

Yash Patel

Scarborough, ON, M1W 2V1 | 437-219-7668 | yash4050@gmail.com

Portfolio: <https://yashpatel0509.github.io/Yash-portfolio/> **LinkedIn:** www.linkedin.com/in/yash0509

PROFILE

Cybersecurity & Threat Management co-op student with enterprise IT experience and hands-on exposure to SIEM monitoring, incident response analysis, identity and access management, and network security. Experienced with **Suricata IDS, Elastic Stack, Azure Active Directory, Intune, and AWS environments**. Seeking a **Summer 2026 Cybersecurity or Security Operations (SOC) Co-op opportunity**.

TECHNICAL SKILLS

Cybersecurity & Detection - SIEM log analysis, Suricata Intrusion Detection System (IDS), Kibana, Wireshark, Snort, alert triage, PGP encryption, hashing.

Networking & Systems - TCP/IP, VLANs, OSPF, IPv6, subnetting, Linux (Ubuntu, Kali), Windows, Bash.

Cloud & Tools - Amazon Web Services (EC2, IoT Core), Azure Active Directory, Intune, Autopilot, SCCM, ServiceNow, Jira, Excel.

Risk & Security Concepts - Identity and Access Management (IAM), least privilege, incident response exposure, security controls, third-party risk.

PROFESSIONAL EXPERIENCE

Desktop Support Analyst | Healthcare of Ontario Pension Plan

Nov 2024 – Feb 2025

- Automated secure endpoint provisioning using Microsoft Intune and Autopilot, improving deployment consistency.
- Managed user access and group permissions in Azure Active Directory, supporting least-privilege access control.
- Assisted with VPN, DNS, and network troubleshooting to minimize service disruptions.
- Supported security patching, operating system updates, and endpoint lifecycle activities.

Help Desk Analyst | Cognizant (Client - Enbridge)

Sept 2022 – Nov 2024

- Resolved high-volume incidents using ServiceNow and Jira across hardware, VPN, and enterprise applications.
- Deployed and imaged devices using SCCM and PXE, following ITIL change procedures.
- Performed Active Directory account administration and access troubleshooting.
- Documented resolutions and reviewed logs to support audit, compliance, and risk validation.

ACADEMIC PROJECTS

IoT Security Monitoring & Threat Analysis

- Engineered a secure IoT environment using Raspberry Pi, AWS IoT Core, and Python automation.
- Built a virtual Security Operations Center (SOC) using Suricata IDS and Elastic Stack for real-time monitoring.
- Conducted controlled DDoS simulations and analyzed traffic using AWS VPC Flow Logs stored in S3.

Security Case Studies & Incident Response Analysis

- Analyzed large-scale breaches, supply-chain attacks, and identity data exposures focusing on incident timelines, root cause, and impact.
- Developed incident response and crisis communication plans, including executive summaries and stakeholder notifications.
- Produced policy, governance, and third-party risk recommendations to strengthen organizational preparedness.

Network & Web Application Penetration Testing

- Conducted end-to-end penetration testing against a Metasploitable2 environment.
- Exploited misconfigurations in VNC and Apache Tomcat, achieving privilege escalation.
- Identified Cross-Site Scripting (XSS) and SQL Injection vulnerabilities and authored a professional risk-based report.

Active Directory Exploitation & Lateral Movement

- Simulated red-team activity by exploiting MS17-010 (EternalBlue) for initial access.
- Performed credential harvesting using Mimikatz and password cracking with John the Ripper.
- Executed Pass-the-Hash attacks using Impacket to achieve lateral movement.

CERTIFICATIONS

AWS Cloud Security Foundations (**AWS Academy**) | Introduction to Linux (**Linux Foundation**) |
Introduction to Digital Forensics (**Cyber5W**) | Introduction to Cybersecurity (**Cisco**) |
IPv6 Address Planning & Fundamentals (**APNIC**) | Critical Infrastructure Protection (**OPSWAT**)

EDUCATION

Cybersecurity & Threat Management (Post-graduate Certificate) Sept 2025 – Apr 2026 (*Expected*)

Seneca College of Applied Arts and Technology

Computer Networking and Technical Support (Diploma) Jan 2020 – Dec 2021

Seneca College of Applied Arts and Technology