NIKNAZ SADEHVANDI

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

Portfolio: https://nscybersecurity.com/ | GitHub: https://github.com/niknaz-65 |

LinkedIn: linkedin.com/in/niknaz-sadehvandi-a34179325

Cybersecurity Analyst

Target roles: SOC Analyst, Cybersecurity Analyst, Incident Response Analyst, SIEM Analyst

Cybersecurity Analyst with experience in SIEM monitoring, endpoint and network telemetry analysis, and security investigations. Founder of NS Cybersecurity, delivering Elastic SIEM ingestion pipelines, Sysmon and Zeek telemetry validation, Windows security assessments, and hardening recommendations aligned with MITRE ATT&CK, NIST, and SOX ITGC. M.S. Cybersecurity Technology (GPA 4.0, President's List).

WORK EXPERIENCE

NS Cybersecurity | Remote | Dec 2024 – Present

Founder & Cybersecurity Consultant

- Designed and deployed a Fleet-managed Elastic SIEM endpoint pipeline using Sysmon v15+ to support endpoint visibility and investigations.
- Analyzed Windows process execution, authentication activity, firewall events, and outbound connections to identify security risks.
- Deployed Zeek network monitoring on Ubuntu 24.04; ingested structured DNS and HTTP telemetry into Elastic SIEM to support network visibility and detection.
- Validated telemetry accuracy and data completeness using Kibana Discover and targeted KQL queries.
- Conducted simulated alert investigations and delivered actionable hardening and monitoring recommendations.
- Handled weekly Elastic SIEM alerts from initial triage through investigation, containment, and reporting in an NS Cybersecurity lab environment.
- Delivered endpoint hardening and SIEM monitoring recommendations for small-business environments under NS Cybersecurity.

Sunset Auto Sales | March 2019 – Present

Cybersecurity & IT Support Technician

- Supported and secured 60+ Windows endpoints in a small business environment; resolved 25–30 tickets per week involving malware triage, MFA enforcement, and endpoint issues.

- Maintained security and incident documentation while resolving high-volume operational and security-related support tickets.
- Reduced recurring malware incidents by about 50% by enforcing MFA, tightening endpoint configurations, and standardizing basic security hygiene.

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 | University of Maryland Global Campus (UMGC) | GPA: 4.0

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

A.A. Information Technology | Central Piedmont Community College (CPCC)

A.S. Architectural Drawing | IAU

CERTIFICATIONS & TRAINING

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; prioritized alerts, documented findings, and escalated high-risk events to senior staff (simulated).

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 Scenarios

- 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, Nessus/Tenable, Event Viewer, VirusTotal, auditpol
Endpoint Tools: Microsoft Defender; EDR concepts (alerts, isolation, containment)