Parv Choksi

587-437-4999 | parv.choksi81@outlook.com | linkedin.com/in/choksiparv | github.com/Parmingo

Education

Dalhousie University — Halifax, NS
Bachelor of Computer Science – Certificate in Cyber Security — *Sept. 2022 – May 2026*

University of Calgary — Calgary, AB
Bachelor of Science - Concentration in Biology — *Sept. 2018 – May 2022*

Certifications

Coursera — Halifax, NS
Google Cybersecurity Professional Certificate — *Jan. 2024 – Mar. 2024*

CompTIA — Halifax, NS
Security+ (SY0-701) — In Progress — *Sept. 2025 – Nov. 2025*

Skills Summary

Technical: Incident Response, Threat Analysis, Endpoint Protection, Power BI (DAX), PowerShell, Python, SQL, Docker, Azure Runbooks, Microsoft Sentinel, Microsoft Defender, Microsoft Azure, Trellix, HP Sure Click, Burp Suite, OWASP ZAP, Wireshark, Linux, Windows
Frameworks & Standards: ITSG-33, NIST SP 800-53, OWASP Top 10, Zero-Trust Architecture

Work Experience

Cyber Security Analyst – Incident Response Team — May 2024 – Sept. 2024
Statistics Canada — *Ottawa, ON*

- Optimized Microsoft Sentinel alerting by refining detection rules, adjusting severity levels, and implementing playbooks, reducing false positives by 40% and improving response times by 25%.
- Responded to Microsoft Sentinel alerts by analyzing logs, contacting users, and implementing fixes, contributing to 30% of the team's resolved alerts and enhancing overall security posture.
- Constructed monthly DLP reports for users with over 3,000 alerts and collaborated with the IR team to mitigate incidents, strengthening data protection.

Cyber Security Analyst – Endpoint Protection Team — Sept. 2024 – Present
Statistics Canada — *Ottawa, ON*

- Improved endpoint protection posture to 98% compliance across Azure virtual machines and VM scale sets through threat detection tuning and remediation coordination.
- Automated security compliance and risk dashboards integrating Defender, Trellix, HP Sure Click, and HBS data using PowerBI, PowerShell, and Azure Runbooks.
- Collaborated with infrastructure and compliance teams to perform vulnerability remediation, security configuration hardening, and alignment with ITSG-33-based security controls.

Personal Projects

Web Exploitation Capture The Flag (CTF) | *Burp Suite, OWASP ZAP, Wireshark, Linux* — Oct. 2025

- Performed penetration testing and web exploitation exercises simulating real-world attack vectors as part of a cybersecurity CTF.
- Identified and exploited OWASP Top 10 vulnerabilities such as SQL injection, cross-site scripting (XSS), command injection, and authentication bypass to retrieve hidden flags.
- Utilized Burp Suite, OWASP ZAP, nmap, and sqlmap for reconnaissance, payload testing, and exploitation, demonstrating practical offensive and defensive security skills.

Automated Threat Intelligence Dashboard | *Python, Power BI, VirusTotal API, MISP* — Aug. 2025

- Developed a Python script to aggregate Indicators of Compromise (IOCs) from open-source threat intelligence feeds and VirusTotal API.
- Transformed and visualized data in Power BI to track emerging malware families and associated IPs/domains.
- Implemented scheduled updates and alerting mechanisms to simulate real-time threat awareness for SOC operations.