






Berkan Türel


 Elazig / Turkey (Mobile)


 turelberkan9@gmail.com


 -----

 [Berkan Türel](#)

 [Berkan Türel](#)

 [Berkan Türel](#)

 [Berkan Türel](#)

 [Berkan Türel](#)

WORK EXPERIENCE

Cyber Security Analyst at PURE7

Remote | 01/2024 - Ongoing

Cyber Security Analyst at Destel @IGA

Remote | 05/2023 - 01/2024

- As a SOC Analyst, I specialized in monitoring and analyzing our organization's network and systems, with a particular focus on cyber threat intelligence. Utilizing advanced security tools like Splunk, FortiSOAR, and Cisco AMP, I ensured prompt detection and response to potential threats while actively contributing to our proactive cybersecurity stance.
- My role prominently featured engagement in cyber threat intelligence analysis and reporting, allowing me to stay at the forefront of emerging threats and vulnerabilities. Through collaboration with internal and external teams, I facilitated the exchange of crucial insights, empowering our organization to preemptively address cybersecurity risks.
- Additionally, I played a pivotal role in incident response activities, leveraging my expertise in Windows Forensics and file analysis tools to mitigate risks effectively and safeguard our systems. My dedication to bolstering our cybersecurity posture remained unwavering as I continuously refined our defense strategies to stay ahead of evolving threats.



Freelance Security Engineer

Fiverr | 12/2022 - present

- Developing network projects and cybersecurity tools tailored to clients' needs.
- Designed, implemented, and maintained a range of cybersecurity tools, including vulnerability scanners, network monitors, and intrusion detection systems.

EDUCATION



Software Engineering

Firat University | 2019 - 2023

- bachelor's degree - 2.97/4.00

LANGUAGES

- Turkish**
Native Language
- English**
Professional Working Proficiency

Volunteer Experience

System Administrator, Cyber Shield Community

I oversee a cybersecurity blog site and a CTI Telegram channel, managing content curation. Additionally, I assist in organizing educational events

Personal Cybersecurity Channel

I curate and share educational cybersecurity videos on my personal cybersecurity channel, fostering knowledge dissemination and awareness in the cybersecurity domain.

SKILLS

- Threat Hunting
- Python
- Cyber Threat Intelligence
- Linux
- Firewall
- EDR
- SOAR
- SIEM
- Sigma Rules

PERSONAL PROJECTS

Automated Cybersecurity Report Aggregator and Notifier

It collects the latest cybersecurity reports from over 200 sharing sites and notifies users via email based on predefined keywords. Using web scraping, it categorizes and summarizes the reports. Users can enhance their security measures proactively by staying informed about current threats and vulnerabilities.

Automated Ransomware Group Activity Tracker and Alert System

RansomTrack is a Python-based project I developed to monitor the activities of ransomware groups and deliver updates via email. Leveraging web scraping techniques, it gathers and analyzes data from various sources, capturing ransomware group movements and sharing announcements. By staying informed about ransomware group activities, organizations can strengthen their cybersecurity measures and proactively defend against potential threats.

Network Reconnaissance Tool

I developed a Network Reconnaissance Tool using Python and the Scapy library. The tool can operate in two modes: active and passive. In active mode, it sends ICMP packets to all IP addresses on the network to discover live hosts. In passive mode, it listens for ARP packets on the network to map IP and MAC addresses of all hosts. The tool provides valuable insights into the network topology and can be useful for both offensive and defensive security purposes.

Attack Simulation Tool

Attack Simulation Tool using Python that can scan given IP addresses for open ports and launch brute force attacks on them. Specifically, the tool can target ports such as Telnet (23), SSH (22), and web (80) to enable remote command execution via brute force attacks. Additionally, the tool allows for file upload to the target system via these ports.

Certificates

Ransomware Attacks: Basics, TTPs, and Countermeasures

Intro to Splunk

THY Cyber Take off 2022