

Yousef Mohammad Khalaf

SOC Analyst | Cyber Analyst

Zarqa, Jordan

+962 7 9558 6321 | E-Mail: yousefmohammadkhalaf@gmail.com | LinkedIn: [linkedin.com/in/yousefkhalf](https://www.linkedin.com/in/yousefkhalf)

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in SOC analysis, security monitoring, incident response, SIEM engineering, threat intelligence, digital forensics, and network security. Experienced in configuring SIEM dashboards, decoders, and correlation rules; analyzing security alerts and logs; and investigating incidents using MITRE ATT&CK. Hands-on experience deploying and configuring OpenCTI as a Cyber Threat Intelligence platform, including Docker-based infrastructure and threat-intelligence connectors. Familiar with Kubernetes fundamentals, containerized deployments, Elasticsearch, Redis, RabbitMQ, MinIO.

TECHNICAL SKILLS

SOC Analysis | Security Monitoring | Incident Response | Threat Intelligence | Threat Hunting | SIEM | Splunk | ELK | OpenCTI | MITRE ATT&CK | Digital Forensics | Network Security | PCAP Analysis | Wireshark | Nmap | Python | Docker | Kubernetes Fundamentals | Elasticsearch | Linux | Security Reporting | Log Analysis | Alert Triage

PROFESSIONAL EXPERIENCE

- SOC Analysis | [Scan Wave](#)** Sep 2024 – Nov 2024
 - Configured SIEM dashboards, custom decoders, and correlation rules for security events.
 - Performed alert analysis and incident response based on MITRE ATT&CK techniques.
 - Enhanced SOC efficiency by building dashboards for real-time threat visibility.
- BTL1 | [Tuned Application](#) – Amman** Feb 2024 – May 2024
 - Gained practical knowledge in Security Fundamentals, Threat Intelligence, Phishing Analysis, and Digital Forensics.
 - Conducted structured incident response exercises and forensic case investigations.
- SOC Analysis Trainer | Freelance** Sep 2025 – Present
 - Delivered hands-on training sessions in **Security Operations Center (SOC) fundamentals**, covering log analysis, SIEM monitoring, incident detection, and alert triage for students and junior security analysts.
 - Designed and delivered practical labs using real-world attack scenarios, including network traffic analysis (PCAP), malware indicators, and threat investigation techniques aligned with industry standards.
 - Collaborated with **universities ([ZU, IU](#)), cybersecurity teams ([JCC](#)), and private companies ([Scalax](#))** to provide customized training programs focused on defensive security, blue team operations, and entry-level SOC analyst readiness.
 - Mentored trainees by explaining attack chains, MITRE ATT&CK techniques, and incident response workflows, helping participants build a strong foundation for **SOC Analyst and Blue Team roles**.
- CTF player and Author**
 - Active CTF Competitor** with a proven record of achieving **multiple first-place rankings** in Capture The Flag (CTF) competitions, demonstrating strong skills in **cybersecurity, problem-solving, and technical analysis**.
 - Professional CTF Challenge Author** specialized in creating advanced challenges in **Digital Forensics (DF), Cryptography, and Miscellaneous (Misc)**, with a focus on **real-world attack scenarios and analytical thinking**.

PROJECTS

- OpenCTI Threat Intelligence Platform – Deployment & Configuration** Mar 2026
 - Deployed and configured OpenCTI as a Cyber Threat Intelligence (CTI) platform for collecting, organizing, correlating, and visualizing threat intelligence.
 - Configured a containerized OpenCTI environment with Docker and supporting services including Elasticsearch, Redis, RabbitMQ, and MinIO.
 - Configured threat-intelligence connectors and worked with threat feeds such as AlienVault OTX and VirusTotal.
 - Developed practical understanding of STIX-based threat intelligence, observables, indicators, threat actors, TTPs, and intelligence relationships.
 - Gained practical exposure to container orchestration concepts and Kubernetes fundamentals relevant to scalable security-platform deployments.
- SecureTheSystem – Cybersecurity Simulation & Training Platform [\[Link\]](#)** May 2025

- Designed an interactive red/blue team simulation environment to train analysts on incident response.
- Integrated Splunk and MITRE Navigator for attack detection and response workflow tracking.
- Created detection rules for SSH brute force, reverse shells, and plugin RCE attacks.

- **PortScannerXBot – Telegram Security Automation Tool** [\[Link\]](#) Aug 2025
 - Developed a Telegram bot using Python and Nmap for automated port scanning and service detection.
 - Added CVE suggestion feature based on version fingerprinting, GeoIP, and WhoIs lookups.
 - Documented mitigation techniques aligned with secure API and zero-trust practices.
- **PCAP Network Traffic Analysis Tool** [\[link\]](#) Aug 2025
 - Implemented **advanced packet filtering, protocol-based search, and content inspection**, supporting **100+ protocols** including IoT, ICS, Bluetooth, and Zigbee.
 - Integrated **real-time traffic visualization**, automated detection of **suspicious network patterns**, and **automatic file extraction** to enhance security monitoring and forensic analysis.
 - Built a **modern GUI with dark mode**, optimized batch processing for **low resource consumption**, and enabled **PCAP/CSV/JSON import and export** for flexible analysis workflows.

RESEARCH & PUBLICATIONS

LLM-WAF: An Intelligent Web Application Firewall Powered by Large Language Models for Advanced Threat Detection

- Yousef Khalaf. International Journal of Wireless and Microwave Technologies, Vol. 16, Issue 4, pp. 317–327, 2026. DOI: 10.5815/ijwmt.2026.04.18.
- Designed an LLM-powered WAF architecture for semantic analysis of HTTP traffic and malicious payload detection.
- Worked with BERT-based NLP, PyTorch, Hugging Face Transformers, real-time traffic analysis, threat scoring, and adaptive learning concepts.

An Effective Encryption Algorithm Based on RSA and DES

- Published research paper by Khalaf et al. in International Journal of Communication Networks and Information Security, 17(4), pp. 10–19, 2025.
- Contributed to research combining RSA public-key cryptography with DES symmetric encryption and comparative evaluation of security and computational considerations.

EDUCATION

Bachelor of Cyber Security | Zarqa University | 2021 – 2025 GPA: 87.3 (Excellent)

Relevant Coursework:

Computer Networks & Information Security • Ethical Hacking • Network Defense • Incident Response • Security Fundamentals

CERTIFICATIONS & TRAINING

Completed: eCIR – Net Rider Academy, 2025 | Security+ – Net Rider Academy, 2025 | Linux+ – TeraCourse, 2025 | SIEM 101 / SOC Analyst Path / SIEM Engineer – Let’s Defend, 2025 | Malware Analysis – Let’s Defend, Mar 2025 | ICIP, Sep 2025 | Trust and Security with Google Cloud, 2024 | Digital Forensics, OSINT & Dark Web – BT Labs, 2024

In Progress: CDSA (HTB) – Certified Defensive Security Analyst | Security+ – CompTIA | eCIR – INE

LANGUAGES

- Arabic - Native
- English

*Certifications