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 12/2025 - Present
Founder & Cybersecurity Consultant Remote

- Endpoint Detection Engineering (Elastic SIEM + Sysmon): Engineered a Fleet-managed Elastic SIEM endpoint pipeline using Sysmon v15+; collected process creation (Event ID 1), network connections (Event ID 3), and PowerShell logging (Event ID 4104); validated ingestion and visibility using KQL for SOC investigations.
- Network Telemetry Integration (Zeek + Filebeat): Deployed Zeek network sensor on Ubuntu 24.04; generated structured network logs (conn, dns, http) and ingested 1,500+ events into Elastic SIEM via the Filebeat Zeek module; validated real-time network telemetry in Kibana Discover.
- Windows Endpoint Security Audits & Hardening: Conducted comprehensive endpoint security assessments by analyzing authentication logs (Event ID 4625), audit policies, firewall rules (inbound/outbound), and active network connections (netstat -ano); correlated processes to PIDs, verified legitimacy of outbound traffic, established IOC baselines, and delivered actionable recommendations to reduce attack surface.
- SOC Log Analysis (Authentication Monitoring): Investigated failed authentication activity (Event ID 4625), established baseline behavior, ruled out brute-force attempts, and provided recommendations for ongoing monitoring and enhanced audit logging aligned with SOC best practices.

Sunset Auto Sales 01/2020 - Present
Cybersecurity / IT Support Technician

- Performed malware investigations, log queries, endpoint troubleshooting, MFA enforcement, system imaging, and detailed security documentation.

Kafpoush 01/2012 - 01/2018
IT Administrator / Helpdesk

- Executed malware remediation, patch management, access control updates, forensic-style system checks, and incident documentation.

Ganjineh 01/2008 - 01/2010
Technical Assistant

- Installed and verified CCTV, access control systems, and network infrastructure; supported troubleshooting and ongoing 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 & TRAINING

Python Basics for Data Science
IBM

R Programming Fundamentals

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 detections for Windows security events; developed analyst triage views to identify anomalous authentication and system activity.

Network Reconnaissance & SOC Automation (Python)

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

Threat Intelligence & Malware Analysis

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

Entry-Level DFIR & Incident Investigation Labs

Investigated network intrusion and DFIR scenarios involving IIS logs, Base64 decoding, SSH-based data exfiltration, and endpoint artifacts using 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, Malware Analysis, Sysinternals (Autoruns)

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