Jonathan Humbert

Greeneville, TN 37745 dhumbert@memphis.systems (423) 552-0070

Professional Summary

Driven cybersecurity professional with 24+ years of hands-on IT experience and a strong focus on threat detection, incident response, and vulnerability management. Adept at creating and tuning detection rules, hunting IOCs, and identifying subtle anomalies missed by automated tools. Holds Security+, CEH Master, and CompTIA AI Essentials; currently pursuing CySA+. Experienced with SIEMs, EDRs, and vulnerability scanning tools across enterprise and multi-site retail environments. Skilled in bridging technical details for non-technical audiences.

Core Competencies

- Threat Detection & IOC Hunting
- Incident Response & Recovery
- Vulnerability Scanning & Remediation
- EDR Deployment & Tuning (Bitdefender GravityZone)
- SIEM Management (Wazuh) & Custom Rule Creation
- Phishing Analysis & Email Security Rule Writing
- Firewall Rule Configuration & Network Defense
- Nessus, OpenVAS, Wireshark, UTM Administration
- Windows Desktop & Server, Active Directory, Linux (Kali, ParrotOS)
- Proxmox, Hyper-V Virtualization
- Python & PowerShell Scripting (Lite)

Professional Experience

Director of IT & Cybersecurity Greeneville Oil & Petroleum, INC. Greeneville, TN

April 2022 – Present

- Lead cybersecurity operations for 32 retail locations, securing 200+ endpoints, 55 POS systems, and enterprise infrastructure.
- Improved real time threat visibility but creating and tuning Wazuh SIEM detection rules, dashboard and alerts. Enabling faster incident response.
- Deployed and managed Bitdefender GravityZone EDR created custom exclusion and detection rules, reducing false positives and improved identification of real threats.
- Conducted regular Nessus vulnerability scans, remediating findings to reduce security gaps and maintain compliance with industry standards.

- Investigated phishing attempts via email header/source analysis; implemented targeted rules in Bitdefender email security to block future attacks.
- Conducted network traffic analysis to identify and disrupt command and control connections, preventing data exfiltration.
- Developed and deployed targeted firewall rules on UTM appliances to block ongoing malicious traffic, immediately reducing active threat activity.
- Led full recovery of critical infrastructure after a server room fire, restoring core systems within 24 hours and preventing extended downtime.

IT Specialist Greeneville Oil & Petroleum, INC. Greeneville, TN

April 2010 – April 2022

- Built and maintained company IT infrastructure from the ground up, supporting expansion from 28 retail locations to 55+.
- Managed full UniFi network stack, firewalls, switches, VPNs, access points etc. across geographically dispersed locations, ensuring secure and reliable connectivity.
- Performed security hardening on POS systems and retail networks, reducing attack surface and strengthening PCI compliance posture.
- Provided technical guidance to leadership, translating security risks into business terms to drive informed decision making and secure budget approval.

Lead Technician All-Tek / Computer Pros Greeneville, TN

2001 – 2010

- Diagnosed and repaired computers, servers, and networking equipment for residential, SMB, and enterprise clients.
- Installed and configured networks, servers, and security appliances.
- Mentored junior technicians in troubleshooting and repair best practices.

Certifications

- CEH Master (EC-Council) – Valid through Aug 2029
- CompTIA Security+ – Valid through Nov 2030
- CompTIA AI Essentials
- In Progress: CompTIA CySA+, CISSP

Education

High School Diploma | Greeneville High School | Greeneville, TN