EREN ÖNDER

Cyber Security Specialist | SOC
Bahçelievler, İstanbul | +90 530 523 55 49 | eerenonder0@gmail.com
linkedin.com/in/erenonder0 | erenonder.com

PROFESSIONAL SUMMARY

I gained hands-on field experience in critical national infrastructure, working in SIEM-based threat detection, incident response, malware analysis, penetration testing, and email security. I am proficient in Splunk and IBM QRadar, with practical experience in SOAR automation, EDR investigation, and MITRE ATT&CK. I develop AI-assisted automation tools to improve the efficiency of analysis and triage processes in SOC operations, and I have a strong interest in offensive security simulation from a red team perspective, as well as malware analysis and reverse engineering. I hold a bachelor's degree in Digital Forensics Engineering (GPA 3.64) and have two peer-reviewed publications on machine learning-based threat detection. I am seeking a position within a SOC team.

CORE COMPETENCIES

Security Operations: SIEM, SOC, Alert Triage, Incident Correlation, Log Analysis, Security Monitoring, Escalation Management

Threat & Incident Management: Incident Response, Threat Detection, Threat Hunting, Phishing Analysis, Malware Triage, IOC Analysis, MITRE ATT&CK, Cyber Kill Chain, Root Cause Analysis

Engineering & Automation: Correlation Rule Tuning, Use Case Development, False Positive Reduction, SOAR Playbook Development

TECHNICAL SKILLS

SIEM & SOAR: Splunk (SPL), IBM QRadar (AQL), Cisco XSOAR / Cortex XSOAR

Endpoint & Email: Cisco AMP, Trend Micro Vision One, Cisco Email Security Appliance, Beamsec, EDR, XDR

Network & Infrastructure: TCP/IP, DNS, DHCP, Firewall, IDS/IPS, Proxy, DLP, Network Segmentation, Active Directory, Windows Event Log, Linux, Kali Linux

Analysis Tools: Wireshark, Nmap, VirusTotal, Sysmon, Sandbox Analysis, Google Dorking, OSINT

Digital Forensics: Network Forensics, Disk Imaging, Timeline Analysis

WORK EXPERIENCE

Istanbul Airport (İGA) İstanbul
Cybersecurity Specialist *03/2026 - Present*

- Detected and escalated security incidents across critical airport infrastructure by monitoring and correlating log sources on Splunk SIEM using custom SPL queries mapped to MITRE ATT&CK techniques.
- Replaced manual enrichment and escalation steps for recurring alert types with automated incident response playbooks built in Cisco XSOAR.
- Analyzed EDR telemetry on Cisco AMP during alert investigations, applying host isolation and IOC-based blocking.
- Analyzed email headers, attachments, and embedded URLs via Cisco ESA and Beamsec, blocking verified IOCs organization-wide and thereby detecting and neutralizing phishing and BEC attempts.

OnBT Kalyon Holding İstanbul
SOC L1 Analyst (Intern) *09/2025 - 01/2026*

- Triaged company-wide security alerts by applying documented L1 playbooks on IBM QRadar and Trend Micro Vision One, escalating confirmed true positives to L2 within SLA.
- Analyzed raw event logs and enriched IOCs using VirusTotal and open-source threat intelligence sources, classifying and escalating phishing, malware, and intrusion attempts on a monthly basis.

Turkish Technology İstanbul
Network Management Intern *07/2025 - 08/2025*

- Evaluated firewall, IDS/IPS, and network segmentation configurations for the corporate network environment against industry best practices, presenting recommendations for improvement.
- Conducted PoC tests for the protection of critical systems and reported comparative findings to team members.
- Detected and classified abnormal network activity through SIEM-based monitoring, documenting findings and reporting to the operations team.

PUBLICATIONS & PROJECTS

Vardia - Cyber Threat Intelligence Platform Personal Project | 2026

- Developed a cyber threat intelligence platform that consolidates CVEs, zero-days, ransomware leaks, dark web announcements, and security news into a single feed, prioritizing them according to the organization's technology stack.
- Built a mechanism that automatically scans the dark web and closed sources for specified keywords, detecting data leak announcements in real time and sending instant alerts — significantly reducing SOC teams' time to leak awareness.

URL Guard - AI-Powered Malicious URL Detection System Personal Project | 2026

- Designed a self-improving phishing/malicious URL detection system that combines machine learning, rule-based analysis, threat intelligence, and AI within a single decision engine.
- Designed a mechanism that evaluates evidence from multiple sources — blacklists, brand impersonation detection, domain and certificate reputation — using AI to produce a reasoned, confidence-scored verdict.

High-Performance Spyware Classification Using Wavelet Transform Features ICAIE 2025 | 09/2025

- Achieved 97.06% spyware detection accuracy on network traffic data by extracting Daubechies wavelet transform features and training a Decision Tree classifier.
- Presented the study as a paper at the 3rd International Conference on Advances and Innovations in Engineering, held at Fırat University, and published it in the conference proceedings.

Cyber MAIN - Intrusion Detection System Concept HAVELSAN Hackathon | 04/2024

- Designed a next-generation, AI-powered intrusion detection system concept for HAVELSAN's MAIN artificial intelligence platform within a 26-hour period, placing 3rd among approximately 40 teams.

CERTIFICATIONS

- Certified Network Security Practitioner (CNSP) – The SecOps Group, 07/2025
- Splunk Training Series (eLearning) – Splunk, 07/2025 – 04/2026: Intro to Splunk, Using Fields, Working with Time, Scheduling Reports & Alerts, Intro to Knowledge Objects, Statistical Processing, Visualizations
- CCNA: Introduction to Networks – Cisco, 01/2024
- Introduction to Cybersecurity – Cisco, 12/2023
- Introduction to Cybersecurity 101 (24 hours) – Turkcell, 03/2023

EDUCATION

Fırat University Elazığ

Digital Forensics Engineering(B.Sc.) *09/2022 - 07/2026*

GANO: 3.64 / 4.00 | Relevant coursework: Network Security, Digital Forensics, Cryptography, Operating Systems

VOLUNTEER WORK & LEADERSHIP

President, SGT Club, Fırat University (2023 – 2025) | Event and Organization Coordinator, Cyber Anatolian Communities (2023 – 2025) | Core Team Member, Google Developer Student Club (2023)

LANGUAGES & INTERESTS

Languages: Turkish (Native), English (B1 – Developing)

Interests: CTF competitions, blue team research, cybersecurity content creation