Hashim Alkhateeb

407-801-9224 | Halkhateeb704@gmail.com | linkedin.com/in/hashim-alkhateeb | github.com/hashdbrown | portfolio

Education

University of Central Florida — Orlando, FL

Master of Science in Computer Science — *Expected May 2026*

Bachelor of Science in Computer Science — *Aug. 2021 – May 2025*

- Awards: Magna Cum Laude, Bright Futures Scholar, Dean's List, President's Honor Roll **GPA: 3.934**
- Relevant Coursework: Malware Software Vulnerability, Cyber Operations Laboratory, Software Engineering

Certifications

CompTIA CySA+ — June 2025

- Completed hands-on labs triaging SIEM alerts, correlating Splunk/Elastic logs, and escalating verified threats
- Ran vulnerability-scanning and threat-hunting exercises on on-prem and Azure resources using Nessus and open-source tools
- Applied secure baseline configurations and access-control policies aligned with NIST guidelines, reducing audit findings

CompTIA Security+ — January 2025

- Demonstrated knowledge of core domains (network defense, risk, crypto) via exams and scenario-based labs
- Explained security best practices to non-technical users, supporting help-desk functions.
- Traced malicious TLS traffic in Wireshark and drafted firewall block rules used in lab scenarios

Experience

Teaching Assistant - Discrete Structures II — Jan. 2025 – May 2025

University of Central Florida — *Orlando, FL*

- Helped 70–80 students one-on-one each week with logic, set theory, combinatorics, and proof techniques, reinforcing patience and clear technical communication skills
- Monitored the Canvas discussion board and held virtual/onsite office hours, providing first-line support for homework and lab questions
- Assisted the instructor with grading problem sets and exams, ensuring consistent application of rubrics and accurate record-keeping

Technical Skills

Security Operations and Monitoring: Threat hunting, Log analysis, SIEM, Splunk, Wazuh, OSSIM, SOAR, Nessus, OpenVAS, Burp Suite, IDS/IPS tuning, Wireshark, Nmap, Netcat, MITRE ATT&CK mapping, CVSS, OSINT, Pi-hole, Unbound, Suricata, KQL
Operating Systems & Support Tools: Windows, Linux, macOS, Command-line troubleshooting, Scripting, Automation, Powershell, Bash
Networking & Protocols: TCP/IP, DHCP, DNS, Firewall, ACL, Endpoint hardening
Programming & Database: Python, Java, JavaScript, C, Node.js, React, HTML, SQL, MySQL, MongoDB, AWS, Docker, Git
Ticketing & Collaboration: Jira, Agile and Scrum, Slack, Google Workspace, Microsoft Suite, Github

Projects

SOC Homelab (Self-Hosted) | *Splunk, Wazuh, Suricata, Pi-hole, Unbound, Tailscale* — June. 2025 – Present

- Leveraged Splunk to centralize sudo authentication logs, uncovering 14 failed login attempts in one day and building a dashboard panel to continuously track abnormal authentication patterns
- Engineered a containerized SOC lab to simulate enterprise environments by integrating IDS/IPS, SIEM, and secure DNS across Linux and macOS systems
- Streamlined security monitoring by designing custom dashboards and refining rules to track file integrity and authentication events
- Mitigated 50+ critical vulnerabilities identified by Wazuh through endpoint hardening across various systems.

- Identified and responded to simulated intrusions by correlating host-based and network-based alerts, reducing detection time by 60% through real-time Suricata log analysis.
- Fortified network privacy by routing Tailscale DNS through Pi-hole and Unbound, blocking over 6,000 out of 35,000+ queries (17.4%) across six active clients

MAGNETO | *Python, React, Docker, Agile, Scrum, Git* Aug. 2024 – May 2025

- Led a 5-person Scrum team, running weekly stand-ups and two-week sprints in Jira
- Developed a web UI that triggers MAGNETO's automated GUI test oracles, cutting manual regression testing effort by roughly 60 percent and surfacing defects earlier in the release cycle
- Built Docker images and GitHub Actions pipelines to spin up a clean test environment on demand, eliminating configuration drift and reducing teammate support requests

UCF Cyber Challenge (CTF) | *nmap, netcat, sqlmap* Feb. 2025

- Competed in a real-time, scenario-based CTF that simulated enterprise breaches and incident response
- Performed network reconnaissance and service enumeration with nmap and netcat to uncover hidden flag servers
- Solved SQL-injection and web-exploitation challenges using sqlmap, Burp Suite, and manual payload crafting