RAYAN MOHAMMED SULAIMAN ALHARBI

Riyadh, Saudi Arabia | +966 580028313 | r.m.harbi4@gmail.com |linkedin.com/in/rayan-alharbi-cyber

Cybersecurity Graduate | Security Operations & Digital Forensics

CAREER SUMMARY

Recent Cybersecurity graduate from Rockford University, United States, with GPA 3.75/4.00. Strong academic preparation in cybersecurity, digital forensics, cybercrime, and risk analysis, supported by advanced practical training through Tuwaiq Academy. Leadership experience includes managing the university's Cybersecurity Club and delivering educational courses recognized by the Saudi Cultural Attaché in the United States.

CORE COMPETENCIES

Digital Forensics | Threat Analysis | Incident Response | Risk Analysis | Network Security | Security Operations | Cybercrime Investigation | Evidence Handling | Technical Documentation | Security Monitoring

TECHNICAL SKILLS

Wireshark | Linux | Magnet AXIOM | FTK Imager | Autopsy | DumpIt | MISP | Cortex | ANY.RUN | Wazuh | Splunk | SQL | MITRE ATT&CK | TheHive

EDUCATION

Rockford University, United States | December 2025 | **Bachelor of Science in Cybersecurity**
GPA: 3.75/4.00 | Second Honors | Minors: Business Administration, Criminal Justice

LEADERSHIP & ACADEMIC ENGAGEMENT

Founder & President, Cybersecurity Club — Rockford University:

- Led cybersecurity activities and peer learning, growing the club to 40+ members**.**

Saudi Cultural Attaché Recognition — United States:

- Recognized for delivering university-level cybersecurity training sessions.

CERTIFICATIONS & TRAINING

- Cybercrime and Advanced Digital Forensics Bootcamp | Tuwaiq Academy
- CompTIA Security+ | 2026
- CompTIA CySA+ | 2026

CYBERSECURITY PROJECTS: Reports are available at https://rayan-cyber.com

Cyber Attack Simulation Using Cyber Kill Chain | Award-Winning Project

- Simulated full attack lifecycle from reconnaissance to exfiltration, including spear phishing and trojan deployment.
- Applied SIEM, EDR, and network monitoring for detection and defence; awarded **Best Cybersecurity Project** at **Tuwaiq Academy**.

Cyber Threat Intelligence Platform | MISP | TheHive | Cortex

- Built simulated CTI and incident response environment integrating MISP, TheHive, and Cortex.
- Analysed APT-based threat events, enriched IOCs through VirusTotal, OTX, and Censys, and supported detection and containment decisions.

Malware Analysis and DFIR Investigation | Agent Tesla

- Performed static and dynamic analysis of Agent Tesla, identifying persistence methods and external network communication.
- Extracted hashes, domains, and IPs, mapped behaviour to MITRE ATT&CK, and provided containment and threat-hunting recommendations.

LANGUAGES: Arabic: Native English: Professional