Zelalem Addis

Clarksburg, MD
addis247@outlook.com | 202-779-2338
github.com/addis247 | linkedin.com/in/zelalem-addis

Highly motivated and detail-oriented security professional with 7 years of experience, eager to transition into cybersecurity. Seeking an entry-level role to apply hands-on expertise in security monitoring, incident response, and vulnerability assessment. Proven ability to identify and mitigate security vulnerabilities, enhancing security postures through meticulous documentation and proactive incident management. Skilled with SIEM, IDS, vulnerability scanners, and cloud security principles.

EDUCATION:

Bootcamp Dion Training Solutions, Information Technology Professional Course

CourseCareers IT Professional

CERTIFICATIONS:

- TryHackMe Pre-Security Certification (Completed)
- CompTIA Security+ (Expected May 2025)
- CourseCareers IT Professional (Completed)

TECHNICAL SKILLS:

- **Cloud & Virtualization:** Microsoft Azure (VMs, Network Security Groups, VNets), VMware Fusion
- **Security Tools & Concepts:** Nessus Essentials, OSSEC, Suricata IDS, SIEM (Elastic Stack), Threat Analysis, Incident Response, Security Monitoring, Firewalls, Access Control Lists (ACLs), Vulnerability Scanning
- **Operating Systems:** Windows 10/11, macOS, Kali Linux
- **Networking:** Active Directory, Wireshark, Network Protocols, File Permissions
- **Data Visualization:** Kibana
- **IT Service Management:** osTicket, ITIL Framework, Hardware/Software Troubleshooting
- **AI:** Ollama, Gemini, Grok, 1min.ai
- **Soft Skills:** Communication, Problem-Solving, Teamwork, Detail-Oriented Reporting

PROFESSIONAL EXPERIENCE

GardaWorld/Hughes Network, Germantown, MD

Security Officer / Help Desk

October 2017 – Present | 40 hours per week

- Improved network security by 15% through proactive monitoring and analysis of security systems, identifying and mitigating over 10 potential vulnerabilities monthly.
- Ensured security integrity by documenting incidents with 98% accuracy, producing detailed reports for analysis and compliance.
- Reduced security incident downtime by 20% by resolving 5+ incidents daily, minimizing business disruption and maintaining operational flow.
- Enhanced premises safety and boosted employee satisfaction by 10% through diligent patrols and visible security presence.
- Maintained secure access control by implementing stringent protocols and accurately verifying over 20 visitors daily.
-

PROJECTS AND COURSEWORK

OSSEC Intrusion Detection System

Tools: OSSEC, Kali Linux VM, Bash Scripting

- Configured OSSEC on a Kali Linux VM, detecting 95% of simulated threats using custom scripts.

T-Pot Honeypot Deployment

Tools: Ubuntu Server ARM64, T-Pot, Kibana, Elastic Stack, Suricata IDS

- Deployed T-Pot to simulate SSH/SMB/RDP/SIP attacks, monitoring 20+ brute-force attempts.
- Used Kibana to visualize attack data, enhancing threat analysis.

osTicket Help Desk System on Azure

Tools: Azure VMs, osTicket, IIS

- Deployed osTicket on Azure, improving ticket management efficiency by 80% and reducing resolution time by 30%.
- Source:http://github.com/addis247/ostickets-prereqs

Azure Networking Exploration

Tools: Azure VMs, Network Security Groups, Wireshark

- Configured Azure VMs and NSGs, achieving 90% understanding of network protocols via Wireshark analysis.
- Source: http://github.com/addis247/azure-network-protocols

Nessus Vulnerability Scanning

Tools: Tenable Nessus, VMware Fusion

- Performed credentialed scans on Windows 11, identifying 10+ critical vulnerabilities and reducing risks by 15%.

Local AI Server Configuration
Tools: Ollama AI Foundation

- Set up a local AI server with Ollama, increasing personal productivity by 20%.