NIKNAZ SADEHVANDI

Matthews, NC • (202) 600-1591 • sadvandniknaz0@gmail.com • https://github.com/niknaz-65

Cybersecurity Analyst

Cybersecurity Analyst with hands-on experience in SIEM monitoring, endpoint telemetry, log analysis, and SOC investigations. Founder of Nikki IT & Security Consulting, delivering Elastic SIEM ingestion pipelines, Sysmon and Zeek telemetry, and Windows security assessments aligned with MITRE ATT&CK. M.S. Cybersecurity Technology (4.0 GPA, President's List).

WORK EXPERIENCE

Nikki IT & Security Consulting | Remote | Dec 2025 – Present

Founder & Cybersecurity Consultant

- Engineered Fleet-managed Elastic SIEM endpoint pipeline using Sysmon v15+; ingested process creation, network connection, and PowerShell events; validated SOC visibility using KQL.
- Deployed Zeek network sensor on Ubuntu 24.04; ingested 1,500+ structured network events into Elastic SIEM via Filebeat; validated real-time telemetry in Kibana Discover.
- Conducted Windows endpoint security audits analyzing authentication failures, firewall rules, and active connections; validated outbound traffic and delivered hardening recommendations.

Sunset Auto Sales | March 2019 – Present

Cybersecurity | IT Support Technician

- Supported and secured Windows endpoints; performed malware investigations, MFA enforcement, endpoint troubleshooting, and system imaging.
- Maintained security documentation and resolved high-volume support tickets across operational systems.

Kafpoush | Oct 2011 – Feb 2016

IT Administrator | Helpdesk

- Executed malware remediation, patch management, access control updates, and forensic-style system checks.
- Provided Tier 1–2 support, incident documentation, and endpoint maintenance.

Ganjineh | Oct 2008 – July 2010

Technical Assistant

- Installed and supported CCTV, access control systems, and network infrastructure.
- Performed troubleshooting and routine maintenance.

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

CERTIFICATIONS

Python Basics for Data Science

IBM

AWARDS & SCHOLARSHIPS

President’s List

UMGC

Process Improvement Recognition, Excellence in Technical Support, High-Volume Ticket Resolution

PROJECTS

SOC Dashboarding & Alert Triage (Splunk SIEM)

Built SOC dashboards and analyst triage views for Windows security events and anomalous authentication detection.

Network Reconnaissance & SOC Automation (Python)

Developed an Nmap-based automation wrapper with structured output and report generation.

Threat Intelligence & Malware Analysis

Conducted static and behavioral malware analysis; processed 30,000+ indicators and extracted IOCs related to persistence and execution.

Entry-Level DFIR & Incident Investigation Labs

Investigated DFIR scenarios using IIS logs, Base64 decoding, SSH exfiltration analysis, and endpoint artifacts with Autopsy, FTK Imager, and Wireshark.

SKILLS

SIEM & Log Analysis: Elastic SIEM, Filebeat, KQL, Splunk, Sysmon, Windows Event Logs, Zeek

Detection Frameworks: MITRE ATT&CK

Endpoint & Forensics: Autopsy, FTK Imager, Autoruns, Malware Analysis

Networking & Recon: DHCP, DNS, netstat, Nmap, TCP/IP, Wireshark

Scripting & Automation: Bash, PowerShell, Python

Platforms: Active Directory, AWS (Fundamentals), Azure (Fundamentals), Linux, Windows

Security Standards: NIST, SOX ITGC

Tools: auditpol, Event Viewer, Nessus/Tenable, VirusTotal