EREN ÖNDER

Siber Güvenlik Uzman Yardımcısı | SOC & Olay Müdahale
Bahçelievler, İstanbul | +90 530 523 55 49 | eerenonder0@gmail.com
linkedin.com/in/erenonder0 | erenonder.com

PROFESYONEL ÖZET

Kritik ulusal altyapıda saha deneyimi kazandım; SIEM tabanlı tehdit tespiti, olay müdahale, zararlı yazılım analizi, pentest ve e-posta güvenliği alanlarında çalışıyorum. Splunk ve IBM QRadar platformlarında yetkinim; SOAR otomasyonu, EDR incelemesi ve MITRE ATT&CK konularında uygulamalı tecrübeye sahibim. SOC operasyonlarında analiz ve triyaj süreçlerinin verimliliğini artırmak amacıyla yapay zekâ destekli otomasyon araçları geliştiriyorum; ayrıca red team perspektifiyle saldırı simülasyonu ile zararlı yazılım analizi ve tersine mühendislik alanlarına ilgi duyuyorum. Adli Bilişim Mühendisliği lisans mezunuyum, GANO 3.64 ve makine öğrenmesi tabanlı tehdit tespiti alanında iki hakemli yayınım bulunuyor. SOC pozisyonunda görev almayı hedefliyorum.

TEMEL YETKİNLİKLER

Güvenlik Operasyonları: SIEM, SOC, Alarm Triyajı, Olay Korelasyonu, Log Analizi, Güvenlik İzleme, Eskalasyon Yönetimi

Tehdit ve Olay Yönetimi: Olay Müdahale, Tehdit Tespiti, Tehdit Avcılığı , Oltalama Analizi, Zararlı Yazılım Triyajı, IOC Analizi, MITRE ATT&CK, Cyber Kill Chain, Kök Neden Analizi

Mühendislik ve Otomasyon: Korelasyon Kuralı İnce Ayarı, Use Case Geliştirme, Yanlış Pozitif Azaltma, SOAR Playbook Geliştirme

TEKNİK BECERİLER

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

Uç Nokta ve E-posta: Cisco AMP, Trend Micro Vision One, Cisco Email Security Appliance, Beamsec, EDR, XDR

Ağ ve Altyapı: TCP/IP, DNS, DHCP, Güvenlik Duvarı, IDS/IPS, Proxy, DLP, Ağ Segmentasyonu, Active Directory, Windows Event Log, Linux, Kali Linux

Analiz Araçları: Wireshark, Nmap, VirusTotal, Sysmon, Sandbox Analizi, Google Dorking, OSINT

Adli Bilişim: Ağ Adli Bilişimi, Disk İmajlama, Zaman Çizelgesi Analizi, Autopsy, Volatility

Programlama ve Betik: C, C++, Python, C#, Flutter, Bash

İŞ DENEYİMİ

İstanbul Havalimanı (İGA) İstanbul
Siber Güvenlik Uzman Yardımcısı *03/2026 - Halen*

- MITRE ATT&CK tekniklerine eşlenmiş özel SPL sorgularıyla Splunk SIEM üzerinde log kaynaklarını izleyip korele ederek kritik havalimanı altyapısındaki güvenlik olaylarını tespit ettim ve eskale ettim.
- Tekrar eden alarm tiplerindeki manuel zenginleştirme ve eskalasyon adımlarını, Cisco XSOAR üzerinde kurguladığım otomatik olay müdahale playbook'larıyla değiştirdim.
- Alarm incelemelerinde Cisco AMP üzerinde EDR telemetrisini analiz ederek host izolasyonu ve IOC tabanlı engellemeler uyguladım.
- Cisco ESA ve Beamsec üzerinden e-posta başlıklarını, ekleri ve gömülü URL'leri analiz ederek doğrulanmış IOC'leri kurum genelinde engellemeye aldım ve bu sayede oltalama ile BEC girişimlerini tespit edip etkisiz hale getirdim.

OnBT Kalyon Holding İstanbul
SOC L1 Analisti (Stajyer) *09/2025 - 01/2026*

- IBM QRadar ve Trend Micro Vision One üzerinde dokümante edilmiş L1 playbook'larını uygulayarak şirket genelindeki güvenlik alarmlarını triyaj ettim ve doğrulanan gerçek pozitifleri SLA süresi içinde L2'ye eskale ettim.
- Ham olay loglarını analiz edip IOC'leri VirusTotal ve açık kaynak tehdit istihbaratı kaynaklarıyla zenginleştirerek her ay oltalama, zararlı yazılım ve sızma girişimlerini sınıflandırdım ve eskale ettim.

Turkish Technology İstanbul
Ağ Yönetimi Stajyeri *07/2025 - 08/2025*

- Kurumsal ağ ortamı için güvenlik duvarı, IDS/IPS ve ağ segmentasyonu yapılandırmalarını sektör iyi uygulamalarına göre değerlendirerek düzenleme önerileri sundum.
- Kritik sistemlerin korunmasına yönelik PoC testleri yürütüp karşılaştırmalı bulguları ekip arkadaşlarıma raporladım.
- SIEM tabanlı izleme ile anormal ağ aktivitesini tespit edip sınıflandırdım, bulguları dokümante ederek operasyon ekibine raporladım.

YAYINLAR VE PROJELER

Vardia - Siber Tehdit İstihbaratı Platformu Kişisel Proje | 2026

- CVE, zero-day, fidye yazılımı sızıntıları, darkweb duyuruları ve güvenlik haberlerini tek bir akışta birleştiren, kurumun kullandığı teknolojilere göre önceliklendirme yapan bir siber tehdit istihbaratı platformu geliştirdim.
- Belirlenen anahtar kelimelerle darkweb ve kapalı kaynakları otomatik olarak tarayıp veri sızıntısı duyurularını gerçek zamanlı tespit eden ve anlık bildirim gönderen bir mekanizma kurdum; bu sayede SOC ekiplerinin sızıntıdan haberdar olma süresini önemli ölçüde kısalttım.

URL Guard - Yapay Zekâ Destekli Zararlı URL Tespit Sistemi Kişisel Proje | 2026

- Makine öğrenmesi, kural tabanlı analiz, tehdit istihbaratı ve yapay zekâyı tek bir karar motorunda birleştiren, kendi kendini geliştiren bir phishing/zararlı URL tespit sistemi tasarladım.
- Kara liste, marka taklidi tespiti, alan adı ve sertifika güvenilirliği gibi birden çok kaynaktan gelen kanıtı yapay zekâyla değerlendirip gerekçeli ve güven skorlu karar üreten bir mekanizma tasarladım.

Dalgacık Dönüşümü Öznitelikleriyle Yüksek Performanslı Casus Yazılım Sınıflandırması ICAIE 2025 | 09/2025

- Daubechies dalgacık dönüşümü öznitelikleri çıkarıp Karar Ağacı sınıflandırıcısı eğiterek ağ trafiği verisi üzerinde %97.06 casus yazılım tespit doğruluğu elde ettim.
- Çalışmamı Fırat Üniversitesi'nde düzenlenen 3. Uluslararası Mühendislikte Gelişmeler ve Yenilikler Konferansı'nda bildiri olarak sundum ve bildiri kitabında yayımlattım.

Cyber MAIN - Saldırı Tespit Sistemi Konsepti HAVELSAN Hackathon | 04/2024

- HAVELSAN'ın MAIN yapay zekâ platformu için yeni nesil, yapay zekâ destekli saldırı tespit sistemi konseptini 26 saatlik süre içinde tasarlayarak yaklaşık 40 takım arasından 3. sırayı elde ettim.

SERTİFİKALAR

- Certified Network Security Practitioner (CNSP) - The SecOps Group, 07/2025
- Splunk Eğitim Serisi (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
- Siber Güvenliğe Giriş 101 (24 saat) - Turkcell, 03/2023

EĞİTİM

Fırat Üniversitesi Elazığ

Adli Bilişim Mühendisliği (Lisans) *09/2022 - 07/2026*

GANO: 3.64 / 4.00 | İlgili dersler: Ağ Güvenliği, Adli Bilişim, Kriptografi, İşletim Sistemleri

GÖNÜLLÜ ÇALIŞMALAR VE LİDERLİK

SGT Kulübü Başkanı, Fırat Üniversitesi (2023 - 2025) | Etkinlik ve Organizasyon Koordinatörü, Cyber Anatolian Communities (2023 - 2025) | Çekirdek Ekip Üyesi, Google Developer Student Club (2023)

DİLLER VE İLGİ ALANLARI

Diller: Türkçe (Anadil), İngilizce (B1 - geliştirilmekte)

İlgi Alanları: CTF yarışmaları, mavi takım araştırmaları, siber güvenlik içerik üretimi