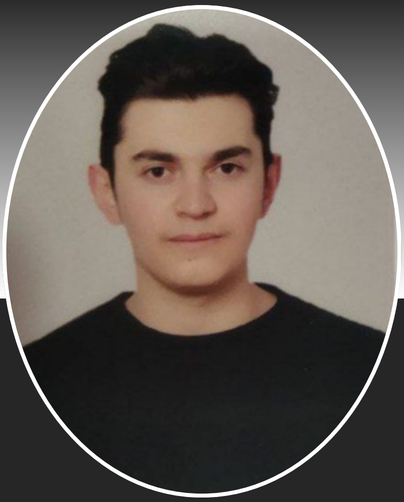

YILMAZ KARATAŞ

Computer Science

CONTACT

☎ 0535 026 6901

✉ yilmazkaratas571@gmail.com

https://github.com/yilmazkrts

Selçuklu/Konya

SKILLS

- Python
- Linux
- OWASP TOP 10
- ELK Stack
- Google Cloude

LANGUAGE

- Turkish
- English

ABOUT ME

I am a candidate focused on developing myself in the field of cybersecurity, particularly in Web Penetration Testing. I actively use platforms such as HackTheBox and PortSwigger Academy to enhance my practical skills, and I contribute to log management and security analysis processes at the company where I am currently interning. Additionally, I have built a basic SIEM environment using ELK Stack and continue to improve it.

WORK EXPERIENCE

Cyber Security & Log Analysis
15.09 – halen

Worked with Elasticsearch, Logstash, and Kibana (ELK Stack) technologies to explore log collection, analysis, and visualization processes. Collected web application logs through Logstash, processed them in Elasticsearch, and visualized the data using Kibana. Developed an alert system that automatically triggered when multiple failed login attempts occurred within a short time frame.

Language Model Development
14.05- 18.08

Anssoft

Developed AI-based applications using the LangChain framework and open-source language models. Optimized model performance through fine-tuning and implemented RAG (Retrieval-Augmented Generation) architecture to create intelligent systems capable of retrieving and processing external data sources. Gained hands-on experience in enhancing the reasoning and retrieval capabilities of large language models.

EDUCATION

Selcuk University 2020 - 2026

Computer Sciences

Refahiye science high school 2016 - 2020

REFERENCES

Muammer Ağtaş

Network and Application Monitoring Specialist/Halkbank

Phone: 0538 030 19 76

Dear Hiring Manager,

I am writing to express my strong interest in the SOC L1 Analyst position. As a Computer Engineering graduate with a strong focus on blue team operations, SIEM-based monitoring, and security detection, I am eager to contribute to a Security Operations Center while continuously developing my skills in a real-world SOC environment.

As part of my hands-on projects, I designed and deployed a basic SIEM architecture using the ELK Stack (Elasticsearch, Logstash, and Kibana). To generate realistic traffic and logs, I published and hosted a web application, enabling me to simulate real-world attack and anomaly scenarios. I configured Logstash pipelines to ingest live web application logs, analyzed them in Elasticsearch, and built custom Kibana dashboards to monitor authentication events, request patterns, and abnormal behaviors.

Within this environment, I implemented alerting mechanisms to detect suspicious activities such as multiple failed login attempts within a short timeframe. This provided me with practical experience in SOC L1-level alert triage, log analysis, prioritization, and initial incident assessment.

In addition to my project-based experience, I was accepted into the Garanti BBVA Technology Security Academy, where I successfully completed general aptitude, English, and technical evaluation stages. This selective process further strengthened my technical foundation and readiness for SOC-focused roles.

Furthermore, I was selected for the Siber Vatan Cybersecurity Program, where I received comprehensive training in Linux systems and network security. As part of the program, I successfully completed a Capture The Flag (CTF) competition, gaining hands-on experience in security analysis and problem-solving through realistic scenarios. I am currently accepted into the program’s advanced online and in-person training and bootcamp phases, further enhancing my defensive security skill set.

These experiences improved my ability to recognize attacker behavior through logs and to align detection mechanisms with frameworks such as MITRE ATT&CK. In parallel, I actively enhance my offensive security awareness through platforms such as Hack The Box and PortSwigger Academy, enabling me to better understand attacker techniques and strengthen defensive detection capabilities.

I am detail-oriented, highly motivated, and comfortable working in shift-based SOC environments. I am confident that my practical SIEM experience, structured cybersecurity training, and strong willingness to learn will allow me to add value as a SOC L1 Analyst.

Thank you for your time and consideration. I would welcome the opportunity to further discuss how my skills and motivation align with your SOC operations.

Sincerely,
Yılmaz KARATAŞ