Trevor Lee

(970) 342-5393 | lee8trevor@gmail.com | https://github.com/Trevor23Lee | linkedin.com/in/trevor-lee-801921231

Qualifications and Skills

- **Cybersecurity**: Network security, firewalls, VPNs, IDS/IPS, data encryption, secure protocols (SSL/TLS), vulnerability assessments, penetration testing, incident response, risk management (ISO, NIST), Zero Trust, MITRE ATT&CK. OWASP Top 10, Burp Suite, Wireshark, nmap
- **Programming Languages**: Python, SQL, Java, C++/C, Matlab.
- **Operating Systems**: Windows, Linux.
- **Technical Skills**: GitHub, Splunk, SIEM solutions, malware analysis tools, Cloud computing (AWS, GCP, Azure), Docker, Kubernetes, Machine Learning/A.I.

Certifications and Courses

- Google Cybersecurity Professional Certificate - September 2024
- CompTIA Security + Certificate - November 2024

- *TryHackMe:* Pre Security, Intro to Cyber Security, Complete Beginner, SOC Level 1
- *LetsDefend:* SOC Analyst Learning Path (In Progress)
- *HackTheBox*: SOC Analyst (In Progress)

Education

Bachelor of Science in Computer Science May 2024

-With a minor in Computer Engineering GPA: 3.69

Colorado State University, Fort Collins, Colorado

Associates of Applied Science, Cum Laude May 2021

Front Range Community College, Fort Collins, Colorado GPA: 3.62

Work Experience

Teacher Assistant Jan. 2023 - May 2023, Aug. 2023 - May 2024

Colorado State University, Fort Collins, Colorado

- Providing support to students in their Discrete Structures course and Introduction to Machine Learning course
- Assisting with grading worksheets and gaining a fresh perspective to enhance personal knowledge

Hewlett Packard Enterprise Intern May 2023 - Sep. 2023

Fort Collins, Colorado

- Orchestrated integration of Kubecost into GreenLake Cloud Platform which automates provisioning and cost management of Kubernete clusters
- Developed a cleanup utility for deleting user entries using SQL, Dockerfiles and Jenkinsfiles
- Demonstrated proficiency in cloud technologies, including database management, microservices architecture, Kubernetes, and Docker. Leveraged this expertise to foster effective team collaboration and streamlined project delivery

---

Cyber Security Projects

Network Traffic Analysis with Wireshark

- Completed TryHackMe labs and analyzed PCAP files from malware-traffic-analysis.net to investigate network traffic.
- Investigated HTTP, DNS, and TCP traffic to identify malware indicators and suspicious IP connections.
- Documented findings, including TTPs (Tactics, Techniques, and Procedures), and suggested mitigation strategies.

Web Application Vulnerability Assessment with Burp Suite

- Conducted vulnerability assessments through TryHackMe's *OWASP Top 10* labs and hands-on Burp Suite practice.
- Detected and documented vulnerabilities such as SQL injection and XSS by intercepting and analyzing web traffic.
- Delivered a structured vulnerability report with severity ratings and suggested remediation measures.

Log Analysis and Incident Response with Splunk (SIEM)

- Worked on TryHackMe's *SOC Level 1* and *Threat Intelligence* labs to ingest and analyze system logs.
- Configured dashboards and alerts to detect brute-force attempts and unusual login activities.
- Simulated an incident response process by creating an attack timeline and outlining remediation steps.