Yousef Khalaf

Zarqa-Jordan | yousefmohammadkhalaf@gmail.com | 00962798672395

LinkedIn: Yousef Khalaf

Summary

Fresh cybersecurity graduate with hands-on SOC experience in log analysis, threat detection, and scripting. Skilled in tools like Splunk, Wireshark and metasploit. Active CTF competitor. Passionate about solving real-world security challenges and continuously learning.

Education

B.Sc. in Cybersecurity

Zarqa University - GPA: 86.3 (Excellent) Expected Graduation: 2025

Scientific Publication

An Effective Encryption Algorithm Based on RSA and DES Published on ResearchGate - 2024

Developed a hybrid encryption algorithm combining RSA and DES to enhance data security and computational performance.

Practical Training

BTL1 - Tuned Application (Feb 2024 – Jun 2024)

- Security Fundamentals
- Phishing Analysis and Mitigation
- Threat Intelligence
- Digital Forensics
- Structured Incident Response

SOC - Scan Wave (Sep 2024 – Nov 2024)

- SIEM Configuration
- Decoder and Rule Creation
- Dashboard Development
- Alert Analysis and Response

PROJECTS

SecureTheSystem – Cybersecurity Simulation & Training Platform

Led the development of an interactive red/blue team training system simulating real-world cyberattacks and defenses in isolated virtual environments. Key Highlights:

- Deployed vulnerable machines (Apache, Jenkins, WordPress, Samba, FTP, Honeypot) for red team attack simulation.
- Integrated log analysis and exploit detection via Splunk and MITRE ATT&CK Navigator.
- Developed Laravel-based web platform for VM distribution, report submission, leaderboard tracking, and AI feedback using Gemini API.
- Created detection rules for SSH brute force, file exfiltration, plugin RCE, and reverse shell activities
- Implemented full remediation and hardening process post-exploitation using security best practices.

Cybersecurity Instructor & Trainer

- Delivered multiple training sessions focused on SOC analysis and cybersecurity fundamentals for entry-level professionals.
- Designed and taught a specialized course in malware hunting, emphasizing practical detection and analysis techniques.
- Led a 10-week comprehensive cybersecurity course at Zarqa University, tailored for future SOC analysts and blue team members.
- Delivered a cybersecurity workshop in collaboration with IEEE at Isra University (IU).
- Conducted a workshop under the Continuing Education Center at Zarqa University, focusing on practical cybersecurity skills.
- Developed and customized course content for junior SOC analysts, blue team trainees, and university-level students.

Courses

- eCIR – Net Rider Academy
- Security+ – Net Rider Academy
- Linux+ – Teracourse
- SIEM 101 / SOC Analyst / SIEM Engineer – Let's Defend
- How to Investigate a SIEM Alert – Let's Defend
- Introduction to OSINT / Dark Web / Digital Forensics – BT

Skills

Technical skills

- Cybersecurity Tools: Wireshark, Autopsy, Volatility, Nmap, etc.
- SIEM Platforms: ELK Stack, Splunk.
- Operating Systems: Linux, Windows.

Soft skills

- Communication
- Problem solving
- Presentation
- Organizational and Planning
- Time management and Team management

Languages

- Arabic (Native language)
- English (practical level)