

Yash Patel

Scarborough, M1W 2V1 | 437-219-7668 | Yash4050@gmail.com | www.linkedin.com/in/yashpatel0509

Profile

Cybersecurity & Threat Management postgraduate student at Seneca College with hands-on experience in threat detection, SIEM log analysis, network security, cloud environments, and enterprise IT operations. Strong exposure to Suricata IDS, Elastic Stack, Linux, Python, Intune, SCCM, and identity access administration. Experienced in troubleshooting incidents, evaluating security controls, and supporting secure device provisioning in large enterprise environments. Familiar with security control evaluation, alert investigation workflows, and enterprise access governance. Seeking Summer 2026 Cyber Security / SOC Analyst / Cyber Risk Co-op.

Technical Skills

Cybersecurity & Detection - Suricata IDS, Kibana, SIEM log analysis, Snort rules, Wireshark, PGP & hashing.

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

Cloud & Tools - AWS IoT / EC2, Intune, Autopilot, SCCM, Azure AD / Active Directory, ServiceNow, Jira.

Risk & Security Concepts – Security control evaluation, incident response exposure, IAM & least-privilege.

Professional Experience

Desktop Support | Healthcare of Ontario Pension Plan

Nov 2024 – May 2025

- Automated secure device deployment using Autopilot & Intune, improving provisioning consistency and reducing onboarding time across enterprise endpoints.
- Managed user permissions and access through Azure AD & SSO groups, supporting secure onboarding and least-privilege access control.
- Configured VPN, DNS, and network settings and assisted with incident troubleshooting to minimize service disruption.
- Supported security patching, OS updates, hardware diagnostics, and asset lifecycle activities across corporate endpoints.

Help Desk Analyst | Cognizant (Client - Enbridge)

Sept 2022 – Nov 2024

- Resolved 100+ tickets/week across hardware, VPN, application, and network issues using ServiceNow & Jira.
- Performed account administration & access troubleshooting in Active Directory and SSO environments.
- Imaged and deployed laptops/desktops using PXE & SCCM, following ITIL change processes and documentation standards.
- Coordinated secure deployment and shipping of IT equipment across Canadian business units.

Academic Projects

IoT Threat Detection System — Raspberry Pi, Suricata, Elastic Stack

- Deployed Suricata IDS to monitor IoT traffic, created custom detection rules, and forwarded logs to Elasticsearch.
- Built Kibana dashboards to analyze alerts including port scans, malformed MQTT packets, and anomalous device behavior.
- Demonstrated detection pipeline, alert triage, and investigation workflow concepts.
- Investigated alerts and validated false positives vs true positives during analysis.

Machine Learning Fraud Detection Model (Python)

- Developed Random Forest classification model for fraudulent transaction detection.
- Performed data cleaning, feature selection, EDA, and precision/recall evaluation to improve model performance.
- Relevant to Fraud Technology / Analytics security stream.

Network Security & Routing Project — Cisco Packet Tracer

- Designed multi-router topologies using OSPF, VLAN segmentation, IPv6, DHCP and gateway routing.
- Tested connectivity, failure behavior, and applied basic hardening techniques.
- Analyzed traffic flows and validated security configurations.

PGP Encryption & Hashing Lab

- Implemented RSA key generation, SHA hashing, encryption/decryption workflows to demonstrate confidentiality and integrity principles.

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