SAPTARSHI PATEL

SOC ANALYST — Security Monitoring, Threat Detection, & Network Security

saptarshipatel@outlook.com (+1)-647-898-1525 Toronto LinkedIn

SKILLS

- **Network Security**: Firewalls, IDS/IPS, Site-to-Site VPN, ACLs, NAT/PAT, DHCP Snooping, and DAI.
- **Security Operations**: SIEM (Splunk, Microsoft Sentinel), log analysis, alert triage, and Excel (VLOOKUP).
- **Identity & Access Management**: Active Directory, MFA, RADIUS, TACACS+, and single sign-on.
- **Cloud, OS & Virtualization**: AWS, Azure, VMware, VirtualBox, Linux (Ubuntu, Kali), Windows 10/11.
- **Security Tools & Documentation**: Wireshark, Nessus, Metasploit, SharePoint, Python, Bash scripting.

WORK EXPERIENCE

Security Concierge (Part-time) **August 2023 – Present**
Elite Residential Concierge Service *Ontario*

- Facilitated exceptional customer care by greeting 50+ residents daily and addressing resident concerns promptly through documented service protocols.
- Executed responses to 10+ emergency incidents monthly, including fire alarms and lift entrapments, following established response procedures.
- Managed access control systems regulating 20+ authorized entries daily to maintain resident safety through credential verification processes.

PROJECT EXPERIENCE

Mobile Application Security Analyzer **GitHub**
Developer

- Developed a web-based Android application security analyzer with a Wix front-end, enabling secure uploads of 10+ APK files through an intuitive user interface.
- Engineered a Python Flask backend integrated with AndroGuard, performing static analysis on 50+ APKs and identifying 20+ common vulnerability patterns.
- Formulated automated PDF report generation, delivering 10–15 page security reports with 100% consistency and actionable remediation insights.
- Instructed security best practices including temporary file storage, input validation, and access controls, reducing data exposure risk to near zero.

CCNA 200-301 Network Security Lab Project
Developer

- Designed enterprise network infrastructure with 50+ routers, Layer 3 switches, firewalls, VLAN segmentation, and defense-in-depth architecture across 8+ VLANs.
- Configured security controls including standard and extended ACLs, port security, DHCP snooping, DAI, and AAA authentication on 25+ network nodes.
- Deployed secure connectivity using site-to-site IPsec VPNs, SSH device management, and WPA3-Enterprise wireless authentication across 4+ network segments.
- Implemented centralized logging using syslog servers and SNMPv3 for traffic monitoring and security event analysis from 15+ devices.

SOC Simulation and Threat Detection Home Lab
Developer

- Architected a virtualized SOC environment using Elastic Stack SIEM (Elasticsearch, Kibana), integrating 4+ systems including Windows 10 with Sysmon, Kali Linux, and pfSense.
- Configured centralized log ingestion with Elastic Agent and Beats processing 500+ daily security events across 5+ sources normalization parsing.
- Developed custom detection rules aligned with MITRE ATT&CK identifying 8+ brute force, privilege escalation, and lateral movement techniques correlation heuristics.
- Executed simulated attacks using Metasploit, Nmap, and Hydra, analyzing 15+ incidents through SIEM dashboards and KQL queries attribution triage.

EDUCATION

Post Graduate Degree in Cybersecurity May 2023 – December 2024
Loyalist College, Toronto, Canada
Bachelor of Engineering in Electronics and Communication July 2017 – June 2021
Gujarat Technological University, India

CERTIFICATIONS

- **CompTIA Security+ (SY0-701)** Credential Link
- **eLearnSecurity Junior Penetration Tester [eJPT v2]** Credential Link
- **Cisco Certified Network Associate (CCNA 200-301)** – Expected Feb 2026