MEHMET DEMIR

İstanbul/Esenyurt

https://www.linkedin.com/in/karlos34/ | https://github.com/jackalkarlos | mdmrrr.34@gmail.com

Digital Forensics Analyst / IR Handler

PROFESSIONAL SUMMARY

I am a Digital Forensics and Incident Response (DFIR) analyst with direct experience handling security incidents across both government and private sector environments. I have conducted investigations on Windows and Linux systems, performed in-depth registry and artifact analysis, and responded to a wide range of cyber threats in real time. My work often involves identifying malicious activity, uncovering root causes, and taking swift action to contain and remediate incidents. I frequently use security products like SentinelOne, Cortex XDR, and CrowdStrike to monitor, analyze, and respond to threats, and I write custom scripts to streamline forensic workflows and improve investigation efficiency.

I have led and accelerated compromise assessment initiatives, leveraging tools such as Thor APT Scanner and other IOC (Indicator of Compromise) scanning solutions to rapidly identify and mitigate advanced persistent threats (APTs). By automating scan workflows and integrating threat intelligence feeds, I reduced assessment timelines by 40% while maintaining high accuracy in detecting stealthy adversarial activities.

In addition to my professional work, I regularly participate in Capture the Flag competitions and bug bounty programs, which help sharpen my skills in vulnerability discovery and exploitation. I also teach digital forensics and incident response at İstanbul Gelişim University's Cyber Academy, where I support students in bridging the gap between academic theory and real-world cybersecurity challenges.

TECHNICAL SKILLS

- Windows & Linux Forensics (Registry, Memory, Log Analysis)
- Malware Analysis & Threat Intelligence (IOC, TTP, YARA)
- SIEM, EDR & XDR Tools: SentinelOne, Cortex, CrowdStrike, Cyber Reason, Carbon Black, Splunk
- Python & PowerShell Scripting for Automation
- Network Traffic & PCAP Analysis
- MITRE ATT&CK, Cyber Kill Chain
- CTF & Bug Bounty: Exploitation, Reverse Engineering, Real-time Problem Solving
- Cybersecurity Training: Digital Forensics & Incident Response at IGU Cyber Academy

PROFESSIONAL EXPERIENCE

DFIR Analyst – ADEO Cyber Security **Sep 2023 - Present**

- Led digital forensic investigations and incident response across government and private sector environments, ensuring rapid containment of threats.
- Automated forensic workflows by developing Python/PowerShell scripts to accelerate incident response and artifact analysis.
- Spearheaded resolution of 20+ critical incidents by coordinating cross-functional teams and implementing containment strategies.
- Analyzed and resolved incidents using SIEM (Splunk), and EDR/XDR (SentinelOne, Cortex, Defender, Carbon Black, Cyber Reason) tools, reducing incident resolution time by 30%.
- Identified root causes through in-depth analysis of disk, memory, and system artifacts, enhancing organizational forensic protocols.

DFIR Intern - ADEO Cyber Security **Jul 2023 – Sep 2023**

- I have acquired in-depth knowledge of professional DFIR processes and have prepared myself for a career in the corporate environment.
- Assisted in analysis of disk and memory artifacts.
- Learned proper chain of custody and evidence handling procedures.

System Support Specialist – Acıbadem Hospital **July 2022 – Sep 2022**

- I was responsible for setting up the infrastructure of the hospital.

EDUCATION

İstanbul Gelişim University **(Expected Oct 2024)**

BSc, Information Security

CERTIFICATIONS

SentinelOne IR Engineer - SIREN **Aug 2024**

SentinelOne

CCNA: Introduction to Networks **Jan 2023**

Cisco

Network Security **May 2022**

Cisco

HONORS AND EXTERNAL CONTRIBUTIONS

- **SKYDAYS CTF 2025 2.** **Mar 2025**
- **VRT Bug Bounty** **Mar 2025**
- **PWNLabMe CTF 2024 1.** **Jan 2025**
- **STMCTF 2024 3.** **Dec 2024**
- **Teacher at “İGÜ Siber Akademi”** **Aug 2024**
- **SUCTF 2.** **May 2024**
- **PWNLabMe CTF 2023 2.** **Dec 2023**
- **STMCTF 2023 9.** **Dec 2023**
- **STEMCTF 1.** **Dec 2023**
- **Kapsül HackMe CTF Web Security** **Jul 2023**