NIKNAZ SADEHVANDI

Matthews, NC | (202) 600-1591 | sadvandniknaz0@gmail.com

LinkedIn: linkedin.com/in/niknaz-sadehvandi-a34179325 | GitHub: github.com/niknaz-65 | Portfolio: niknaz65.github.io

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on experience in incident response, vulnerability analysis, malware investigation, forensic imaging, and log monitoring. Skilled in Windows/Linux security auditing, packet capture analysis, threat detection with Splunk, and malware behavior analysis using msfvenom. Strong understanding of MITRE ATT&CK, NIST 800-86, SIEM workflows, and evidence handling.

PROFESSIONAL EXPERIENCE

Junior Cybersecurity Analyst | Sunset Auto Sales (03/2020 – Present)

Executed SOX ITGC testing, validating system configurations, password policies, change management, and user access.

Improved audit readiness by 20% through streamlined documentation.

Reduced false positives by 25% and triage time by 30%.

Enhanced Splunk monitoring by integrating new threat-intelligence feeds.

Customer Service Associate | Bloomingdale's (05/2015 – 12/2019)

Resolved 100+ weekly issues with 90% first-contact resolution.

Trained new associates and improved documentation accuracy by 25%.

Administrator / IT Helpdesk Support | Kafpoush (12/2010 – 02/2015)

Reduced system vulnerabilities by 30% through IT support and security tool optimization.

Performed biometric and user access validation for 100+ audits annually.

Architectural & IT Assistant | Ganjineh (03/2004 – 06/2009)

Installed CCTV, access control, and security systems, increasing compliance by 30%.

PROJECTS

Cybersecurity & Digital Forensics Labs | UMGC (2025)

Performed forensic imaging, hashing (MD5/SHA1), and evidence of preservation.

Analyze malicious payloads using msfvenom; validated IOCs with VirusTotal.

Investigated persistence with Autoruns and registry tools.

Configured Linux servers; conducted Nmap scans.

Captured and analyzed packets via Wireshark & NetworkMiner.

Digital Forensics & Incident Response | UMGC

Investigated intrusions including SSH abuse and privilege escalation.

Documented IR findings aligned with MITRE ATT&CK & NIST.

Custom ALU & CPU Architecture Design | Logisim Evolution (2025)

A functional Arithmetic Logic Unit (ALU) and Central Processing Unit (CPU) were created and simulated using Logisim-Evolution. The program was used in conjunction with digital logic circuits, binary arithmetic, and control flow design.

Executed routine operations including adding, subtracting, bit shifting, logical AND/OR/NOT, and EQ, GT, and LT comparison flags.

Arrangement of control signals, registers, data buses, and multiplexers for the execution of instructions.

Verified data paths and flag behavior through live simulation to show CPU-level processing.

EDUCATION

M.S. Cybersecurity Technology, University of Maryland Global Campus (GPA 4.0)

B.S. Information Technology, University of Phoenix (Magna Cum Laude)

A.A. Information Technology, Central Piedmont Community College

A.S. Architectural Drawing, Islamic Azad University, Iran (GPA 18.11/20)

TECHNICAL SKILLS

Splunk, FTK Imager, Autopsy, NetworkMiner, Wireshark, Nmap, Linux services, msfvenom, VirusTotal, Python, PowerShell, Bash.

CERTIFICATIONS

Python Basics for Data Science, IBM (2024)

R Programming Fundamentals, Stanford Online (2024)