

## Nisha P McDonnell

eunishap@gmail.com • [Linkedin](#) • [Github](#) • [Blog](#)

Top 5% on TryHackMe

### SUMMARY

---

Network Security Engineer with a passion for strengthening cyber defenses, conducting thorough investigations, and effectively handling incidents. Committed to continuous learning and skill development through hands-on projects using home lab and active participation in CTF events.

### SKILLS

---

- **Security Tools:** Splunk, Vulnerability Patching, Palo Alto Firewall, Nessus, OpenVAS, Suricata IDS, Microsoft Sentinel SIEM
- **Operating Systems:** Windows, Linux
- **Cloud Platforms:** Microsoft Azure, AWS
- **Infrastructure as Code (IAC):** Terraform
- **Virtualization:** VMware
- **Network Devices:** Cisco Routers, Switches, Dell Servers, Cisco Unified Communications
- **Active Directory:** O365, LAN/WAN
- **Network Analysis:** Wireshark, Traffic Analysis, Network Protocols, tcpdump
- **Languages:** PowerShell, Python, YAML, JSON
- **Others:** GitHub, HTML, Service Now, Prognosis IR Cloud

### EXPERIENCE

---

#### CDW | Remote, TX

##### Engineer II – Managed Services

Nov 2020 – Present

- Managing critical PKI certificate installations, enhancing network security
- Investigates security advisories and implements and coordinates patching activities to mitigate critical vulnerabilities
- Executes problem-solving skills to identify solutions to complex network issues and providing root cause analysis
- Improves incident resolution time by 25% through the implementation of ITIL processes
- Monitored systems for anomalies through network traffic analysis and log monitoring

#### CDW | Remote, TX

##### Network Consulting Engineer

Nov 2018 – Nov 2020

- Provide support to designing, planning, and building communications networks
- Configuring LAN switches and VPN devices to support voice communications networks
- Used automation tools for the deployment, migration, and upgrade of UC Application servers
- Analyzed existing voice and data networks, providing recommendations and solutions
- Successfully achieved an average 85% of expected billable revenue targets

**CDW | Remote, TX**

**Associate Consulting Engineer**

**Mar 2017 – Nov 2018**

- Analyzed existing voice and data networks, providing recommendations and solutions
- Used automation tools for the deployment, migration, and upgrade of UC Application servers

**Cypress-Fairbanks ISD | Remote, TX**

**Instructor, Technology Applications**

**Aug 2009 - Mar 2017**

- Implemented and secured applications, web-based platforms, and content management systems
- Maintained confidentiality and privacy of student and staff information in compliance with security policies and procedures
- Protected student data and integrated technology for quality curriculum and instruction

## **KEY PROJECTS**

---

### **Open-Source SOC Home Lab**

- Monitoring, Logging, SIEM, Security, EDR, Threat Intelligence, IDS/IPS, Scanning

### **Cybersecurity Vulnerability Management Project (Nessus and OpenVAS)**

- Executed credentialed vulnerability scans and remediated vulnerabilities, enhancing cybersecurity posture

### **Azure Cloud Detection Project : Sentinel SIEM**

- Utilized PowerShell scripting, Windows Event Viewer, and APIs for real-time attack visualization.

## **CERTIFICATIONS**

---

- CompTIA Security+ CE
- Microsoft Azure Administrator Associate
- Microsoft Azure Network Engineer Associate
- ITIL Foundations v3
- Cisco Certified Network Associate (CCNA)
  - CCNP Enterprise Core Specialist

## **EDUCATION**

---

- Master's in Cybersecurity and Information Assurance
  - Western Governor's University
  - In progress
- Bachelor of Science, University of Louisiana at Lafayette