Manarth Patel

27 McRoberts Crescent, Courtice, ON • 6475532371 • mpatel237@icloud.com • linkedin.com/in/manarthpatel • https://patelmanarth.github.io/manarth-patel-portfolio/

SOC Analyst | IT Support | Threat Detection | SIEM | Incident Response | Open Work Permit (PGWP) Holder – Eligible to work full-time in Canada

Entry-level IT and cybersecurity professional with hands-on experience in technical support, system troubleshooting, and security monitoring through real-world projects and lab environments. Skilled in SIEM tools (Wazuh, Splunk), log analysis, and incident detection, with a strong foundation in networking and system administration.

Built and managed a home cybersecurity lab simulating enterprise environments, performing attack simulations and blue team detection aligned with MITRE ATT&CK. Strong problem-solving abilities with a customer-focused mindset, seeking opportunities in IT support, service desk, or SOC analyst roles.

WORK EXPERIENCE

Local Convenience Store • Oshawa • 05/2024 - Present

Lead Sales • Part-time

- Managed daily store operations including transactions, inventory, and customer service
- Delivered customer support in a fast-paced environment, improving communication and multitasking skills

Business Web Solutions • India • 01/2023 - 06/2023

Web Dev Intern

- Assisted in securing backend APIs through authentication and input validation improvements
- Performed vulnerability checks on client applications under supervision
- Collaborated with developers to improve data handling and access control practices

Chatkazz • Anand, India • 11/2019 - 05/2022

Technical Support (Family Business) • Part-time

- Provided day-to-day technical support for POS systems, billing software, and network connectivity
- Troubleshot hardware and software issues to ensure uninterrupted store operations
- Resolved customer-facing technical issues, strengthening communication and problem-solving skills
- Identified and resolved system issues by analysing errors and logs where applicable

GenieApp Solutions • Canada • 06/2021 - 09/2021

Backend Developer Intern

- Built and tested REST APIs using FastAPI and MongoDB
- Implemented input validation and security checks for application endpoints

PROJECTS

Operation Hydra – Corporate APT Simulation • 07/2025 - 08/2025

Capstone – Hacking & Exploits

- Simulated a real-world cyberattack lifecycle including SQL injection, privilege escalation, and lateral movement
- Detected malicious activity using Wazuh SIEM and Sysmon logs

SKILLS

IT Support & Systems: access control, Active Directory, Hardware/software troubleshooting, Linux (Ubuntu), POS systems, Remote support and issue resolution, User account setup, Windows OS

Security & SOC Skills: Alert triage & incident investigation, Log Analysis (Sysmon & Windows Event Logs), MITRE ATT&CK fundamentals, Network monitoring (Wireshark & Zabbix), SIEM Monitoring (Wazuh & Splunk), Vulnerability scanning (Nessus & OpenVAS)

Tools & Technologies: AWS EC2, Bash, Confluence, Git, JIRA, MongoDB, MySQL, pfSense Firewall, PowerShell, Python, REST APIs, Wireshark, Zabbix

Languages (Bilingual/Multilingual): English (Fluent), French (B1 – Elementary, learning), Gujarati (Native), Hindi (Native)

- Performed incident response actions including system isolation and security hardening
- Demonstrated end-to-end attack and defence aligned with SOC workflows

Honeypot Deployment and Early Threat Monitoring • 06/2025 - 07/2025

Capstone – Network Monitoring & Pen Testing

- Deployed honeypots to observe attack behaviour and log intrusion attempts
- Analysed attack patterns and documented defensive strategies

Personal Cyber Risk Scanner • 04/2025

Independent Project

- Developed a tool using Nmap and Python to identify open ports and weak configurations
- Built a Streamlit interface with automated reporting

CERTIFICATIONS

CompTIA Security+ (Preparing)

CompTIA

Splunk Core Certified User (SPLK-1001) (Preparing)

Splunk (Cisco)

CCSP Specialization (Planned)

Pearson - Coursera

SOC Analyst Certificate

Cisco - Coursera

IT Support Professional Certificate (In Progress)

Google - Coursera

VOLUNTEERING & LEADERSHIP

CHARUSAT University • 01/2021 - 01/2023

Student Central Council Leader

- Organized two national-level hackathons (100+ teams)
- Coordinated cultural/technical/sports events with student-faculty collaboration

EDUCATION

Postgraduate Certificate in Cybersecurity

Durham College
Canada
01/2025 - 09/2025

- Courses: Ethical Hacking (EHE), Digital Forensics (DFE), Risk Management, Incident Handling, GRC, Auditing, Access Control
- Tools: Kali, Splunk, Wazuh, pfSense, Zabbix, FTK Imager, Autopsy, etc.

Postgraduate Certificate in Artificial Intelligence

Durham College
Canada
01/2024 - 09/2024

- Courses: ML/DL, NLP, Vision, Python, AI app development
- Projects: YOLOv8 face tracking, AI matchmaker, AI-integrated fraud analysis

Bachelor of Engineering in Information Technology

CHARUSAT University
India
01/2019 - 06/2023

- Core: Networking, Databases, Web Dev, AI/ML, Cloud, Cryptography, Mobile App Dev
- Labs: Raspberry Pi automation, Docker (intro), Firebase apps, GCP (basic), Web Security