# Saeed Damra

Amman, Jordan
+962 7 8931 7222
saeeddamra@hotmail.com
www.linkedin.com/in/saeeddamra
saeed1197.github.io

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

09/2022 - PRESENT

### **DFIR Specialist – JOCERT Team** / National Cyber Security Center

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.

09/2021 - 09/2022

### **SOC** / National Cyber Security Center

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.

09/2020 - 09/2021

### **System Administrator** / National Cyber Security Center

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

### **Bachelor of Computer Science**/Hashemite University, Jordan

## Certificates

- CEH
- ICS DFIR (Kaspersky)
- IR (Kaspersky)
- YARA (Kaspersky)
- Advanced DFIR (Kaspersky)
- Linux+
- CCNA
- BTL2 (Currently Preparing)

# Skills

- Digital Forensics

  - Disk and memory forensics (Volatility, FTK, EnCase, Autopsy)
  - Forensic imaging and data acquisition (FTK Imager, dd)

- Network forensics

  - Incident triage and containment
  - Root cause analysis
  - Log analysis (Windows Event Logs, Syslog, firewall, DNS, etc.)

- Tools & Platforms

  - SIEM
  - XDR solutions (Cortex, Vision One)
  - Packet analysis (Wireshark, tcpdump)

- Scripting & Automation

  - Python, PowerShell, Bash (Automation and Analysis)
  - Regex (Logs and Pattern matching)