Logan Elkins

Houston, TX, USA   17754818073   contact@loganscybervault.com   https://loganscybervault.com

logan.elkins

Summary

A detail-oriented cybersecurity specialist, bringing a strong blend of IT and cybersecurity proficiency, meticulously honed over two years. I have earned the CompTIA Security+ certification and the Splunk Core Certified Power User certification, both of which have substantially elevated my professional standing. My inherent curiosity, coupled with my rapid learning abilities, has consistently driven my success in unfamiliar settings and enabled me to seamlessly adapt to the ever-changing landscape of cybersecurity.

Certifications

Comptia Security +   June 2024
https://www.credly.com/badges/7f7e000f-9718-4b2d-8208-bf02e88ee63e/linked_in_profile

Splunk Core Certified Power User   April 2024
https://www.credly.com/badges/665e5ea6-b2f3-4519-ad9c-2133d16a2651/public_url

Skills

Active Directory, Snort, Wireshark, Splunk, TheHive, Nessus, MITRE ATT&CK Framework, Yara, Sysinternals, Windows Event Logs, Metasploit, nmap, Kerberos, Windows 10/11, Linux, NS, DHCP, ICMP, TCP/IP, Firewalls, VPN, Wi-Fi Standards, SNMP, SMTP, SSH, LDAPS, UDP, SSL/TLS, IMAPS, network access control, identity and access management, Malware Analysis, C Programming

Experience

Freelance   August 2023-Present
Cybersecurity Architect

- Designed and deployed a secure, segmented network specifically for small office/home office settings.
- Rolled out a comprehensive security stack with tools like Wazuh, MISP,Cortex, and The Hive, bolstering threat detection and incident management.
- Configured a Next-Generation Firewall using OPNsense, integrated with Zenarmor plugin, to advance perimeter security.
- Constructed a secure, isolated environment for the collection, analysis, and detonation of malware, facilitating detailed security research.
- Established a remote access VPN to ensure secure and reliable access to network resources.

In my role as a Cybersecurity Lab Architect, I have successfully designed and deployed robust security architectures tailored for diverse environments.

Inovasi   July 2022-Present
IT Support Specialist

- Installed, troubleshot, and maintained networking equipment, with a deep understanding of network topologies, protocols, and interconnectivity to ensure robust and reliable network performance.
- Proactively researched and resolved a variety of desktop and network issues, utilizing extensive product knowledge and technical skills.
- Effectively diagnosed and resolved customer and end-user inquiries, concerns, and technical issues through phone, email, and remote diagnostic tools, enhancing user satisfaction and support efficiency.
- Executed IT security tasks, responding to incidents using Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools within a Security Operations Center (SOC) framework.
- Designed, coded, and tested software applications using Python, contributing to the development of internal software solutions.

As an IT Support Specialist, I have been able to completely redesign the company network, improving security and reliability while enabling the ability for remote access via a dedicated VPN server.

Education

Masterschool   Aug 2023 - Mar 2024
Cybersecurity Training Program

- Gained hands-on experience in Networking, Operating Systems, Python, and engaged in real-world industry projects.
- Trained specifically for the CompTIA Security+ (SY0-601) Exam, with specialized courses like Splunk for Security Analytics and Firewall Administration.
- Acquired insights into Operationalizing MITRE ATT&CK, ISO 27001:2013 compliance, and TCP/IP security.
- Developed comprehensive IT support skills with dedicated training on Windows 10 and 11, Network Troubleshooting, and Help Desk fundamentals.