Elif Özkan

Junior Cyber Security Analyst

Personal details

Elif Özkan

elifozkanofis@gmail.com

05524369692

github.com/elif-ozkan?tab=repositories

linkedin.com/in/elif-özkan-04b603279

Skills

- Entity Framework
- React
- Active Directory
- Basic Networking
- Logging
- Syslog Windows
- Splunk
- Wazuh
- Bash script
- ISO 27001
- Kali Linux
- Web Application Security
- Reconnaissance/Information Gathering
- Penetration Testing
- Nmap
- Metasploit
- Wireshark

Profile

I am a Junior Cyber Security Analyst with hands-on experience in SOC-oriented tools and security laboratories. I have actively worked with SIEM platforms (Wazuh, Splunk), log analysis, and the fundamental processes of threat detection. I have a strong interest in MDR environments and in integrating artificial intelligence techniques into cybersecurity operations. Through my internships, projects, and practical lab studies, I have gained experience with Active Directory, Linux systems, network traffic analysis, and common security testing tools. I aim to contribute to real-world detection, monitoring, and response processes within a professional security team while continuously improving my technical and analytical skills.

Education

Information Systems Engineering **Sep 2021 - Jul 2025**
Kocaeli University, Kocaeli

Employment

Junior Artificial Intelligent Engineer **Jul 2025 - Jan 2026**
MaviAy Software, Kocaeli

- Within the scope of the project, I made forward-looking predictions using the React Reinforcement Learning method and deep learning models.

Software & Cyber Security Long Term Intern **Feb 2025 - Jun 2025**
iCredible Technologies, Inc., İstanbul

- I developed a web project using Entity Framework and React, and received Logging training on web security vulnerabilities.

Windows System Assistant Intern **Dec 2023 - Nov 2024**
Splunk TRtek MEDICAL SOFTWARE, Kocaeli, Türkiye

- I received training in Active Directory, Basic Networking, Logging, and Syslog Windows.
- I took training on Splunk usage for logging and also practiced by implementing Wazuh on a virtual machine.
- I completed hands-on projects regarding user authorization and permission management using Active Directory.
- I also worked on practical exercises and projects related to Bash script writing.

Cyber Security Intern **Aug 2024 - Aug 2024**
ÖLÇSAN Teknoloji, İstanbul

- Trained in ISO 27001, Kali Linux, Web Application Security, Nmap Reconnaissance/Information Gathering, and Penetration Testing.
- Hands-on experience solving vulnerable machines using Nmap, Metasploit, Wireshark, theHarvester, sqlmap, and Burp Suite.

Volunteer Cybersecurity Editor **Sep 2025 - Present**
Arslan Yazılım

theHarvester

sqlmap

Burp Suite

Artificial Intelligence

Cyber Threat Intelligence

SOC tools

SIEM platforms

MDR environments

Deep learning models

Reinforcement Learning

Languages

English

- I write informative cybersecurity content.
- I have written articles on Cryptology & Encryption Algorithms, Volatility usage, Burp Suite, Metasploit, Binwalk & firmware analysis, and Steganography.

Courses

Cisco Networking Academy Curriculum **Nov 2025**
Followed the Cisco Networking Academy curriculum and completed hands-on training using Cisco Networking Academy's Cybersecurity Lab application in English VirtualBox. Continuing my studies and preparations within the scope of the exam.

ISO/IEC 27001:2022 ISMS Awareness and Internal Auditor **Nov 2024**
After receiving theoretical training on information security procedures and auditing stages, I applied my knowledge to sample scenarios, put it into practice, and prepared reports.

Cybersecurity Summer Camp **Jul 2025**
Performed hands-on exercises on firewall installation and configuration. Enhanced my theoretical knowledge in SOC and Cyber Threat Intelligence, and gained information about the MITRE ATT&CK Framework. After completing basic penetration testing training, I participated in CTFs on the Cyberexam platform.

Introduction Cyber Security **Feb 2025**
Received theoretical training on the global impacts of cyber threats, the effects of cybersecurity on various industries, vulnerabilities in networks, and why cybersecurity is a rapidly growing profession.

Detection Engineering Learning Path **Jul 2024**
Completed training and hands-on labs covering basic XDR/EDR, SIEM, log collection, introduction to Bash scripting, and fundamental Windows security. Acquired skills in developing rules to analyze security events and establish correlations.

SOC Analyst Learning Path **Feb 2024**
Learned phishing and web attack detection, VirusTotal usage, basic malware document analysis, log analysis, and related tools including Event Viewer and Syslog. Completed challenge applications, incident analysis, and playbook exercises.

XDR-EDR Basics **Feb 2024**
Gained theoretical knowledge on fundamental XDR and EDR concepts.

Secure the Future Achievement Certificate **Dec 2024**
Participated in the program organized in collaboration with Microsoft Türkiye, ADEO Cyber Security, Soitron Türkiye, Cyberwise, and KoçSistem. Acquired valuable knowledge and self-development opportunities in critical areas of cybersecurity, including: Microsoft infrastructure fundamentals, SOC & Threat Intelligence, Incident Response & Cybersecurity Engineering, Microsoft Information Security Fundamentals, Microsoft Identity and Access Security. Gained familiarity with products and structures used in these fields. Conducted experiments to build my own security laboratory.

Kali Linux 101 **Oct 2023**
After completing the theoretical training on Kali Linux usage, I performed hands-on

applications on a virtual machine.

Cyber Threat Intelligence and Threat Hunting **Jul 2023**
Received training and performed hands-on exercises on cyber threat intelligence concepts, including Deep Web, VirusTotal, Elasticsearch usage, and an introduction to memory analysis.

Social Engineering and Phishing **Aug 2023**
Gained knowledge about what social engineering is, how it is carried out, its critical importance, and various types of phishing.

Projects

OWASP LLM Security Labs **Dec 2025**
Laboratory project to evaluate the security of LLM-based systems
I am currently developing a hands-on lab project focused on manual security testing aligned with the OWASP LLM Top 10. Within the scope of the project, practical analysis is being performed on risks such as prompt injection and jailbreak scenarios, data leakage, insecure output handling, and model misuse. The project is actively under development, with future plans to implement semi-automation and SOAR (Security Orchestration, Automation and Response) integration.

Cyber Sentinel: AI-Powered Anomaly Detection Collection of Network Traffic Anomaly Datasets and Classification with AI Models **Sep 2024**
Collection and classification of network traffic anomaly datasets using AI models
The most commonly used network traffic anomaly datasets in the literature have been collected. These datasets were utilized for classification using transformer-based artificial intelligence models. The performance of the developed deep learning-based system was compared with other models, and the results were supported and explained through Explainable AI (XAI) techniques. The project is still under active development. As it is currently in the academic publication phase, the project can be shared upon request.

Build SOC Labs **Jan 2026**
I built an end-to-end SOC lab by integrating Suricata IDS with Wazuh SIEM in a low-resource environment, where I deployed ET Open Rules and validated detections through controlled attack simulations such as Nmap and testmyids. I configured the Wazuh Agent to ingest and analyze Suricata JSON logs (eve.json) and performed terminal-based SIEM alert correlation on the Wazuh Manager without relying on dashboards by directly analyzing alerts.json. To ensure system stability and efficiency, I optimized performance by intentionally disabling the dashboard and limiting log processing to alert-only events.

Volunteer Community Work

Member, Cyberus Cybersecurity Team
Fundamental cybersecurity training and competition participation
Fundamental cybersecurity training completed, including hands-on vulnerable machine exploitation. Competed in Hackmasters 2023 cybersecurity competition. Actively exploited SQL Injection vulnerabilities using sqlmap. Found XSS vulnerabilities through in-depth manual testing.