VIOLET FIGUEROA

CYBER SECURITY ANALYST

Vancouver, BC, Canada (Remote-Ready) | 604.220.5617 | violet@violetfigueroa.com

LinkedIn | GitHub

PROFESSIONAL SUMMARY

CompTIA Security+ certified cybersecurity analyst with 1.5 years of hands-on expertise in incident response, digital forensics, and vulnerability management. Proven ability to communicate technical findings to diverse audiences and drive measurable security improvements. Skilled in Splunk, Wireshark, MITRE ATT&CK, and NIST 800-53. Seeking analyst or SOC roles in dynamic, high-impact environments focused on proactive threat hunting and cross-functional security communication.

TECHNICAL SKILLS

Security Tools: Splunk, QRadar, Wireshark, BurpSuite, OWASP ZAP, Nmap, Log Analysis, IDS/IPS, EDR, WAF, Firewalls, OpenVAS, MITRE ATT&CK, NIST 800-53, OWASP Top 10, ISO 27001, Volatility, Autopsy, Threat Modeling

Programming: Python, JavaScript (ES6+), Bash, SQL, HTML5, CSS3, Node.js, Express, React, PostgreSQL, APIs (REST/JSON), Git, Docker, Linux (Debian/Kali)

Analysis: Vulnerability Assessment, Threat Hunting, Gap Analysis, Risk Management, Executive Briefs, Technical Documentation, Incident Reports, Playbooks

Networking: TCP/IP, VLANs, VPN, Routing & Switching, Firewall Rules, Wi-Fi Configuration, LAN/WAN, Network Monitoring, Azure Networking, Remote Access

Tools Platforms: Microsoft 365, Azure AD, Ticketing Systems, Remote Support Tools, Linux Servers, Windows Server, PowerShell, GitHub

WORK EXPERIENCE

Freelance IT Support Technician | Self-Employed 2012 - Present

Greater Vancouver Area

Providing on-site and remote technical support to seniors, families, and community members for Windows/macOS systems, home networking, and mobile device troubleshooting.

- Install and configure operating systems, perform hardware upgrades, diagnose and resolve system failures, and remove malware and optimize system performance for end users.
- Set up and troubleshoot home routers, Wi-Fi networks, printers, and peripherals; establish backup solutions and educate users on digital hygiene and device maintenance.
- Used ticketing and remote support tools to track and resolve issues efficiently while maintaining strong customer relationships.
- Deliver clear technical explanations using non-technical language; maintain professional support standards and customer satisfaction.
- Resolved 100+ support cases across a range of hardware, OS, and networking scenarios.

Cybersecurity Analyst, Web Developer & IT Support | Accessible Places Sept 2022 - Jan 2024

Remote, Greater Vancouver Area

Led cybersecurity, IT support, and web development for a distributed remote team of 30 endpoints.

- Provided primary IT support for 30 fully remote endpoints, handling VPN setup, endpoint patching, and day-to-day troubleshooting of connectivity and system issues.
- Analyzed logs and network data using Wireshark and Nmap to troubleshoot issues and identify potential security gaps across the infrastructure.
- Configured advanced firewall rules and multi-factor authentication (MFA) across all accounts, reducing malware incidents by 100% and account compromise cases to zero.
- Conducted monthly system audits, identifying and remediating 12+ vulnerabilities.
- Trained users in digital hygiene, increasing phishing awareness scores by 40%.

Volunteer | VanLUG (Vancouver Linux Users Group)

2025 - Present

Vancouver, BC

Volunteer supporting open-source education, right-to-repair, and sustainable technology practices.

- Organized and supported community meetups on Linux, privacy, and sustainable hardware reuse.
- Advocated right-to-repair principles and contributed to open-source education initiatives.
- Promoted privacy-first tooling and secure operating practices across community members.

PROJECTS

Premium House Lights: The Heist

May 2025

- Identified root causes (unrestricted file upload, flat network architecture, excessive privileges).
- Performed log and network analysis, and delivered actionable security recommendations to executive leadership.

LogHawk – Security Log Monitoring Tool

Dec 2024

- Utilized Python and Bash to parse system logs and identify potential threats.
- Published as open-source code on GitHub, demonstrating secure coding and automation skills.

P11: Secure Architecture Report

Apr/May 2025

- Designed and documented a secure network architecture for a simulated enterprise.
- Recommended security controls and architectural improvements to mitigate identified risks.

P10: Forensics Report

Apr 2025

- Conducted a forensic investigation on a compromised system, analyzing logs and artifacts.
- Reconstructed the incident timeline and documented findings in a legal-grade report.

Intellectual Property Theft Investigation

Mar 2025

- Used memory analysis, event log review, and network traffic analysis to uncover brute-force attack, malware deployment, and data exfiltration.

EDUCATION

Diploma in Cybersecurity

Nov 2024 - May 2025

Lighthouse Labs

- Completed 30+ hands-on labs covering incident response, digital forensics, threat hunting, and security operations using Splunk, Wireshark, Volatility, and related tools.
- Collaborated in simulated SOC team environment and authored comprehensive forensic capstone reports integrating MITRE ATT&CK and NIST 800-53 controls.

Bachelor of Arts (Incomplete)

2013 - 2017

Simon Fraser University

- Interactive Arts and Technology. Completed 60 credits.
- Built strong programming, documentation, and communication skills.

CERTIFICATIONS

- CompTIA Security+ (SY0-701) | Aug 2025
- A+ and Network+ equivalent skills through 10+ years of hands-on IT support and formal cybersecurity training; exam-ready if required.
- Cyber Security Bootcamp Diploma | Lighthouse Labs | Completed May 2025