S e a n C a v d a r

cavdarsean@gmail.com | (613) 678 0435 | Ottawa, ON | in/scavdar/

Certified Cybersecurity Analyst with an extensive set of CompTIA certifications, including Security+, CySA+, and CSAP. Specializing in security risk identification, mitigation, and security infrastructure, I am expertise in security analysis and incident response. Proficient in monitoring and analyzing potential and active threats using advanced security tools and processes, such as SIEM and EDR. Currently, I am actively involved in performing tasks such as vulnerability management, incident handling, endpoint security, and phishing analysis.

TECHNICAL SKILLS & TOOLS

Security Tools:

- Proofpoint
- Splunk
- CrowdStrike
- IBM QRadar
- FireEye
- Wireshark Packet Analysis
- Metasploit
- Next Generation Firewall (NGFW)
- Kali Linux

Networking Tools:

- Wireshark (Packet Analysis)
- PfSense (Firewall and Network Security)
- TCP/IP Protocol Analysis
- VPN Configuration and Management

Programming and Development Tools:

- HTML/CSS
- Python
- JavaScript
- Linux (Ubuntu)

PROFESSIONAL EXPERIENCE

CyberNowLabs — *Mar 2022 – Present*
SOC Analyst (Full time/Remote) — *(Sterling, VA, USA)*

- *Real-time log monitoring in the Security Operations Center, covering various devices.*
- *Monitored network traffic for security events and conducted triage analysis through CrowdStrike EDR and SIEM Splunk.*
- *Conducted log analysis on IBM QRadar SIEM solutions and Splunk Enterprise Security, providing recommendations to technical teams.*
- *Analyzed files, domains, and emails using online resources like IBM X-Force Exchange, VirusTotal, AnyRun, and MX Toolbox.*
- *Analyzed PCAP files and identified anomalies with Wireshark, creating detailed IOC reports.*
- *Worked with Tenable Nessus, Kali Linux, and Metasploitable.*
- *Collaborated with the Engineering team to reduce noise in SOC tools.*
- *Monitored security systems and diagnosed malware events.*

- *Ensured network, systems, and applications' integrity and protection using SIEM tools.*
- *Ensured the integrity and protection of networks, systems, and applications, following security policies and NIST Risk Framework.*
- *Investigated and analyzed security incidents, including phishing emails and malware events.*
- *Conducted post-mortem analysis on logs, traffic flows, and phishing activities.*
- *Identified and investigated high-priority threat campaigns and malicious actors.*

Ideabytes Inc. *Sept 2021 – Mar 2022*
Penetration Tester (Co-Op) *(Kanata, ON, Canada*

- *Performed internal and external penetration testing and web application testing.*
- *Conducted vulnerability assessments and reviewed results.*
- *Utilized various tools, including Ubuntu, Kali Linux, and pfSense.*
- *Tested and secured computer ports using Nessus.*
- *Monitored packet captures with Kali Linux.*
- *Developed expertise in ethical hacking, penetration testing, and security analysis.*

Empathy Schools *Sept 2011 - Aug 2018*
IT Specialist (Full Time) *(UB, Mongolia)*

- *Monitored system and network performance, conducted troubleshooting, and organized maintenance activities.*
- *Installed and configured software and hardware, including printers and network cards.*
- *Provided technical support and training for systems and networks.*
- *Implemented and maintained Windows domain environments, LANs, and security measures.*
- *Managed Active Directory and network services.*

EDUCATION

Willis College, Cyber Security Analyst *Sept 2020 - Mar 2022*
Advanced Diploma *(Ottawa, ON, Canada)*

Mongolian National University *Sept 2007 July 2011*
Bachelor *(UB, Mongolia)*

The National University of Economics *Sept 2017 - July 2018*
Master of Business Administration *(UB, Mongolia)*

CERTIFICATIONS

- *CompTIA Security +*
- *CompTIA CySA+*
- *CompTIA CSAP*
- *Azure Administrator Associate*
- *Azure Infrastructure Solution*
- *Azure Solution Architect Expert*
- *DevOps Engineer Expert*