

MADUSHAN JEGATHEESWARAN | SECURITY + | GSEC | GFACT

contact@madushanxj.com | 647-531-1527 | Toronto, ON | www.madushanxj.com | linkedin.com/in/madushanxj

SUMMARY OF QUALIFICATION

- IT Security Analyst I with 3+ years of experience in information technology including 4+ years of practical experience in cybersecurity.
- Experience in network monitoring, incident resolution, troubleshooting, and administering network devices such as routers and switches.
- Knowledge of vulnerability assessment standards and security frameworks: CIS controls, NIST, MITRE ATT&CK, OWASP10, HIPAA, GDPR, SANS TOP 20, ISO 9001 and 27001 security business management systems.
- Experienced Researcher with natural motivation to continue learning and strong abilities to keep abreast of emerging cybersecurity threats, industry trends, and regulatory changes to adapt and enhance control frameworks.
- Expertise in conducting penetration testing and analyzing security events to enhance organizational defenses
- Strong written and verbal communication skills to create and maintain technical documentation, contributing to organization's effort to manage information security and risk.

TECHNICAL SKILLS

Network Protocols: NAT, UDP, TCP/IP, DHCP, DNS, HTTP/HTTPS, SMTP, TLS/SSL.

Security Tools: SpiderFoot, Nmap, Netcat, Metasploit, John the Ripper, Tcpdump.

Security Devices: Firewalls, anti-virus, anti-spam, HIDS, NIDS, HIPS, NIPS, EDRs, IDS, SOARs.

Security Skills: SQL Injection, Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Local & Remote File Inclusion, Information Disclosure, Remote Code Execution 1 (RCE).

Monitoring & Logging: SIEM, Snort, Sguil, Wireshark, Zeek, Splunk.

Threat Management: Firewalls, DLP, EDR, HIDS/NIDS, HIPS/NIPS, Content Filtering.

Operating Systems: Mac, Windows, Linux (Ubuntu, Kali, Slingshot, Security Onion)

Cloud Technologies: Azure: Defender, Sentinel, AWS: S3, EC2, Cloudfront and Route S3

Virtualization Technologies: VMware, Virtual Box

Tools & Programming Languages: PowerShell, Python, SQL, HTML, Tableau

Document Management Tools: Dropbox, LaTeX, Overleaf, Microsoft Office (Word, Excel, PowerPoint, SharePoint)

Programming Languages: Python, Java (Intermediate), C++

CERTIFICATIONS & TRAINING

• GIAC Security Essentials Certification (GSEC)	12/2025
• GIAC Foundational Cyber Technology (GFACT)	03/2025
• CompTIA Security +	06/2023
• Cisco Junior Cybersecurity Analyst	01/2024
• Security Blue Team Junior Analyst	03/2023
• Harvard Cybersecurity: Managing Risk in the Information Age	02/2019

WORK EXPERIENCE

Cybersecurity Researcher (Freelance) | Hackerone | Toronto, ON | 01/2019 - Present

- Conducted comprehensive penetration testing, uncovering an average of 15 vulnerabilities per assessment, and provided detailed proof- of-concept reports that increased security awareness by 20%.
- Utilized Burp Suite, OWASP ZAP, and Nmap to identify security weaknesses in web applications, networks, and systems.
- Collaborated with development teams to communicate vulnerabilities and guide remediation efforts, resulting in a 30% reduction in security risks.

Tech Support Services Analyst | RBC | Toronto, ON | 01/2021 - 05/2023

- Resolved **90% of support tickets** within SLA guidelines, improving response times by **30%**.
- Managed an average of **50+ IT support requests daily**, troubleshooting hardware, software, and network issues.
- Assisted in the deployment and configuration of **250+ new workstations**, ensuring smooth employee onboarding.
- Documented incidents and solutions, reducing repeat issues by **20%**.
- Provided exceptional technical support via phone, email and chat.

PROJECTS

TryHackMe

- Acquired knowledge in cybersecurity encompassing SOC operations, threat intelligence, network security, endpoint monitoring, SIEM usage, digital forensics, and incident response.
- Gained practical skills in threat detection and analysis through hands-on experience with industry-standard tools like Snort, Wireshark, Sysmon, Splunk, Autopsy, and Volatility, applied in diverse security scenarios.
- Developed proficiency in cybersecurity frameworks, threat intelligence tools, and phishing analysis, establishing a strong foundation in cybersecurity practices and techniques.

Nessus Essentials, Home Lab

- Proficiently configured Nessus Essentials for credentialed vulnerability scans on Windows 10 Home Lab Hosts, enhancing the identification and resolution of security weaknesses.
- Established a structured Vulnerability Management Function within the home lab's sandbox networks, streamlining vulnerability identification, prioritization, and remediation. This initiative optimized security practices and fortified network defenses.
- Conducted comprehensive vulnerability assessments using Nessus, successfully identifying and remediating critical security issues within the home lab environment. Additionally, introduced automated remediation processes to bolster network resilience against potential threats.

Azure Sentinel (SIEM), Home Lab

- Deployed Azure Sentinel (SIEM) and integrated it with a live virtual machine functioning as a honeypot for active monitoring and analysis of global RDP Brute Force attacks.
- Employed a customized PowerShell script to geolocate attackers, providing precise geographic data within Azure Sentinel for in-depth threat analysis, enhancing threat intelligence and response capabilities.

Palo Alto Firewall, Home Lab

- Proficiently orchestrated network virtualization within the EVE-NG platform, showcasing skills in network configuration.
- Demonstrated adeptness in IP assignment within the Palo Alto environment, streamlining network operations.
- Successfully centralized control by configuring the Palo Alto Firewall Management Interface, enabling secure, browser-based management and monitoring for enhanced network security.
- Effectively established Palo Alto Firewall L3 Zones, IP address objects, and Virtual Routers to streamline network segmentation and routing, enhancing overall network organization and security.

EDUCATION

Certificate - Accelerated Cybersecurity Training Program | Toronto Metropolitan University | Toronto, ON | 10/2024 - Present

- Seven month accelerated program consisting of 2 SANS Institute courses: SANS SEC401 and SEC275 and an additional Cybersecurity Professional Practice Course on cybersecurity impact to business operations, corporate risk & governance, leading strong knowledge of cybersecurity and achievement of three SANS GIAC certifications: GSEC, and GFACT.
- Actively participated in the SANS SEC401 Security Essentials boot camp, covering Active Defense, Cryptography, Defensible Network Architecture, Linux and Windows Security, Data Security Technologies, vulnerability scanning, as well as AWS and Mac Security.
- Gained hands-on experience with security tools including Nmap, Nessus, Metasploit, and Netcat through practical cybersecurity labs in the SANS SEC401 Hacker Techniques, Exploits & Incident Handling bootcamp.
- Applied Linux/UNIX CLI and Windows CMD/PowerShell to conduct encryption/decryption operations, network analysis, memory forensics, malware investigations, Windows system examinations, and DNS interrogation.

BSc - Computer Science | York University | Toronto, ON | 09/2015 - 04/2019

GED - High School Diploma | Father Michael McGivney Catholic Academy | Toronto, ON | 09/2011 - 06/2015