YOHANNES TEKLU

SECURITY ANALYST

PROFESSIONAL SUMMARY

Proactive and results-driven Cybersecurity Analyst with over three years of self-directed learning and practical experience in SOC operations, incident response, and vulnerability assessments. CompTIA Security+ certified, with expertise in leveraging advanced cybersecurity tools and frameworks to identify, mitigate, and resolve complex threats. Demonstrates a passion for continuous learning and problem-solving, with hands-on experience in cybersecurity labs and simulated environments. Seeking to bring value to a security-focused organization through innovative defense strategies and collaboration.

SKILLS

- Threat detection
- Incident response
- ELK Stack
- Snort
- Sysmon
- MITRE ATT&CK
- NIST
- Anomaly detection
- Linux (Ubuntu, CentOS, Kali Linux)
- GDPR
- Analytical thinking
- Teamwork
- Log analysis
- Splunk
- Wireshark
- Zeek
- Wazuh
- Cyber Kill Chain
- PCAP analysis
- Windows
- HIPAA
- NIST Standards
- Communication

EDUCATION

Bachelor of Science in Cybersecurity Candidate
Expected graduation MAY 2025 | Old Dominion University (ODU)

CONTACT

757- 230-7502

yohannes.cyber@gmail.com

Virginia Beach, VA 23462

CERTIFICATIONS

- CompTIA Security+
- CompTIA A+

SELFLEARNINGEXPERIENCE

Dedicated over three years to mastering cybersecurity concepts through self-directed learning and hands-on labs., Completed structured learning paths on platforms like TryHackMe, focusing on SOC operations, incident response, and network security., Developed and implemented custom IDS/IPS detection rules in simulated environments, improving threat detection capabilities by 35%., Created Splunk and ELK Stack dashboards for log analysis and anomaly detection in training scenarios., Conducted comprehensive traffic analysis using Wireshark, Snort, and Zeek to identify malicious activities., Investigated endpoint security anomalies with Sysmon and Wazuh, creating custom rules to enhance detection., Applied cybersecurity frameworks like MITRE ATT&CK to model adversarial tactics and develop mitigation strategies., Participated in over 200 hours of hands-on labs to build expertise in log analysis, incident response, and digital forensics., Designed and executed mock incident response workflows to simulate real-world cybersecurity challenges., Researched emerging threats and implemented proactive defense strategies in virtual lab environments.

ACCOMPLISHMENTS

- Reduced incident response times by 25% through effective workflows and tools.
- Completed over 200 hours of practical labs on TryHackMe, mastering SOC operations and cybersecurity frameworks.
- Enhanced threat detection accuracy by 35% through custom IDS/IPS signatures and proactive strategies.

PROJECTS

SOC Analyst Training (TryHackMe), Conducted log analysis using Splunk and ELK Stack to identify security anomalies., Investigated Indicators of Compromise (IOCs), correlating events to determine root causes., Improved incident response by creating advanced queries for efficient detection. Traffic Analysis Essentials, Utilized Wireshark, Snort, and Zeek for live network traffic monitoring., Detected and mitigated malicious activities through custom detection rules. Endpoint Security Monitoring, Strengthened endpoint security by identifying suspicious processes using Sysmon and Wazuh., Enhanced detection capabilities through proactive rule creation and analysis. Cyber Defense Frameworks, Applied MITRE ATT&CK and Cyber Kill Chain frameworks to simulate adversarial behavior., Enhanced operational workflows by integrating defense-in-depth strategies.