Steven Hosek

Network & Security Operations Technician

New York, NY | steve@stevenhosek.dev | linkedin.com/in/stevenhoseknyc | stevenhosek.dev

Seeking SOC Analyst, Network Security Analyst, or Infrastructure Security roles · Remote preferred

SUMMARY

Network and security operations technician with five years in 24x7 managed services, supporting 10+ client organizations across 150+ sites with security event triage, incident response, and phishing analysis.

EXPERIENCE

NOC Technician I

Oct 2021 – Present

Sourcepass · Bohemia, NY (On-site)

- Monitor and support network and security operations for 10+ client organizations across 150+ sites, including data centers, triaging and actioning 50+ alerts per 12-hour shift.
- Triage security events with incident response playbooks, correlating SIEM, firewall, and endpoint logs and checking IOCs to separate false positives from real impact.
- Analyze phishing and email threats in Defender for Office 365 and Proofpoint, investigate endpoint alerts in FortiEDR and Cylance, and run threat hunts in Microsoft Sentinel and LogRhythm.
- Troubleshoot site-to-site VPNs, firewall policies, routing, BGP, and WAN connectivity across Fortinet, Palo Alto / Panorama, Cisco, and Meraki, plus 802.1X / Cisco ISE.
- Support vulnerability remediation, upgrade planning, and certificate maintenance for Cisco IOS XE, Nexus, CUCM / Unity / CER, Windows Server / AD, VMware, Nutanix, and NetScaler.
- Own tickets end to end in ConnectWise, coordinate vendor TAC and ISP escalations, keep clients updated during incidents, and validate service restoration.

Service Desk Analyst (Raytheon contract)

Jun 2021 – Oct 2021

DXC Technology · Remote

- Provided Level 1 support in a security-sensitive defense contractor environment, including executive and VIP users.
- Resolved identity, MFA, and access issues involving smart cards and hardware / software tokens; escalated in ServiceNow.

Help Desk Analyst (The Freeman Company contract)

Apr 2021 – Jul 2021

Infogain · Remote

- Provided Level 1 and 2 support by phone, chat, and email in a high-volume enterprise environment.
- Handled account, group, and mailbox requests in Active Directory, Exchange, Office 365, and Okta.

Specialist

Oct 2019 – Feb 2020

Apple · Lake Grove, NY

- Helped customers choose and set up Apple devices and services.

HOME LAB

Virtualization & Backup: Three-host Proxmox VE environment; Proxmox Backup Server writing to a Windows SMB share.
Monitoring: Prometheus, Alertmanager, Blackbox Exporter, Grafana, and Netdata dashboards and availability alerts.
Network Security: FortiWiFi with VLAN segmentation, quarantine rules, AdGuard Home DNS filtering, and Tailscale.
Identity & PKI: Active Directory (two DCs), Authentik SSO, step-ca internal CA, Caddy TLS reverse proxy, Passbolt vault.

TECHNICAL SKILLS

Security Operations: Incident response, phishing analysis, IOC investigation, threat hunting, vulnerability management, SOAR, NIST
Firewalls: FortiGate, FortiAnalyzer, Palo Alto / Panorama, Cisco FMC · **EDR & Email:** FortiEDR, Cylance, Defender O365, Proofpoint
SIEM & ITSM: LogRhythm, Microsoft Sentinel, Splunk, OpsGenie · ConnectWise, ServiceNow, IT Glue
Networking: Cisco IOS / IOS-XE, Cisco Nexus, Meraki, BGP, VLANs, GRE / IPsec VPN, DHCP / DNS
Identity & Access: Active Directory, Cisco ISE, RADIUS / 802.1X / MAB, PKI & certificates, smart card & MFA
Systems: Windows Server, Linux, VMware vCenter, Nutanix Prism, Proxmox, SQL Server, NetScaler, M365, PowerShell / Bash
Voice & Video: Cisco CUCM / Unity / CER, SIP, E911 / ELIN, Milestone XProtect
AI Tools: Prompt engineering, ChatGPT / Codex, Claude / Claude Code, Gemini, self-hosted open-weight models
Certifications: Fortinet FortiGate 7.6 Operator · Cisco CCNA (in progress)