesh Bhattacharya

[mangesh.bhattacharya@ontariotechu.net](mailto:mangesh.bhattacharya@ontariotechu.net) | Toronto, ON, Canada | [linkedin.com/in/mangesh-bhattacharya](https://www.linkedin.com/in/mangesh-bhattacharya) | [github.com/Mangesh-Bhattacharya](https://github.com/Mangesh-Bhattacharya) | (416) 670-1418

## PROFESSIONAL SUMMARY

Cybersecurity engineer with co-op experience redesigning AWS IAM under a Zero Trust, least-privilege model, building automated SIEM/EDR detection pipelines, and embedding security controls into CI/CD and patch-management workflows. Master's candidate in Information Technology Security with an AI specialization (Ontario Tech University), applying ML/AI research to threat detection, anomaly analysis, and security automation. Comfortable working across the SDLC, from Active Directory attack-path and privilege-escalation analysis to writing detection logic, automating vulnerability remediation, and partnering with engineering teams to make the secure path the easy path. CEH and CCSK-certified.

## CORE COMPETENCIES

**Cloud & Identity Security:** AWS IAM least-privilege redesign, Zero Trust architecture, identity/authentication & token-security analysis, privilege-escalation path mapping (BloodHound), AWS, Azure

**Secure SDLC & Automation:** Threat modeling, secure coding practices, automated vulnerability remediation (Snyk, Trivy, Ansible), CI/CD security, secure-by-default configuration hardening

**AI/ML for Security:** AI-assisted EDR tooling, ML/GNN-based intrusion & anomaly detection research, adversarial ML & data-poisoning coursework, AI-accelerated triage workflows

**Detection & Monitoring:** SIEM/IDS/IPS/EDR (Wazuh, ELK/OpenSearch, Kibana), SOAR automation, log correlation & forensic analysis, MITRE ATT&CK-based adversarial emulation

**Offensive Security Knowledge:** AD red teaming (Kerberoasting, Pass-the-Hash), Mimikatz, Rubeus, Impacket, malware/sample analysis (Cuckoo Sandbox, VirusTotal, MalwareBazaar)

**Languages & Tools:** Python, Bash, PowerShell, Nmap, Wireshark

## EXPERIENCE

### Cybersecurity Observability & AI Engineer

Dec 2024 - Mar 2025

*Ameya Data Solutions - Co-op, Mississauga, ON (Hybrid)*

- Redesigned AWS IAM policies under a Zero Trust, least-privilege model, cutting over-privileged roles by 45% and shrinking the identity attack surface across cloud workloads.
- Built automated SIEM/IDS/IPS/EDR detection pipelines that replaced ad hoc, point-in-time review with continuous monitoring and automated incident response, reducing false-positive alerts by 38%.

### DevSecOps Engineer

May 2024 - Aug 2024

*Ameya Data Solutions - Co-op, Mississauga, ON (Remote)*

- Built AI-enhanced, self-service EDR and vulnerability-scanning tooling (Python, Snyk, Trivy) that let engineering teams detect and remediate risk directly, without bottlenecking on the security team, improving vulnerability-detection coverage by 33%.
- Automated security configuration and patch management with Ansible, embedding secure-by-default guardrails into deployment workflows alongside developers.

### Data Analyst Intern

Aug 2023 - Dec 2023

*Ameya Data Solutions - On-Call, Mississauga, ON (Remote)*

- Deployed Fluent Bit and OpenSearch/Kibana log-analytics pipelines that cut log-correlation and forensic-analysis effort by 35%, accelerating security incident triage.
- Hardened Windows, Linux, and macOS endpoints as part of a continuous, scaled endpoint-security assessment effort.

## EDUCATION

Master of Information Technology Security, AI Specialization (MITS-AI) - Ontario Tech University

Expected Apr 2027

Honours Bachelor of Information Technology (Cybersecurity) - Seneca Polytechnic

Aug 2025

Engineering Diploma (Computer Systems Networking & Telecommunications) - Humber Polytechnic

May 2021

## CLOUD & AI-SECURITY PROJECTS

**Active Directory Red Team Lab** - Practiced Kerberoasting, Pass-the-Hash, and BloodHound/SharpHound-driven privilege-escalation mapping across GOAD, HTB, and TryHackMe AD environments; translated identified authentication and privilege-escalation weaknesses into preventive and detective SIEM detection logic.

**Malware Analysis & Threat-Intelligence Pipeline** - Built a Cuckoo Sandbox detonation environment integrated with the VirusTotal and MalwareBazaar APIs to automate sample triage and static/dynamic analysis, authoring custom detection rules and validating sandbox isolation.

**Wazuh SIEM & Ransomware Detection Lab** - Built a self-hosted SIEM/EDR lab modeling production security operation, configuring detection rules and log pipelines to identify and alert on active ransomware behavior.

## CERTIFICATIONS

ISC2 Candidate | Certified Ethical Hacker (CEH) - Cisco Networking Academy | Certificate of Cloud Security Knowledge (CCSK) - Cloud Security Alliance | Cisco Certified Network Associate (CCNA) | Microsoft Certified: Azure Fundamentals