Fatih Serdar Çakmak

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

EXPERIENCE

Fibabanka — Istanbul, Turkey
Cybersecurity Operations (SOC) Intern — Mar 2026 – Present

- Triage production SIEM and EDR alerts in a BDDK-regulated banking SOC, escalating confirmed incidents to senior analysts.
- Design and run n8n automation workflows for the SOC, covering LLM-assisted alert triage, IOC enrichment, and phishing analysis to reduce manual L1 steps.
- Review CTI feeds and track daily alert volumes; write incident documentation used in shift handovers and audit records.

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

- Triaged alerts and filtered false positives across SIEM, SOAR, EDR, and NDR platforms on a live SOC shift.
- Wrote and tuned Cortex XSOAR playbooks for phishing and recurring threat patterns together with senior analysts.
- Handled L1 incident response tasks and prepared case reports within SLA targets.
- Monitored Active Directory and Windows/Linux logs; supported basic network segmentation work.

PROJECTS

Tamga: Self-Hosted LLM Security Proxy — Go, Python (FastAPI), Next.js | github.com/yatuk/tamga

- Built a proxy that sits between applications and LLM providers (OpenAI, Anthropic, Azure, Vertex); redacts PII such as TC Kimlik and IBAN numbers, blocks leaked secrets, and flags prompt injection.
- Implemented the static scanner as an Aho-Corasick DFA, keeping per-request scan latency under one millisecond; CI runs a 309-prompt adversarial suite on every change.
- Mapped controls to KVKK, BDDK, GDPR, and PCI-DSS; added hash-chained audit logs and an incident dashboard.

MCPRadar: Security Scanner for MCP Servers — Python, published on PyPI | github.com/yatuk/mcpradar

- Scans Model Context Protocol servers for tool poisoning, prompt injection, and supply-chain rug pulls using six detection rules (zero-width Unicode, encoded blobs, permission scope mismatches, and more).
- Outputs SARIF for the GitHub Security tab; SQLite snapshot diffing catches servers that change schemas after approval.

SOC n8n Workflows: SOC Automation Playbooks — n8n, JSON | github.com/yatuk/soc-n8n-workflows

- Published ten import-ready n8n playbooks for SOC work: LLM-assisted alert triage, phishing analysis, IOC enrichment, human-approved containment, CVE watch, and reporting, based on patterns from real shifts.

EDUCATION

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

Kocaeli ENKA Technical Schools — 2019 – 2023
Industrial Automation, Technical High School Diploma

TECHNICAL SKILLS

Security Operations	SOC Operations, Alert Triage, Incident Response, Threat Detection, Log Analysis, Phishing Analysis, IOC Enrichment, CTI, MITRE ATT&CK
Platforms & Automation	SIEM, SOAR (Cortex XSOAR), EDR/NDR, n8n, Wireshark, Docker, Git
AI/LLM Security	Prompt Injection Defense, PII Redaction, MCP Security, LLM-Assisted Triage
Infrastructure	Active Directory, Windows/Linux Administration, Network Security Basics
Compliance	BDDK Regulatory Awareness, KVKK, ISO/IEC 27001 Awareness, Incident Reporting
Code	Python, Go, SQL, C/C++, FastAPI
Languages	English (Professional), Turkish (Native)