Niknaz Sadehvandi

Matthews, NC | sadvandniknaz0@gmail.com | (202) 600-1591 | LinkedIn: www.linkedin.com/in/niknaz-sadehvandi-a34179325

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 5+ years of experience in vulnerability management, digital forensics, incident response, and enterprise security operations. Skilled in security tools, compliance audits (PCI, SOX, financial), and business continuity/disaster recovery planning. Adept at collaborating across IT, risk, and compliance teams to design secure architectures, improve governance, and lead investigations. Holds an M.S. in Cybersecurity Technology (4.0 GPA, President's List) and certifications in Python and R. Recognized for delivering actionable security solutions, reducing risk exposure, and enhancing enterprise resilience.

TECHNICAL SKILLS

Security & Forensics: Vulnerability Assessments · Incident Response · Digital Forensics · Evidence Collection · Security Audits · Proof of Concept Testing · Phishing Response · XDR Management

Enterprise Security: Business Impact Analysis · Security Architecture · Governance & Policies · Standards/Baselines · Business Continuity · Disaster Recovery

Systems & Platforms: Windows · Linux · Mac · AWS · Network Devices · Secure Configurations · Application Security

Tools & Programming: Tenable · Splunk · Wireshark · FTK Imager · Autopsy · Autoruns · VirusTotal · Python · Java · R · AI-Assisted Analysis

Soft Skills: Leadership · Documentation · Vendor Liaison · Team Training · Communication · Problem-Solving

PROFESSIONAL EXPERIENCE

Junior Cybersecurity Analyst | Sunset Auto Sales, Charlotte, NC | 2023–Present

- Conduct vulnerability assessments and incident management across Linux, Windows, and Mac environments.
- Monitor and manage Splunk, Wireshark, and XDR tools, triaging phishing alerts and mitigating risks.
- Support PCI audits, quarterly access reviews, and RBAC policy implementation.
- Perform forensic investigations; deliver reports used for financial audits and compliance reviews.
- Collaborate with leadership to update security policies, procedures, and baselines.
- Develop proof-of-concept solutions for emerging security needs.

• Contribute to disaster recovery and business continuity planning, ensuring resiliency.

Administrator | Kafpoush, Germantown, MD | 2010–2015

• Administered IT systems, user accounts, and access controls for secure daily operations.
• Conducted log reviews and internal security audits; escalated anomalies for investigation.
• Automated reporting and optimized database management, reducing manual errors by 40%.
• Partnered with vendors to implement infrastructure hardening and secure configurations.

PROJECTS (ACADEMIC)

Digital Forensics & Incident Response Lab – University of Maryland Global Campus | Jan – Mar 2025

• Investigated Windows intrusion using FTK Imager, Autopsy, and Autoruns.
• Identified persistence mechanisms, unauthorized accounts, and SSH-based exfiltration.
• Analyzed IIS logs to confirm credential compromise and lateral movement.
• Produced a remediation plan: system rebuild, IP blacklisting, and ongoing monitoring.

EDUCATION

Master of Science in Cybersecurity Technology | University of Maryland Global Campus | 08/2024 – 07/2025

- President's List | GPA: 4.0

Bachelor of Science in Information Technology | University of Phoenix | 10/2022 – 02/2024

- Magna Cum Laude

WEBSITES, PORTFOLIOS, PROFILES

HTTPS://NIKNAZ-PORTFOLIO.GITHUB.IO/NIKNAZ-PORTFOLIO/

www.linkedin.com/in/niknaz-sadehvandi-a34179325

CERTIFICATIONS

- Python Basics for Data Science – IBM, 2024-01
- R Programming Fundamentals – Stanford Online, 2024-01