

MUHAMMED MARUF GÜVELİ

muhammedmarufguveli@gmail.com | linkedin.com/in/mguveli | github.com/whymami

İstanbul, Türkiye | Askerlik: Tamamlandı

ÖZET

Hepsiburada ekosisteminde SIEM, SOAR, EDR ve log yönetimi alanlarında aktif operasyonel deneyim kazanmış; 42 İstanbul altyapısıyla güçlü bir teknik temele ve kodlama yetkinliğine (Python, Bash) sahip Junior SOC / L1 Analist adayı. Güvenlik alarmlarının analizi (triage), eskalasyon süreçleri, incident response playbook otomasyonu ve log akış izleme süreçlerinde pratik tecrübe sahibi. TryHackMe SOC Level 1 path tamamlama yetkinliği ve temel düzey MITRE ATT&CK entegrasyon farkındalığı ile kurumsal güvenlik operasyonlarına değer katmaya hazırdır.

TEKNİK YETKİNLİKLER

- SIEM&LogYönetimi:** Splunk(SplunkPowerUser), LogAnalizi, WEF(WindowsEventForwarding), Sysmon, Anomali Tespiti
- SOAR & Otomasyon:** Cortex XSOAR (Incident Response, Playbook Tasarımı, Otomatik Triage & Eskalasyon)
- Güvenlik Çözümleri & Ağ:** CrowdStrike EDR, Ağ Güvenliği & Port Kontrolleri, WinRM, TCP/IP, DNS, HTTP/HTTPS, CCNA Temelleri
- Framework & Standartlar:** MITRE ATT&CK Framework (Temel Seviye Entegrasyon & Tehdit İzleme)
- Programlama & Scripting:** Python, Bash, C, C++
- İşletim Sistemleri:** Windows Server, Linux (Kurumsal Geçiş, Yönetim & Log Toplama)
- Pratik Siber Güvenlik:** TryHackMe (SOC Level 1 Path Completed)

DENEYİM

- Hepsiburada—Cyber Security Intern** (Ekim2024–Ekim2025)
 - Log Operations & Monitoring:
 - Günlük olarak log üretmeyen sistemlerin otomatik olarak tespit edilmesi, bu verilerin Splunk platformuna entegre edilmesi ve merkezi raporlama altyapısında depolanması sağlanmıştır.
 - Log akışı kesintilerinin proaktif olarak izlendiği ve anomali ile trend değişimlerinin raporlandığı özel monitoring yapıları tasarlanmıştır.
 - XSOAR Automation & Response (Playbook & Triage):
 - CrowdStrike EDR çözümünden gelen güvenlik alarmlarının XSOAR platformunda otomatik olarak incident'a dönüştürülmesi ve ilk triage süreçlerinin hızlandırılması sağlanmıştır.
 - Aylık kapatılan güvenlik olaylarının %5'inin rastgele seçilerek analist performans değerlendirme süreçlerinin otomatize edildiği playbook oluşturulmuştur.
 - Windows log kesintilerinde otomatik müdahale protokolleri geliştirilmiştir;
 - firewall port durumu kontrolleri, WinRM servis izleme/otomatik restart mekanizmaları, WEF subscription durum denetimleri ile ilgili ekiplere otomatik ticket açılması ve Slack entegrasyonu sağlanmıştır.

- **Instagram Sayfa Yöneticiliği - Kurucu/SerbestÇalışma** (2018-2025)
 - • Milyonlarca kullanıcıya erişen Instagram üzerinde iki adet yüksek takipçili haber sayfasının yönetimi üstlenilmiştir; kitle yönetimi, bilgi akışı ve reklam/etkileşim süreçleri koordine edilmiştir.
- **Avcılar Belediyesi Bilgi İşlem Müdürlüğü - Stajyer** (Temmuz 2023 – Ağustos 2023)
 - Teknik Destek Operasyonları:
 - Günlük IT destek talepleri etkin bir şekilde yönetilmiş, donanım ve yazılım arızalarının teşhis, çözüm ve dokümantasyon süreçleri koordine edilmiştir.
 - Altyapı Geçiş Projesi:
 - Kurumsal Linux geçiş projesinde aktif rol üstlenilerek eski sistemlerin modernizasyonuna ve optimizasyonuna teknik katkı sağlanmıştır.

EĞİTİM

- 42 İstanbul Yazılım Okulu (2024–2025)
 - Odak Alanları: C, C++, Python, Bash, Docker, IoT, Siber Güvenlik, Ekip Çalışması, Algoritma Geliştirme ve Problem Çözme
- Dumlupınar Üniversitesi - Bilgisayar Programcılığı (2021-2023)
 - Odak Alanları: Web Programlama, Nesne Tabanlı Programlama (OOP), Veritabanı Yönetimi

SERTİFİKALAR & PLATFORMLAR

- SOC Level 1 Path Completed — TryHackMe
- Splunk Power User (SPLK-1002) — Splunk
- CCNA: Introduction to Networks — Cisco
- CyberOps Associate — Cisco
- Introduction to Cybersecurity — Cisco
- Linux Unhatched — Cisco

REFERANSLAR

- **Anıl Kuş (Head of Security, Hepsiburada)** | anil.kus@hepsiburada.com
- **Ahmet Manga (CDC Team Lead, Hepsiburada)** | ahmet.manga@hepsiburada.com