Sagarpreet Hooda

sagarhooda.uscan@gmail.com +1 (905)-782-4256 Toronto, Ontario linkedin.com/in/sagarhooda-york

sagarhooda-cyber-portfolio.vercel.app github.com/sagarh12

Computer Science student graduating in April 2027 with a year of experience in IT Security Operations at Toronto Hydro, a critical infrastructure energy utility. Worked across Identity and Access Management and Threat, Risk and Compliance, with practical experience in Public Key Infrastructure (PKI) and certificate creation (Venafi, Microsoft Certificate Authority, OpenSSL), SCADA smart cards, Active Directory, Entrust multifactor authentication, Microsoft Azure and Entra ID, IBM QRadar (SIEM), VPN and network access, and PowerShell and Python automation. Also a research assistant and the Founder and President of AI Ignite at York.

Education

Honours BSc Computer Science September, 2022 – April, 2027
York University, Lassonde School of Engineering | Toronto, ON | Lassonde Entrance Scholarship

Professional Experience

Senior Technical Student, Cybersecurity Operations September, 2025 – September, 2026
Toronto Hydro, IT Security Operations | Co-op | Toronto, ON (Hybrid)

- Issued and renewed **TLS certificates** in **Venafi** across dev, test and production during a **certificate authority migration**, and handled **certificate revocation list (CRL)** renewals and **Root CA** tasks as part of **Public Key Infrastructure (PKI)** support.
- Created certificate signing requests (CSRs) with **OpenSSL**, including subject alternative names and 2048 or 4096-bit keys, signed them through **Microsoft Certificate Authority** templates for server, client and **mutual TLS** authentication, and built PKCS#12 bundles delivered through **Secret Server** instead of email.
- Helped re-distribute **SCADA smart cards** to Control Room Operators and Engineers across critical energy infrastructure, validating accounts, creating and issuing cards in **Entrust**, and documenting the procedure; scripted smart-card certificate assignment for separate production and test environments, generating the requests and certificates, building PFX files and loading them onto the cards, and troubleshooting PKI and enrollment errors.
- Worked in **Microsoft Azure and Entra ID** under senior supervision, setting up **conditional access** for specific applications and groups, handling role assignments and granting access to Azure-hosted GenAI services, and supporting the company-wide rollout of **multi-factor authentication** requirements for all users.
- Triaged **IBM QRadar (SIEM)** events as part of **SOC incident response**, including external-IP logins, account lockouts, suspicious application activity and unauthorized AD changes, and tuned QRadar use cases so recurring false positives stopped landing in the investigation queue.
- Found and disabled more than 1,000 unused accounts across the Active Directory domains, cutting standing access.
- Replaced manual folder-access requests with a **PowerShell script** that sets and verifies permissions straight from the ticket, saving 3-4 minutes per request when folder inheritance was intact, and wrote further scripts in PowerShell and Python for account onboarding, bulk Active Directory queries and access reports.
- Supported secure remote access across **VPN**, **Citrix** and **Entrust**, including login, expiry and application visibility problems and managed secure-access client and Wi-Fi bypass for different staff types; set up Entrust multi-factor authentication for users (email, phone and soft token) and enrolled privileged users in Microsoft Authenticator.
- Created and changed **Active Directory** accounts and security groups across production, test and development domains, including enabling, disabling, unlocking, expiry changes and proxy-address updates; granted Windows Server access (regular and administrator), reset passwords by reissuing access packages and extended expiring Citrix accounts, so remote users kept working without a repeat ticket.
- Gave users file, folder, **OneDrive (Microsoft 365)**, **MOVEit** and server access through Active Directory (AD), repaired folder permissions when inheritance broke; managed MOVEit file-transfer users, locked-IP unblocks and MFA resets, adding access through AD first so permissions stayed in sync, and checked password and account expiry through AD attributes.
- Set up privileged and service accounts and stored their credentials in **Delinea Secret Server**, sharing each secret only with the people who needed it.
- Wrote five standard operating procedures for **IAM** requests, certificate management and onboarding, and co-wrote a 28-page ticket resolution guide with more than 70 procedures, now the handbook for incoming student technicians.
- Supported **TRC** risk assessments and audit requests, helped with endpoint security tasks in **SentinelOne**, and handled **endpoint** exception requests (secure-access bypass).
- Worked 40-50 Identity and Access Management (IAM) and Threat, Risk and Compliance (TRC) tickets a day in **BMC Remedy**, with busy days above 100, against P1-P4 SLA targets; watched SLA clocks on the queue, raised change requests in Remedy, and coordinated server decommission work orders across the SIEM, firewall and endpoint owners.

Communications & Website Assistant September, 2026 – Present
Schulich School of Business, York University | Part-time | Toronto, ON

- Manage and improve Schulich websites in WordPress, including content updates, maintenance and technical fixes.
- Build workflow automations with Zapier, Salesforce and Google Forms to streamline communications, data collection, and operations.
- Use AI tools with OneDrive and Google Drive to improve content workflows and documentation.

Research Assistant, Cost-Effective Robot Tutor for Students September, 2026 – Present
York University | Supervisor: Professor Meiying Qin

- Designed and developed an adaptive robot tutor on the Biskee robot platform at York's Markham campus using Python, ROS/ROS2, OpenCV and Git/GitHub, implementing reinforcement learning that personalizes teaching strategies based on student responses and an AI-driven dialogue manager that adapts explanations to each student's knowledge level.
- Developed OpenCV computer vision to monitor student engagement in real time, integrated motion control and sensor communication through ROS/ROS2, and designed user study protocols to collect interaction data and evaluate system performance.

Website Assistant April, 2025 – August, 2025

Lassonde School of Engineering, York University | Toronto, ON

- Maintained university websites and event pages in WordPress, writing custom HTML, CSS and JavaScript where the CMS could not do what the team needed.
- Built and automated weekly Mailchimp email campaigns and organized structured datasets for event logistics, scheduling, and outreach analytics.

AI Web Development Intern January, 2025 – April, 2025

Accio | Internship | Toronto, ON

- Built front ends for AI-powered web platforms in Next.js and React, wiring interfaces to Ollama-backed local language models so features ran inference without an external API.
- Developed responsive, reusable UI components and connected them to backend APIs to drive dynamic, data-driven pages.

Projects

AI Alert Triage Copilot

Next.js, TypeScript, Claude API, Python, pandas, MITRE ATT&CK

- Automates Tier-1 SOC triage by matching QRadar-shaped offences to the real ATT&CK catalogue before the model is called, with a pandas script that prepares CICIDS2017 and UNSW-NB15 data.

InboxGuard

JavaScript, Node.js, MCP, Chrome Extension (Manifest V3)

- Open-source layer that stops hidden prompt injection in emails from reaching AI assistants an MCP proxy cleans each email and holds payments and outbound mail until a person approves them.

Ontario Electricity Demand Forecasting

Python, pandas, scikit-learn, Streamlit

- Day-ahead hourly forecaster for Ontario demand (2018-2025) with leakage-tested time splits. Gradient boosting reached 2.94% MAPE on a held-out year, 34% lower MAE than a same-hour-yesterday baseline (uses actual weather in place of a forecast).

Leadership & Involvement

Founder and President, AI Ignite at York

York University | Toronto, ON

- Founded the club to close the gap between what CS courses teach and the AI tools industry uses. Recruited and led an 18-person executive team across technical, marketing, finance and operations, grew the club to over 50 members, and secured student-government ratification and college affiliation.
- Designed two programs, Spark (no-code AI for any background) and Forge (structured prompting, RAG, evaluation and fine-tuning). Every session is a 90-minute hands-on build.

Cybersecurity Conferences and Volunteering

Toronto, ON

- Volunteered on the AV crew at siberXcon 2026 (May 2026) after completing volunteer training, covering venue setup, breakout-session assistance, and workshop lead and assistant shifts. Received a volunteer certificate.
- Attended SecTor 2025 with the Toronto Hydro team and discussed current security tooling with Fortinet, Zscaler, Claroty, Mimecast, Bell and Thales.

Certifications

- **Completed:** AI Security Lifecycle (Plan and Scope, Deploy) | Securing LLM Applications in Banking | Cloud Architecture Foundations | Core Cloud Infrastructure
- **In progress:** CompTIA Security+ | Microsoft SC-900 | Microsoft AZ-900

Skills

- **Identity and Access Management (IAM):** Active Directory, Windows Server, Entrust (multi-factor authentication, soft tokens), Citrix, VPN, Microsoft Authenticator
- **Public Key Infrastructure (PKI) and certificates:** Venafi, Microsoft Certificate Authority, OpenSSL, certificate signing requests (CSR), TLS and mutual TLS, PKCS#12, certificate revocation lists (CRL)
- **Smart cards and OT/SCADA:** Entrust smart card provisioning, smart-card certificate assignment, SCADA control room user access
- **SIEM and security monitoring:** IBM QRadar (SIEM), SentinelOne, incident response, alert triage, use case tuning
- **Cloud:** Microsoft Azure, Entra ID, conditional access (application and group-based), role assignments, multi-factor authentication policy rollout, Microsoft Authenticator, OneDrive
- **Networking and remote access:** VPN, Citrix, secure access client, firewall request coordination
- **Privileged Access Management:** Delinea Secret Server
- **IT service management:** BMC Remedy (incident, work order, task and change), SLA management, standard operating procedures, MOVEit, NTFS permissions
- **Languages and scripting:** PowerShell, Python, TypeScript, JavaScript, Java, SQL
- **Development and tools**: Next.js, React, Node.js, FastAPI, Firebase, ROS/ROS2, OpenCV, Git, Pytest, Vitest, WordPress, Zapier, Salesforce, Power BI, Microsoft Teams