Saeed Damra

DFIR

+962789317222
saeeddamra@hotmail.com
saeed1197.github.io
Amman, Jordan

SUMMARY

I'm a Digital Forensics and Incident Response (DFIR) professional specializing in investigating cyber threats, identifying indicators of compromise, and mitigating the impact of security incidents. With a strong foundation in cybersecurity principles and hands-on experience in forensic analysis and incident response.

EXPERIENCE

12/2022 - Present

DFIR Specialist – JOCERT Team

National Cyber Security Center (NCSCJO) ↗

DFIR Specialist within the JOCERT team, responsible for investigating and responding to cybersecurity incidents through security alert analysis and forensic examination of compromised systems. Digital evidence is collected and preserved in accordance with legal and compliance requirements. Utilizes EDR and forensic tools to identify malicious activity, contain threats, and support system recovery. Collaborates with SOC teams, threat intelligence units, and legal departments to ensure an effective, coordinated response. Contributes to root cause analysis, incident reporting, and the enhancement of incident response procedures and overall security posture.

08/2022 - 12/2022

SOC

National Cyber Security Center (NCSCJO) ↗

Worked as a SOC Analyst where I gained hands-on experience in a Security Operations Center environment. I was responsible for monitoring, analyzing, and responding to security incidents using SIEM tools and other cybersecurity technologies. My role involved threat detection, incident escalation, and applying cybersecurity principles to support incident response efforts.

09/2020 - 08/2022

System Administrator

National Cyber Security Center (NCSCJO) ↗

Provided technical support for Security Operations Center (SOC) infrastructure by configuring and maintaining SIEM connectors to onboard new log sources (e.g., firewalls, endpoints, cloud services), ensuring continuous data flow and platform reliability.

EDUCATION

2015 - 2019

Computer Science

Hashemite University
Bachelor's degree

CERTIFICATES

BTL2 (Preparing)

ICS DFIR (Kaspersky)

IR (Kaspersky)

YARA (Kaspersky)

Advanced DFIR (Kaspersky)

Linux+

CCNA

CEH

SKILLS

Memory forensics

Forensic imaging

Scripting

Log analysis

Network forensics

Working with EDR

LANGUAGES

Arabic	Native	English	Intermediate