Amim Mohammad

✉ mohammadamim1@gmail.com
 https://github.com/amimmohammad
in https://www.linkedin.com/ca/mohammad-amim
☎ +1 (289) 404-9068 📍 Toronto, ON

PROFESSIONAL SUMMARY

Dedicated IT professional with a strong background in creating, scaling, maintaining, and securing IT solutions and platforms. Seeking a supportive and nurturing role to leverage expertise in IT asset management and information security. Proven ability to enhance operational efficiency and ensure the security and integrity of IT assets and information.

EDUCATION

Bachelor of Information Technology - Networking & Security   **2019 - 2023**

Ontario Tech University (Ontario, Canada)

- Relevant Coursework : Data Structures, Algorithms, Operating Systems, Network Security, Database Management, Cloud Computing, Machine Learning, IT Security
- Honors : Dean's List

CERTIFICATIONS

Certified

- AWS Certified Cloud Practitioner
- Cisco Certified Network Associate (CCNA)
- CompTIA Security+
- CompTIA PenTest+
- Cyber Defense (TryHackMe)
- Cyber Security (TryHackMe)
- Junior Penetration Tester (TryHackMe)
- Pre Security (TryHackMe)
- PCAP 31-03
- Microsoft Azure
- ITIL 4 Foundations

UnCertified/ under Progress

- CompTIA Cyber Security Analyst+
- Cisco Certified Network Professional
- Certified Information Systems Security Professional (ISC2-CISSP)
- Offensive Security Certified Professional
- IBM Cloud Security Engineer Specialist

TECHNICAL SKILLS

Programming

- Bash
- C
- C++
- C#
- Cascading Style Sheets (CSS)
- File Handling
- HTML
- Java
- Node.js
- Object-Oriented Programming (OOP)
- PHP
- Python
- SQL

Security & Hacking

- Burp Suite
- Computer Forensics
- Cryptography
- Cybersecurity
- Cyber Security Risk
- Incident Management
- Kali Linux
- Meta Sploit
- Nessus
- Nmap
- OWASP
- Penetration Testing
- Privilege Escalation
- Public Key Cryptography
- SecureCRT
- Threat & Vulnerability Management
- Vulnerability Scanning
- Web Exploitation
- Wireshark

Networking

- Amazon Web Services (AWS)
- Active Directory
- Border Gateway Protocol (BGP)
- DHCP
- DNS Administration
- Docker
- EIGRP
- Internet Protocol Suite (TCP/IP)
- IP Networking
- Kubernetes
- L2 Redundancy
- Linux
- Microsoft Azure
- NAT
- Network Services
- Network Troubleshooting
- OSPF
- PAT
- QoS
- RAS
- Windows
- Windows Server

Business

- Accounting
- Computer Information Systems
- Computer Peripherals
- Customer Service
- Data Engineering
- Documentation
- Group Policy
- Management
- Operating Systems
- Oracle VirtualBox
- Public Speaking
- Sales

PROFESSIONAL EXPERIENCE

Remediation Specialist   **Jan 2023 - Present**
Longo Brothers, Toronto, ON
1 year 6 months

- **Requirement:** The company needed to manage and mitigate security vulnerabilities effectively to prevent data loss and reduce potential costs associated with breaches.
- **Action Taken:** Utilized the Brinqa platform to manage and mitigate vulnerabilities, developed an executive PowerBI dashboard for enhanced trend reporting, and conducted TCA assessments for SSP governance and risk.
- **Implementation:** Deployed comprehensive vulnerability management strategies using Brinqa, designed a user-friendly PowerBI dashboard to visualize trends and insights, and performed thorough TCA assessments to ensure robust SSP governance and risk management.
- **Outcome:** Achieved an 87.6% reduction in vulnerabilities, which prevented data loss and resulted in a cost savings of $3.3M. Enhanced the company's security posture and reporting capabilities, ensuring continuous improvement in risk management.

Cyber Security Consultant   **Sep 2022 - Jan 2023**
Deloitte, Vaughan, ON
5 months

- **Requirement:** The company needed to secure the digital infrastructure for CIC's OperateNext - Managed Devices team and achieve SOC2 and SOC3 compliance to protect sensitive information and enhance network security.
- **Action Taken:** Played a pivotal role in implementing encryption protocols, deploying firewalls, and enhancing endpoint security measures across multiple platforms.
- **Implementation:** Developed and executed robust encryption strategies, implemented advanced firewall solutions, and strengthened endpoint security by integrating comprehensive security tools and best practices. Coordinated closely with the OperateNext team to ensure all security measures met SOC2 and SOC3 compliance standards.

- **Outcome:** Successfully secured the digital infrastructure, achieving SOC2 and SOC3 compliance. Safeguarded vital information and fortified network security, resulting in a significant reduction in security incidents and enhanced overall protection of managed devices.

Cyber Security & Compliance Intern   **Apr 2022 - Sep 2022**
OpenText, Toronto, ON
6 months

- **Requirement:** The company needed to enhance security awareness among employees and ensure compliance with ISO 27001 and NIST standards to mitigate risks and strengthen overall cybersecurity posture.
- **Action Taken:** Spearheaded initiatives to elevate security awareness by creating and executing phishing campaigns and conducted in-depth risk assessments aligned with ISO 27001 and NIST standards.
- **Implementation:** Designed and rolled out targeted phishing campaigns, reaching over 20,500 employees to educate them on recognizing and responding to security threats. Conducted thorough risk assessments by analyzing and documenting compliance with ISO 27001 and NIST standards, and provided recommendations for improvements.
- **Outcome:** Achieved a 17% increase in security vigilance among employees, significantly raising overall awareness of security threats. Enhanced the company's compliance with ISO 27001 and NIST standards, contributing to a stronger governance, risk, and compliance (GRC) framework and reducing the company's vulnerability to cyber threats.

Backend Developer - Software Security   **Sep 2019 - Dec 2019**
Bumima Innovations, Toronto, ON
4 months

- **Requirement:** The company needed a real-time integration system for cryptocurrency trading to improve trade efficiency and ensure robust data security.
- **Action Taken:** Developed and implemented a real-time integration system interfacing with 10 cryptocurrency trading APIs using Python. Focused on enhancing trade efficiency and reinforcing data security.

- **Implementation:** Designed, scripted, tested, implemented, debugged, and developed the integration system using Python. Decreased trade latency by optimizing the system and integrated data security measures. Documented third-party network incidents and provided assistance on data security, integrity, and industry best practices.
- **Outcome:** Achieved a 12% improvement in trade efficiency and significantly enhanced data security for cryptocurrency transactions. The system's success underscored the importance of secure and efficient trading operations, contributing to the company's overall performance and reputation in the industry.

PROJECTS

Active Directory: System Administration

- Active Directory Administration: PowerShell (Automated provision, maintaining and development of user accounts).
- Setting up Remote Access Server (RAS) features to support NAT/PAT implementation and maintenance of Windows DNS and DHCP services.
- Skills: DHCP · Active Directory · DNS Administration · NAT · PAT · RAS

Microsoft Azure Sentinel (SIEM)

- Honeypot Deployment and Analysis Used custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third-party API in order to derive geolocation data.
- Configured Log Analytics Workspace in Azure to ingest custom logs containing geographic information (latitude, longitude, state/province, and country).
- Configured Azure Sentinel (Microsoft's cloud SIEM) workbook to display global attack data (RDP brute force) on the world map according to physical location and magnitude of attacks.
- Skills: Microsoft Azure · Powershell · Windows

Nessus Essentials: Vulnerability Management

- Used Nessus Essentials to perform credentialed vulnerability scans against Windows 10 Hosts.
- Conducted vulnerability assessment with Nessus: remediated vulnerabilities.
- Developed automated remediation process to preemptively deal with vulnerabilities from Windows updates and third-party software.