RUTVIK PATEL

Cybersecurity Analyst | SOC Operations · Cloud Security · Vulnerability Management
Kitchener, ON • +1 (226) 961-9538 • rutvikonline@gmail.com • linkedin.com/in/rutvikonline • github.com/rutvikonline2303

PROFESSIONAL SUMMARY

Cybersecurity professional specializing in SOC operations, SIEM detection engineering, vulnerability management, and cloud security. Skilled at tuning Splunk and Microsoft Sentinel detection logic to reduce alert fatigue, automating incident response, and hardening Microsoft Azure and Entra ID environments, backed by hands-on penetration testing. CompTIA Security+ and CISM certified. Eligible to work in Canada on an open work permit.

TECHNICAL SKILLS

Security Operations & SIEM: Splunk, Microsoft Sentinel, Azure Log Analytics, IBM QRadar, KQL, alert triage, detection tuning, log analysis, incident response (IR)

Threat & Vulnerability Mgmt: Tenable Nessus, vulnerability lifecycle & remediation, threat intelligence, MITRE ATT&CK, SOAR (Wazuh, Tines), EDR concepts

Cloud & Infrastructure: Microsoft Azure (Entra ID, Conditional Access, MFA, Firewall, NSG), Terraform, ARM Templates, Docker, UniFi

Offensive Security: Burp Suite Pro, Metasploit, Nmap, Wireshark, Intigriti, OWASP Top 10, penetration testing

Compliance & GRC: NIST CSF, NIST SP 800-115, MITRE ATT&CK, ISO 27001, ISO 21434 (Automotive)

Scripting & Languages: Python, PowerShell, Bash, SQL

Tools & Platforms: Git, VS Code, Postman, Linux (Kali / Ubuntu)

PROFESSIONAL EXPERIENCE

System Technical Analyst
Mar 2025 – Present
London Language Institute — *London, ON*

- Administer and secure Microsoft Azure infrastructure (Virtual Machines, Virtual Networks, Load Balancers), maintaining business continuity and SLA adherence.
- Enforce a Zero Trust access model with Entra ID Conditional Access and MFA, strengthening identity security across the organization.
- Automate infrastructure deployments using Terraform and ARM templates, reducing manual configuration errors and improving deployment consistency.
- Monitor system health and security telemetry through Azure Log Analytics and Application Insights, proactively resolving performance and availability issues.

Assistant System Engineer
Jul 2022 – Jun 2023
Tata Consultancy Services — *India*

- Managed the enterprise vulnerability lifecycle via Intigriti — validating critical submissions and coordinating remediation with engineering teams within SLA.
- Operationalized CybelAngel threat intelligence to detect brand abuse and coordinate rapid takedown of phishing domains and leaked credentials.

Penetration Tester
Jan 2022 – Jun 2022
Tech-Defence Labs Solutions — *India*

- Performed black-box and gray-box web penetration tests with Burp Suite Pro, identifying and validating OWASP Top 10 vulnerabilities including SQL injection.
- Conducted post-exploitation with Metasploit to validate endpoint detection (EDR) and incident response effectiveness, documenting findings against MITRE ATT&CK and NIST SP 800-115.

SECURITY PROJECTS

Azure Sentinel Honey-Cloud — *Microsoft Sentinel (SIEM), KQL, PowerShell, Network Security Groups*

- Built a live honeypot environment ingesting and visualizing real-time RDP brute-force attacks, enriching security events with geolocation data via a custom PowerShell pipeline.
- Analyzed attack telemetry, traced malicious traffic to three specific ASN blocks, and implemented targeted geo-blocking policies that proactively reduced the attack surface.

Azure CSPM Scanner — *Python, Azure SDK, CIS Azure Foundations Benchmark, GitHub Actions*

- Built a read-only Python tool that scans an Azure subscription against CIS Benchmark controls (public blob access, internet-exposed RDP/SSH, Key Vault protection, SQL auditing), outputs a severity-weighted 0–100 score and HTML report, and gates CI/CD — with a credential-free mock mode and unit-tested check engine.

Sentinel Detection-as-Code — *Microsoft Sentinel, KQL, ARM, GitHub Actions, MITRE ATT&CK*

- Managed Microsoft Sentinel analytics rules as version-controlled YAML, validated in CI and compiled to ARM for repeatable deployment, with KQL detections mapped to MITRE ATT&CK for RDP brute-force, Entra ID password spray, illicit OAuth consent, and Azure Storage exfiltration.

EDUCATION

Master of Applied Computing Science, University of Windsor — Sep 2023 – Dec 2024
Bachelor of Technology, Computer Science, Ganpat University — Nov 2018 – Dec 2022

CERTIFICATIONS

CompTIA Security+ • **Certified Information Security Manager (CISM)** — ISACA