# Ali Kesik

Cyber Security Analyst | Blue Team | Threat Detection & Response

Ankara, Turkiye | +90 530 037 2629 | ali.kesik76@gmail.com

LinkedIn: linkedin.com/in/alikesik | GitHub: github.com/alikesk222

## Professional Summary

Cyber Security Analyst with hands-on experience in SOC operations, threat hunting, SIEM tools, and vulnerability management. Skilled in both offensive and defensive techniques, including malware analysis, social engineering detection, and packet/log analysis. Passionate about security architecture, incident response, and AI-assisted cyber operations.

## Core Competencies

- SOC Operations: Real-time monitoring, incident response, threat detection

- SIEM Tools: Splunk, IBM QRadar

- Vulnerability Assessment: Nessus, OpenVAS, Qualys

- Network Analysis: Wireshark, TCP/IP, DNS, VPN

- Offensive Security: Kali Linux, Metasploit, Nmap, Burp Suite

- OSINT Tools: Shodan, VirusTotal, Hybrid Analysis

- Frameworks: NIST-800, MITRE ATT&CK, OWASP Top 10

- Programming: Python, SQL, JavaScript, HTML/CSS

- Soft Skills: Analytical mindset, teamwork, communication, self-motivation

## Experience

Cyber Security Analyst Intern | Ankara Yildirim Beyazit University (Mar 2023 - Present)

- Conducted threat detection using SIEM & packet analysis tools.

- Performed vulnerability scanning and implemented remediation plans.

- Ensured policy compliance and developed threat reports.

Cybersecurity Intern | UISAP Software Solutions (Jul 2022 - Sep 2022)

- Built SAP-compatible web interfaces.

- Developed low-code mobile apps and explored Flutter basics.

## Education

BSc in Software Engineering - Ankara Yildirim Beyazit University (2021 - Present)

# Ali Kesik

Cyber Security Analyst | Blue Team | Threat Detection & Response

## Certifications

- Cisco CyberOps Associate

- Cisco CCNAv7: Introduction to Networks

- Cyber Security Expert - Istanbul Arel University

## Languages

- Turkish: Native

- English: Advanced (Professional Working Proficiency)

## Tools & Technologies

Splunk, QRadar, Kali Linux, Burp Suite, Metasploit, Nmap, Wireshark, OpenVAS, Nessus, Shodan, VirusTotal, Hybrid Analysis, Python, SQL, VMware, VirtualBox, FortiGate, WAF, Git, HTML/CSS/JS