

# Niknaz Sadehvandi

Matthews, NC • (202) 600-1591 • Email: [sadvandniknaz0@gmail.com](mailto:sadvandniknaz0@gmail.com)

LinkedIn • GitHub • Portfolio: <https://niknaz-65.github.io/>

## AWARDS

**Winner:** UMGC, 2025, President's List (4.0 GPA).

**Winner:** Sunset Auto Sales, 2024, Process Improvement Recognition.

**Winner:** Sunset Auto Sales, 2023, Excellence in Technical Support.

**Winner:** Sunset Auto Sales, 2023, High-Volume Ticket Resolution (300+ tickets).

## CERTIFICATIONS

Python Basics for Data Science (IBM)

R Programming Fundamentals (Stanford Online)

## EXPERIENCE

**IT Support Technician**, Sunset Auto Sales., Charlotte, NC (2020 – Present)

- Closed 300+ Windows hardware/software tickets yearly; improved first-time resolution.
- Managed 25+ user accounts (password resets, permissions updates, 2FA support).
- Performed workstation builds (imaging, AV updates, configuration).
- Conducted malware cleanup and endpoint health checks on 20+ devices.
- Reduced repeat incidents by tightening SOP documentation.

**IT Administrator / Helpdesk**, Kafpoush., Germantown, MD (2012–2018)

- Supported 40+ Windows endpoints (system maintenance, AV updates, permissions).
- Performed malware cleanup, workstation installations, and backup procedures.

**Technical Assistant, Ganjineh.**, Tehran, Iran (2008–2010)

- Installed CCTV, access control, and basic network infrastructure.
- Supported IT documentation, hardware setup, and troubleshooting.
- Assisted engineers with physical security implementations

## PROJECTS

**Splunk SIEM Analysis:** Built detections for failed logins, privilege changes, anomalous processes; designed Dashboards.

**Malware Analysis:** Extracted 20+ IOCs; analyzed registry, process, and C2 behavior.

**Threat Intelligence (OSINT):** Processed 30,000+ indicators from OTX/LevelBlue.

**Python Network Recon Toolkit:** Automated Nmap scanning; generated HTML reports.

**Traffic Simulation (Java, OOP, Multithreading):** Built a multi-threaded Java Swing simulator with synchronized car and traffic-light threads; implemented event-driven controls and designed UML class architecture

**Digital Forensics Labs (UMGC):** Investigated persistence, unauthorized accounts, IIS log anomalies, SSHexfiltration.

## EDUCATION

M.S. Cybersecurity Technology | UMGC | GPA 4.0

B.S. Information Technology | University of Phoenix | Magna Cum Laude

A.A. Information Technology | CPCC

A.S. Architectural Drawing | IAU

## SKILLS

Windows, Linux, Active Directory, Splunk, Wireshark, Nmap, Nessus, FTK Imager, Autoruns, TCP/IP, DNS, DHCP, Python, PowerShell, OSINT, vulnerability scanning, forensic imaging.