Fatih Serdar Çakmak

Istanbul, Turkey • +90 538 482 8810 • fscakmak@proton.me • linkedin.com/in/fatihserdar • github.com/yatuk • fscakmak.com

PROFESSIONAL SUMMARY

Computer Engineering student at ITU, currently in my second consecutive cybersecurity internship. Worked across **SIEM, SOAR, EDR, and NDR** platforms: log correlation, alert triage, playbook development, and incident response. Blue team focus, MITRE ATT&CK, BDDK compliance.

EXPERIENCE

Fibabanka Istanbul, Turkey
Cyber Security Operations (SOC) Intern Mar 2026 – Present

- Monitored production security alerts, reviewed **CTI feeds**, and handled daily triage under senior analyst supervision.
- Supported incident documentation and firewall log review in a **BDDK**-regulated environment.

Doğuş Teknoloji Istanbul, Turkey
Cybersecurity and Incident Response Intern Jul 2025 – Mar 2026

- Worked across **SIEM, SOAR, EDR, and NDR** platforms: log correlation, alert triage, playbook writing, and false-positive filtering across enterprise infrastructure.
- Helped senior analysts write and refine **SOAR playbooks** for recurring threats including phishing; assisted with EDR alert tuning to reduce detection noise.
- Provided **L1 incident response** support, contributed to Root Cause Analysis (RCA), and prepared case reports aligned with SLA requirements.
- Monitored **Active Directory** and Windows/Linux system logs; applied network segmentation principles to maintain secure IT/OT boundaries.

TECHNICAL PROJECTS

SOC Case Study Project (SIEM/SOAR Simulation) [GitHub]

- Simulated multi-stage attacks mapped to **MITRE ATT&CK** TTPs; built log datasets to improve SIEM correlation rules and designed Python-based SOAR playbook flows for automated triage.

Database Management System (WDI Analytics) [GitHub]

- Full-stack data platform with RBAC, parameterized SQL to prevent injection attacks, and enforced data integrity across 10,000+ records.

EDUCATION

Istanbul Technical University (İTÜ) 2023 – 2027 (Expected)
B.Sc. in Computer Engineering

Kocaeli ENKA Technical Schools 2019 – 2023
Industrial Automation (Technical High School Diploma)

TECHNICAL SKILLS

– **Cybersecurity:** SOC Operations, Incident Response (IR), Log Analysis, CTI, SIEM, SOAR, EDR Alert Tuning, SOAR Playbook Development, Log Source Configuration, False-Positive Filtering, MITRE ATT&CK.

– **Infrastructure:** Network Security, Network Segmentation, Firewall Log Analysis, Active Directory, Windows/Linux Administration, Vulnerability Assessment.

– **Compliance:** BDDK Regulatory Awareness, Banking Security Standards, Incident Reporting.

– **Tools & Programming:** Python, Go, C/C++, SQL, Cortex XSOAR, Wireshark, Git.

– **Languages:** English (Professional), Turkish (Native).