

# Aref Rezai

4091 Sheppard Ave E  
Scarborough, ON, M1S 3H2  
Email: aref.rezaie@gmail.com  
Cell: (647) 562-1919  
[LinkedIn](#)

## OBJECTIVE:

Detail-oriented and proactive IT Technician with a strong foundation in network configuration and system troubleshooting. Certified in Microsoft Security, Compliance, and Identity Fundamentals (SC-900), I am seeking to apply my technical skills and a keen interest in cybersecurity to a Security Operations Center (SOC) role, with the goal of contributing to threat analysis and incident response.

## HIGHLIGHTS OF QUALIFICATIONS:

- Foundational Cybersecurity Knowledge: Certified in Microsoft Security, Compliance, and Identity Fundamentals (SC-900), demonstrating a solid understanding of cybersecurity principles and best practices.
- Incident Response & Analysis: Proven ability to troubleshoot and diagnose system issues under pressure, with recent hands-on lab experience in triaging security alerts and incident analysis.
- Solid understanding of network systems, including TCP/IP and network security defenses, from configuring and optimizing network infrastructure.
- Hands-on experience with security hardware, including the installation and configuration of IP-based security solutions and CCTV systems.

## TECHNICAL SKILLS:

- SIEM Tools (Security Information and Event Management)
- Endpoint Detection & Response (EDR) Tools
- Incident Response and Triage
- Understanding of Malware and Network Attack Vectors
- DDoS Attack Concepts
- Basic Scripting (Python)
- Web Application Security Vulnerabilities (e.g., SQL Injection, XSS)
- Cloud Technologies and Security

## EDUCATION:

**CYBERSECURITY (POSTGRADUATE CERTIFICATE)** 2026

George Brown College, Toronto, ON

**CLOUD COMPUTING TECHNOLOGIES (POSTGRADUATE CERTIFICATE)** 2023

George Brown College, Toronto, ON

**COMPUTER SYSTEMS TECHNOLOGY (3 YEARS ADVANCED DIPLOMA)** 2021

George Brown College, Toronto, ON

## CERTIFICATIONS:

- MS-900 - Microsoft 365 Fundamentals Certified 2023
- SC-900 - Microsoft Security, Compliance, and Identity Fundamentals Certified 2023
- AZ-900 - Microsoft Azure Fundamentals Certified 2023

## **PROFESSIONAL EXPERIENCE:**

### **MATERIAL HANDLER**

**Apr 2025 – Aug 2025**

**DYNEX TECHNOLOGIES**, Chantilly, VA, USA

- Inspected incoming and outgoing goods for quality and quantity against purchase orders and shipping
- Managed and organized inventory for a fast-paced warehouse
- Collaborated with team members to optimize storage solutions and improve material flow
- Accurately packed and scanned inventory for shipments using RF scanners, maintaining precise stock levels and ensuring correct order fulfillment.

### **IT TECHNICIAN**

**Nov 2023 - Jan 2025**

**EasyTech4Business Inc**, Richmond Hill, ON, Canada

- Configured and optimized network systems, enhancing data transmission efficiency and significantly improving user experience.
- Installed, terminated, and tested Ethernet (Cat6) cabling, including RJ45 connectors and keystone jacks, for residential and commercial data/voice networks.
- Provided exceptional support to end-users, fostering strong relationships and enhancing overall service quality.
- Installed and configured CCTV systems, DVRs, and IP-based security solutions.
- Performed comprehensive hardware and software troubleshooting to diagnose and resolve system issues, ensuring optimal performance and minimal downtime.

## **School and Capstone Projects:**

### **Built a Log Analysis and Alerting System**

This project focused on the core skill of a SOC analyst: monitoring and responding to threats using logs.

- **Project Description:** Set up a free or open-source Security Information and Event Management (SIEM) tool like the **Elastic Stack (ELK)** or **Splunk's free tier** in a virtual machine. Configure it to collect logs from a sample host (e.g., Windows Event Logs). Create custom dashboards to visualize key security events and write rules to generate alerts for suspicious activities, such as repeated failed login attempts or unauthorized access.
- **Skills Demonstrated:** **Log Management, SIEM, Threat Monitoring, Alerting, Data Analysis, and Basic Scripting.**

### **Incident Response and Digital Forensics**

- **Project Description:** Simulate a security incident, such as a compromised web server. Using a digital forensics tool, perform an investigation of the compromised system to identify how the attacker gained access, what they did, and what data they may have exfiltrated. Documented every step of the process, from initial containment to a full report of the findings.
- **Skills Demonstrated:** **Digital Forensics, Incident Response Lifecycle, Malware Analysis, Risk Analysis, and clear Documentation.**