

NIKKI SADVAND

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

Portfolio: <https://nscybersecurity.com/> | GitHub: <https://github.com/Nikki-65> |

LinkedIn: [linkedin.com/in/Nikki-Sadvand-a34179325](https://www.linkedin.com/in/Nikki-Sadvand-a34179325)

Cybersecurity Analyst

Cybersecurity Analyst with hands-on experience in SIEM monitoring, alert triage, endpoint and network telemetry analysis, and structured incident investigations. Experienced in Elastic-based detection workflows and incident response processes aligned with MITRE ATT&CK and NIST 800-61.

WORK EXPERIENCE

NS Cybersecurity | Remote | Dec 2024 – Present

Security Operations Engineer — NS Cybersecurity (Independent Lab Environment)

- Designed, deployed, and operated a Fleet-managed Elastic SIEM endpoint pipeline using Sysmon v15+ to support endpoint visibility and security investigations.
- Deployed Zeek network monitoring on Ubuntu 24.04; ingested structured DNS and HTTP telemetry into Elastic SIEM to support network-layer detection and anomaly analysis.
- Validated telemetry accuracy and data completeness using Kibana Discover and targeted KQL queries to ensure reliable detection outcomes.
- Analyzed Windows process execution, authentication events, firewall logs, and outbound network connections to detect anomalous behavior and validate potential security incidents.
- Executed structured SOC investigations following NIST 800-61 incident response lifecycle, correlating endpoint and network telemetry to validate findings.
- Handled weekly Elastic SIEM alerts, performing tiered triage, investigation, containment validation, and structured incident documentation.

Sunset Auto Sales | March 2019 – Present

Cybersecurity & IT Support Technician

- Supported and secured 60+ Windows endpoints within a small Active Directory-based 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 approximately 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 Splunk dashboards and triage workflows for Windows authentication anomaly detection, prioritizing alerts and documenting escalation findings.

Network Reconnaissance & SOC Automation (Python)

- Developed an Nmap-based automation wrapper with structured output to support security analysis and reporting.

Threat Intelligence & Malware Analysis

- Processed 30,000+ threat indicators from open-source intelligence feeds and malware sandboxes, extracting actionable IOCs to support detection and hunting use cases.

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, Kibana, KQL

Incident Response & Detection: Sysmon, Windows Event Logs, Zeek, EDR investigation workflows

Threat & DFIR Tools: Autopsy, FTK Imager, Autoruns, VirusTotal

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

Scripting: PowerShell, Python, Bash

Platforms: Active Directory, Windows, Linux

Frameworks: MITRE ATT&CK, NIST 800-61, SOX ITGC