Simon Reyes
Winsted, CT 06098
🖂 simonreyes345@gmail.com | ☎ (646) 821-2419
🔗 LinkedIn | GitHub

Professional Summary

IT and cybersecurity professional with 6+ years of hands-on experience across network administration, endpoint protection, and security operations. Skilled in threat detection, incident response, compliance readiness (CMMC, NIST, PCI), and secure infrastructure deployment. Proven success supporting diverse business environments as both an in-house technician and freelance consultant. Currently operating in an MSP setting with advanced tools like SentinelOne, Huntress, Proofpoint, SonicWall, and OpenVPN. Strong focus on developing hybrid Red/Blue Team capabilities through continuous lab work and project execution.

Certifications

- **CompTIA Security+** – May 2025
- **CompTIA Network+** – Dec 2023
- **CompTIA A+** – Mar 2019

Core Competencies

- Endpoint Detection & Response (Huntress, SentinelOne, Proofpoint)
- Firewall, VPN, and VLAN Configuration (SonicWall, Cisco, OpenVPN)
- Microsoft 365, Exchange, Azure AD, Entra ID
- DNS Security (SPF, DKIM, DMARC)
- Compliance Standards: CMMC, NIST 800-171, PCI-DSS
- Remote Monitoring (ConnectWise, LabTech Automate)
- Backup & Disaster Recovery (Veeam)
- GPO and Active Directory Management
- Threat Isolation & Incident Response
- PowerShell, Python (basic), YAML (Sigma Rules)

Professional Experience

Jr. Network Administrator

TAB Computer Systems – East Hartford, CT
March 2024 – Present

- Support over 100 managed clients, resolving endpoint, server, email, and firewall issues.
- Perform Huntress and SentinelOne remediation, including threat isolation and persistence removal.
- Configure SonicWall firewalls, VLANs, VPNs, and Proofpoint email filtering rules.
- Administer Microsoft 365 hybrid and cloud-only tenants, including Exchange Online and On-Prem.
- Set up DUO MFA, edit GPOs for security enforcement, and implement DKIM/SPF/DMARC records.
- Assist with client compliance across CMMC, PCI-DSS, and NIST frameworks.
- Collaborate with internal departments to triage escalated issues, document findings, and apply remediations.
- Use ConnectWise and LabTech Automate for endpoint oversight and ticket management.

Security Analyst

Security Validation – Newark, NJ
Feb 2023 – Jan 2024

- Triaged and remediated incidents across hotel and hospitality networks involving POS (Aloha), PMS (Opera), and access control systems (Saflok).
- Performed endpoint and network investigations using proprietary tools and threat intelligence feeds.
- Responded to vishing/phishing simulations without error; supported security awareness campaigns.
- Participated in security audits and hardening of hospitality infrastructure.
- Led junior team members in troubleshooting and documented edge-case issues in internal knowledge base.

IT Consultant (Freelance)
Self-Employed – Goldsboro, NC / Remote
Aug 2017 – Feb 2022

- Configured site-to-site OpenVPN tunnels and Cisco ISR routers for remote client connectivity.
- Deployed secure CyberPanel environments, managed DNS records, and hardened Linux VPS servers.
- Troubleshot networks and endpoints for small businesses including veterinary clinics and a radio station.
- Delivered DNS security (SPF/DKIM/DMARC), firewall rules, mail migration, and backup solutions.
- Diagnosed system performance issues, conducted malware cleanup, and handled legacy system upgrades.
- Created documentation for IT continuity and disaster recovery readiness.

IT Technician III
ITSS – Goldsboro, NC
Sep 2019 – Apr 2020

- Installed, repaired, and optimized Windows servers and LAN infrastructure.
- Ran cable, configured Cisco routers and VoIP systems, and deployed smart devices.
- Maintained logs, client documentation, and billing for projects.
- Using Ticketing system I scheduled picked up remote and onsite tickets and scheduled them accordingly, after doing so I would submit my jobs for billing to my immediate supervisor.

Technical Proficiencies

Security Tools: SentinelOne, Huntress, Proofpoint, DUO, OpenVPN, Sysmon
Infrastructure: SonicWall, Cisco ISR, VLANs, DHCP/DNS, Exchange (On-Prem/Hybrid)
Cloud: Microsoft 365, Azure AD, Entra, SharePoint, Veeam, CyberPanel
Scripting & Automation: PowerShell, LabTech Scripts, Python (basic), YAML (Sigma Rules)
Monitoring & Management: ConnectWise, LabTech Automate, Event Viewer, Wireshark
Platforms: Windows Server, Linux/Kali, Hyper-V, VMware

Education

High School Equivalency

Soft Skills

- Calm and effective in high-stress environments
- Strong documentation and technical writing skills
- Ownership-minded with follow-through
- Collaborative with multi-department teams
- Lifelong learner — building threat hunting and malware analysis labs