JAY PATEL

JUNIOR SECURITY ENGINEER - Security Engineering, Attack Analysis & Automation

jaypatel.jp.9696@gmail.com +1 548-881-0374 London, ON LinkedIn GitHub

SKILLS

- **Security Monitoring & Detection**: Splunk, Wazuh, LimaCharlie, OpenEDR, pfSense, SIEM Management.
- **SOAR & Automation**: Tines, PowerShell, Bash, Ansible, Security Orchestration, Playbook Development.
- **Networking & Infrastructure Security**: TCP/IP, VLANs, Routing, ACL Configuration, Firewalls, IDS/IPS.
- **Systems & Virtualization**: Windows Server, Linux, VMware, Proxmox, Patch Management.
- **Cloud & Identity Management**: Microsoft Azure, AWS (Foundational), Microsoft Entra ID, IAM Policies.

WORK EXPERIENCE

IT Technician Co-op **May 2025 – August 2025**
Martinrea Inc *Tillsonburg*

- Composed Linux system hardening and patch deployment across 40+ enterprise servers using Ansible playbooks, reducing manual configuration effort by 60% and improving compliance consistency.
- Resolved 30+ endpoint, network, and identity access issues, maintaining security baselines and enforcing access controls across Windows and Linux environments.
- Assisted in vulnerability remediation efforts by applying patches and configuration updates, decreasing recurring security incidents by 25%.
- Documented 50+ service tickets and technical incidents while adhering to ITSM workflows and escalation procedures within a structured enterprise support environment.

PROJECTS

SOAR_EDR_Project GitHub Repository
Incident Response Automation

- Designed and deployed a SOAR-integrated EDR lab environment to simulate real-world security incidents and Improved response workflow.
- Automated alert triage actions including host isolation, account disabling, and forensic artifact collection, reducing manual response time by 50%.
- Integrated EDR telemetry with SIEM for centralized log aggregation, correlation, and threat detection across multiple endpoints.

Secure Network Design and Configuration – FANNET (Capstone)
Group Leader & Lead Network Engineer

- Architected and implemented FanNet, a segmented enterprise network supporting 5 departmental VLANs and 55+ simulated users, with centralized firewall enforcement to enhance internal security.
- Configured secure routing protocols and 20+ ACL rules to restrict lateral movement between departments, reducing unauthorized cross-segment traffic by 90% in testing scenarios.
- Deployed Active Directory with role-based access control (RBAC), creating 10+ security groups and enforcing least-privilege access policies across all user accounts.

ByBank Security Architecture and Hardening Project GitHub Repository
Group Leader & Lead Network Engineer

- Architected a secure hybrid enterprise banking network comprising 8 segmented VLANs, hardened perimeter defenses, and zero-trust security principles to protect 50+ simulated endpoints.
- Implemented pfSense firewall with 25+ granular access control rules, management-plane isolation, and real-time traffic monitoring to reduce unauthorized access attempts by 75% during testing.
- Integrated Active Directory with centralized authentication, configuring 15+ role-based access control (RBAC) groups and enforcing privileged account separation policies.

EDUCATION

Advanced Diploma in Cybersecurity **September 2022 – December 2025**
Fanshawe College, Ontario

Diploma in Computer Engineering **August 2018 – June 2021**
Gujarat Technological University, India

CERTIFICATIONS

- **CompTIA Security+** **June 2023 – June 2026**