Thomas Scott Ferguson

Linked-In: Thomas Ferguson

CompTIA Security+ (CE) Certified Professional

San Antonio, TX

Cyber Defense Certified Professional (CDCP)

(512) 827 6791

thoscofer@gmail.com

Seasoned IT professional with 16+ years of technical support experience. CompTIA Security+ CE Certified Professional. Accredited as a Cyber Defense Certified Professional (CDCP), demonstrating practical experience in network traffic analysis, threat hunting, malware analysis, incident triage, digital forensics and report writing. Results-oriented professional dedicated to proactive threat identification and mitigation, committed to ensuring the confidentiality, integrity, and availability of critical systems and data. Seeking a Security Operations Center Analyst or other Security Analyst role at an industry-leading company, bringing the following to the table: Exceptional technical, analytical, troubleshooting, and communication skills, along with a strong customer service background.

Technical Highlights

- ✓ Network traffic analysis using Wireshark
- ✓ Triage Windows endpoints with SysInternals suite tools including: Persistence with Auto-runs/registry Process analysis ProcMon and ProcExp
- ✓ Familiarity with red team tools and tactics such as: privilege escalation, persistence, lateral movement, and malware deployment using tools like Metasploit and Covenant C2.
- ✓ Windows and Linux operating systems
- ✓ Intrusion Detection/Prevention Systems
- ✓ MITRE ATT&CK Framework research/mapping of APTs as well as TTPs of various threat actors
- ✓ Utilizing SIEMs to monitor logging and alerts
- ✓ Log aggregation and analysis tools like ELK, Zeek, Snort, Splunk, Sumo Logic, New Relic.
- ✓ Clear and effective report writing. Concise and effective communication of findings following collection of pertinent digital evidence
- ✓ Network enumeration and vulnerability assessments using and Nmap and Nessus

Training and Certifications

Professional Certifications:

- **CompTIA Security+ (CE) (2023)**
- **Cyber Defence Certified Professional Certification (CDCP) (2022)**
- **Level Effect – CDCP Professional Training:**
  Took on the role of a Cyber Defense Analyst within the Security Operations Center. Gained insights by solving cyber-attack and defense scenarios in a virtual enterprise network. Administered, analyzed, detected, and triage an array of computers and networks, gaining practical and applicable Cyber Defense knowledge and experience.
- **CompTIA Network+ (2008)**
- **CompTIA A+ (2007)**
- **Microsoft Certified Professional (2007)**

Work Experience

Dec 2019 – Present **Network Support Engineer** **BlueJeans by Verizon Austin, TX**

- Quickly and effectively diagnose and resolve customer network (ISP or LAN) issues, software issues or platform issues
- Effectively diagnose and relay outage related issue cases to the appropriate departments and support staff for quick remediation and restoration
- Effectively diagnose more complex issues and coordinate escalations to Tier 2/Engineering for more complex or platform specific issues

Feb 2015 – Dec 2019 **Senior Technology Technician** **Elliott Davis, Chattanooga, TN**

- Hardware, software and network connectivity troubleshooting and maintenance in a Windows 10 environment
- New laptop/desktop imaging and deployment, hardware management (including incident response), Audio Visual setups, and remote support
- Technical support lead for STAR practice management system

Apr 2014 – Jan 2015 **Application Support Tech** **KENCO Logistics, Chattanooga, TN**

- Support Kenco developed software solutions such as their proprietary AS-400 based inventory management system
- Quickly identified and resolved complex issues causing crashes production impacting inventory system
- Escalate urgent issues requiring more in-depth knowledge to appropriate personnel

Oct 2007 – Apr 2014 **Senior Technical Analyst** **EMCO Technologies Madison, AL**

- Senior technical analyst for US Army Corps of Engineers (ACEIT contract)
- Telephone support and remote assistance support for a wide range of issues from password resets to access issues to software installation and configuration and Microsoft Office Suite support
- Extensive US Dept. Of Defense issued Security/Information Assurance training

Security Clearance

US DOD Secret Clearance

- Issued 2008
- Expired 2018

I know that I am still clearance ready as nothing has changed since my last clearance except my credit history is improved.

Education

Jan 2019 – Dec 2019 **Chattanooga State Community College- Chattanooga, TN**

- Undergraduate studies toward Bachelor of Science in Computer Science