Younes Mohammed AL-Salami

Cybersecurity | Security Operations Center (SOC) Analyst

linkedin.com/in/younes-al-salami younesalsalami@gmail.com younes-alsalami.vercel.app

Yemen, Sana'a +967770142444 / +967713711126

PROFESSIONAL SUMMARY

Cybersecurity graduate specialized in the Blue Team and Security Operations Center (SOC), with hands-on laboratory experience in log analysis, network forensics, digital forensics, malware analysis, vulnerability assessment, and incident response. Developed a behavioral ransomware defense system designed for proactive detection and real-time response. Practically applied alert monitoring using Wazuh SIEM, PCAP analysis, Indicator of Compromise (IOC) extraction, YARA rules, threat intelligence techniques, MITRE ATT&CK event mapping, and technical security reporting.

EDUCATION

Sana'a University | Faculty of Computer & Information Technology June 2026

Bachelor of Cybersecurity

GPA: 88.38 — Very Good

Honors: Among the top 5 students in the first graduating cohort of the Cybersecurity specialization at Sana'a University.

EXPERIENCE

Cybersecurity Project Developer (CYBERSECURITY PROJECT DEVELOPER) May 2025 – Present

Developed SBARDS, a multi-layered ransomware defense system designed for proactive detection and real-time response. The system combines pre-execution static analysis without running the file, isolated dynamic analysis using CAPE Sandbox to monitor file behavior and system activity during execution, and behavioral analysis to identify ransomware activity. Integrated malware analysis techniques, YARA rules, IOC extraction, and threat intelligence techniques to support ransomware detection and investigation.

- Tested the system against ransomware scenarios, including mass file modification, file encryption, and Shadow Copies deletion attempts.
- Implemented real-time automated response mechanisms to block suspicious operations and prevent unauthorized file encryption.
- Built a security monitoring dashboard to analyze detection events, monitor system activity, support SOC-focused investigations, and improve security visibility.

SKILLS

Security Information and Event Management (SIEM)
Malware Analysis
Incident Response
Alert Triage
Log Analysis
IOC Analysis
Problem Solving
Team Collaboration
Analytical Thinking
Technical Reporting

CERTIFICATIONS

Mitigate threats using Microsoft Defender XDR — Microsoft Learn — (Sept 2026)

CyberAgent Project Training — Selected Modules: Security Operations, Analytical Tools & Systems Administration — Vilnius University — (Sept 2026)

Intr**oduction to Networks (CCNA)** — Cisco Networking Academy — (Aug 2026)

Internet Security — Internet Society — (Aug 2026)

Malware Analysis Fundamentals — Mahara-Tech — (Aug 2026)

Advanced Digital Forensics: File Systems, Mobile Devices, OSINT - Mahara-Tech (Aug 2026)

Ethical Hacker - Cisco Networking Academy (Jul 2026)

LANGUAGES

• **Arabic**: Native

• **English**: Advanced