NIKNAZ SADEHVANDI

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

Cybersecurity Analyst

Cybersecurity Analyst with hands-on experience in **endpoint security, SIEM monitoring, log analysis, and security investigations**. Founder of Nikki IT & Security Consulting, delivering **Elastic SIEM ingestion, Sysmon and Zeek telemetry validation, Windows security assessments, and hardening recommendations** aligned with MITRE ATT&CK, NIST, and SOX ITGC, **supporting IT and business stakeholders with clear reporting and documentation**. M.S. Cybersecurity Technology (GPA 4.0, President's List).

WORK EXPERIENCE

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

Founder & Cybersecurity Consultant

- Engineered and validated a Fleet-managed **Elastic SIEM endpoint pipeline** using Sysmon v15+; analyzed process creation, network connections, and PowerShell activity using KQL to support investigations and reporting.
- Deployed a **Zeek network sensor** on Ubuntu 24.04; ingested and validated **1,500+ structured network events** into Elastic SIEM via Filebeat; confirmed real-time visibility and data quality in Kibana Discover.
- Conducted **Windows endpoint security audits**, analyzing authentication failures, firewall rules, and active connections; validated outbound traffic and delivered actionable hardening and monitoring recommendations.

Sunset Auto Sales | March 2019 – Present

Cybersecurity | IT Support Technician

- Supported **60+ Windows endpoints** and resolved **25–30 tickets per week** involving malware triage, MFA, and endpoint issues.
- Maintained security and incident documentation while resolving high-volume operational and security-related support tickets.

Kafpoush | Oct 2011 – Feb 2016

IT Administrator | Helpdesk

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

Ganjineh | Oct 2008 – July 2010

Technical Assistant

- Installed and supported CCTV systems, access control solutions, 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

SECURITY PROJECTS (OPERATIONAL)

SOC Dashboarding & Alert Triage (Splunk SIEM)
Built dashboards and analyst triage views for Windows security events and anomalous authentication activity to support investigation and escalation.

Network Reconnaissance & SOC Automation (Python)
Developed an Nmap-based automation wrapper with structured output to support security analysis and reporting.

Threat Intelligence & Malware Analysis
Conducted static and behavioral malware analysis; processed **30,000+ indicators** and extracted IOCs related to persistence and execution techniques.

DFIR & Incident Investigation Labs
Investigated DFIR scenarios involving IIS logs, Base64 decoding, SSH-based exfiltration, and endpoint artifacts using Autopsy, FTK Imager, and Wireshark.

SKILLS

SIEM & Monitoring: Elastic SIEM, Splunk, Filebeat, KQL, Kibana
Telemetry: Sysmon, Windows Event Logs, Zeek
Frameworks & Standards: MITRE ATT&CK, NIST, SOX ITGC
Endpoint & Forensics: Autopsy, FTK Imager, Autoruns, Malware Analysis
Networking: TCP/IP, DNS, DHCP, netstat, Nmap, Wireshark
Scripting: PowerShell, Bash, Python
Platforms & Tools: Active Directory, Linux, Windows, AWS (Fundamentals), Azure (Fundamentals), Nessus/Tenable, Event Viewer, VirusTotal, auditpol