EREN ATALAY

eren.atalay.cs@gmail.com | +44 7496861826 | https://www.linkedin.com/in/eren-atalay/

PROFILE

Cybersecurity professional with hands-on experience in SIEM engineering, threat detection, security monitoring, and internal security tool development. Experienced in building and tuning Wazuh-based monitoring environments, developing detection logic, and analysing telemetry across cloud, identity, and infrastructure platforms including Microsoft 365, Azure AD, Cloudflare, and endpoint-related logs. Strong foundation in cybersecurity operations, threat investigation, and applied machine learning for anomaly detection, supported by a Computer Science background and practical project delivery in both academic and professional environments.

SKILLS

Security Operations & Monitoring: SIEM monitoring, alert triage, log analysis, correlation rules, threat detection, basic incident investigation, phishing analysis, anomaly detection

Security Tools & Platforms: Wazuh, Splunk (basic), ELK Stack (conceptual), Burp Suite, Nmap, Wireshark, OWASP ZAP, Suricata

Cloud & Identity Security: Microsoft 365, Azure AD, Cloudflare logs, Google Cloud Platform (IAM, VM, Storage), secure access controls

Programming & Scripting: Python, Java, C++, Bash, basic PowerShell, Flask

Networking & Infrastructure: TCP/IP, DNS, DHCP, VLANs, subnetting, VPNs, firewall concepts, Windows, Linux (Ubuntu, Kali), macOS

Databases & Data Handling: SQL, MySQL, Pandas, data analysis, log parsing

AI / ML for Security: Scikit-learn, supervised learning, anomaly detection, feature evaluation, model validation

EXPERIENCE

CYBERSECURITY ENGINEER

PyramidLedger | On-site **May 2025 - Present**

- Built and deployed a Wazuh-based SIEM for centralised log collection, correlation rules, and real-time threat detection.
- Developed internal security tools including a bug bounty reconnaissance tool and an AI-assisted phishing detection system.
- Implemented monitoring pipelines for fintech and trading platforms, focusing on anomaly detection and security visibility.
- Investigated security events using Cloudflare, Azure AD, Microsoft 365, and cloud infrastructure logs.
- Created security dashboards and automated alerting workflows to support SOC monitoring and incident response.
- Gained hands-on exposure to banking and financial-sector security architectures and authentication monitoring.

CYBERSECURITY ANALYST INTERNSHIP

Cyberdose | On-Site **Mar 2025 - May 2025**

- Participated in an intensive cybersecurity mentorship programme focused on threat detection, incident response, and SOC operations.
- Performed hands-on security labs including log analysis, phishing investigation, and threat hunting exercises.
- Worked with security monitoring tools and simulated attack scenarios to understand real-world incident response workflows.
- Collaborated with mentors and peers on cybersecurity case studies and defensive security strategies.

AI EVALUATION & ALIGNMENT CONTRIBUTOR

Outlier | Remote **Nov 2024 - Mar 2025**

- Guided prompt design and reviewed AI outputs for RLHF systems.
- Evaluated AI-generated code for accuracy, relevance, and clarity.
- Collaborated with researchers to improve datasets and model behaviour.

DATACENTER TECHNICIAN

Survivor Bilgi Sistemleri | On-site (Part time) **Mar 2020 - July 2021**

- Installed, configured, and maintained servers and network infrastructure.
- Supported patching, backups, and routine security checks.
- Collaborated with network engineers for troubleshooting and optimisation.

CERTIFICATIONS

- Google Cybersecurity Professional Certificate – May 2025
- CompTIA A+ (Cyber Specialization) – Dec 2023

PROJECTS

AI-Powered Network Threat Detection

Developed an ML-based intrusion detection system using supervised and unsupervised models. Achieved 90%+ F1-score detecting anomalies (DDoS, PortScan). Evaluated with cross-validation and confusion matrices.

Technologies: Python, Scikit-learn, Pandas, CICIDS2017 Dataset

Distributed Key-Value Storage Network

Implemented a peer-to-peer network (Java) with PUT/GET operations and node discovery. Tested via Wireshark for protocol compliance.

Technologies: Java, TCP/IP, SHA-256

Cloud File Management Platform

Created Flask-based web app for file upload/download with tagging and search. Integrated Google Cloud Storage and IAM for secure access control.

Technologies: Flask, GCP, Google Cloud Storage, IAM

UK Legal Case Search System using Apache Solr

Scraped UK legal documents, indexed with Solr for keyword and metadata search.

Technologies: Apache Solr, Python, Web Scraping

EDUCATION

BSc Computer Science – City, University of London | Sep 2022 – Jul 2025

Relevant modules: Computer Networks, Operating Systems, Cloud Computing, Information Retrieval, Programming in Java/C++, AI, Theory of Computation. Final-year project: AI-Powered Network Threat Detection.

Foundation Certificate in Science and Engineering – Kaplan International College London | Nov 2021 – Aug 2022

Coursework in Mathematics, Information Technology, and Academic English.