

KURUMSAL SIBER SAVUNMADA AÇIK KAYNAK GÜCÜ: XDR MIMARISI, WAZUH EKOSİSTEMİ VE UYGULAMALI TEHDİT TESPİTİ

Yazar: Kerem Kaan AVCI | Siber Güvenlik / Tehdit Analizi & SOC Operasyonları

Tarih: 2026

ÖZET

Gelişen saldırı vektörleri karşısında saldırganların sistem içi yatay ilerleme (lateral movement) ve kalıcılık (persistence) sağlama süreleri ciddi oranda düşmüştür. Bu durum geleneksel SIEM çözümlerinin pasif log korelasyonunu yetersiz bırakmaktadır. Ticari çözümlerin yüksek lisans maliyetleri ve kapalı kaynak kod yapısı ise kurumları üreticiye bağımlı (vendor lock-in) kılmaktadır. Bu gereksinimler; uç nokta telemetrisini anlık işleyen, davranışsal anomalileri yakalayan ve güvenlik verisini merkezi olarak korele eden XDR (Genişletilmiş Algılama ve Yanıt) mimarilerini bir ihtiyaç haline getirmiştir.

Bu çalışmada, açık kaynak kodlu SIEM/XDR platformu olan **Wazuh** ele alınmış; izole bir test/analiz ortamı üzerinde Ubuntu Server (Manager & Indexer) ve Windows 11 Enterprise (Agent) mimarisi yapılandırılmıştır. Platform üzerinde Güvenlik Yapılandırma Değerlendirmesi (SCA - CIS Benchmark), Tehdit Avcılığı telemetrisi ve yetkisiz yerel kullanıcı oluşturulması (Persistence - MITRE ATT&CK T1098 / T1078) senaryoları simüle edilerek sistemin tespit kabiliyeti ve kurumsal uygulanabilirliği değerlendirilmiştir.

Anahtar Kelimeler: XDR, Wazuh, Uç Nokta Güvenliği, FIM, CIS Benchmark, MITRE ATT&CK, Tehdit Tespiti.

Bölüm 1: Tehdit Ortamı ve XDR İhtiyacı

Güvenlik Operasyon Merkezleri (SOC) uzun yıllar boyunca güvenlik duvarları, sunucular ve ağ cihazlarından gelen logları merkezi bir havuzda toplayarak alarm üreten klasik SIEM mimarilerine bağımlı kalmıştır. Ancak modern saldırı senaryolarında saldırganların içeride yetki yükseltme ve yayılma süreleri ciddi oranda düşmüştür. Bu durum geleneksel SIEM çözümlerinin pasif log korelasyonunu yetersiz bırakmaktadır:

- Reaktif Yaklaşım ve Müdahale Gecikmesi:** Geleneksel SIEM sistemleri kural eşleştğinde ekrana alarm üretir ancak saldırıyı durduracak doğrudan bir uç nokta görünürlüğüne ve anlık telemetri derinliğine sahip değildir. Analistin alarmı fark edip aksiyon almasına kadar geçen sürede saldırganlar yetki yükseltme veya veri sızdırma adımlarını tamamlayabilmektedir.
- Telemetri ve Görünürlük Eksikliği:** Ağ seviyesindeki loglar; bellekte çalışan zararlı kodları (fileless malware), yerel komut satırı manipülasyonlarını ve çekirdek seviyesindeki dosya değişikliklerini tek başına açıklamakta yetersiz kalır.

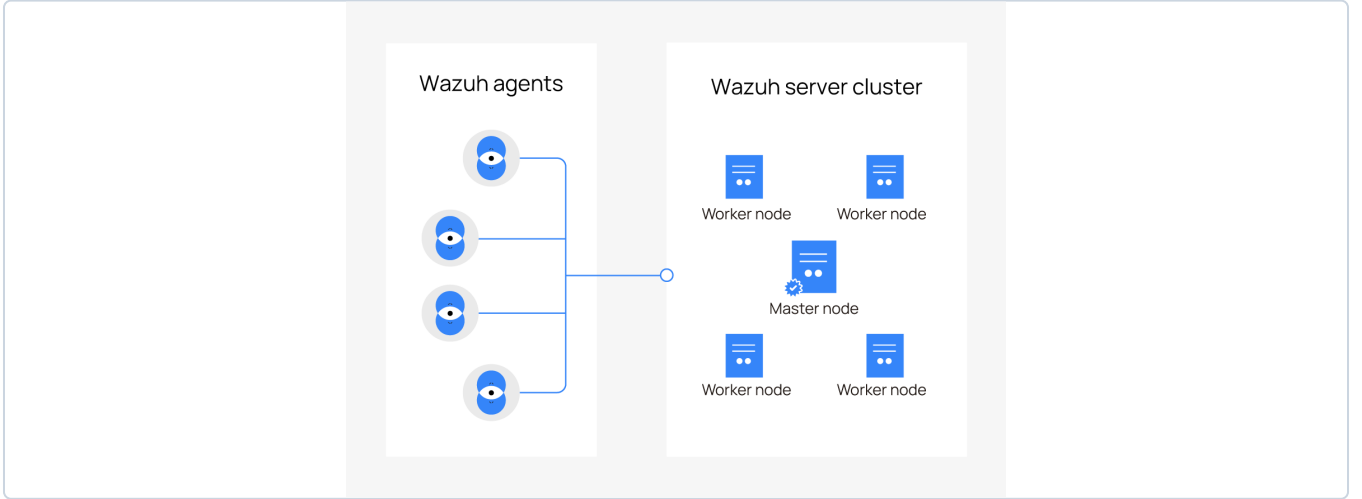
Bu noktada modern savunma mimarisi **XDR (Extended Detection and Response)** yaklaşımına yönelmiştir. XDR; uç nokta (EDR), ağ (NDR) ve bulut ortamlarından topladığı telemetriyi tek çatı altında korele ederek davranışsal anomalileri yakalar ve analistin önüne doğrudan aksiyon alınabilir bir tehdit zinciri koyar.

Bölüm 2: Açık Kaynak Güvenliğin Önemi ve Wazuh Ekosistemi

Ticari XDR çözümleri güçlü analiz yetenekleri barındırsa da yüksek lisans bedelleri ve kapalı kaynak yapısı sebebiyle operasyonel engeller barındırır. Cihaz başına talep edilen lisanslama modelleri bütçe kısıtlarına yol açarken, kapalı mimariler kurumları üreticiye bağımlı (vendor lock-in) kılmaktadır. Açık kaynak kodlu ve GPL lisanslı **Wazuh**, bu kısıtlamaları ortadan kaldırarak kurumsal seviyede bir güvenlik mimarisi sunar.

Wazuh'un Temel Yetenekleri:

- **Yazılım Lisans Maliyetinden Bağımsızlık:** Uç nokta sayısı arttıkça ek yazılım lisans bedeli doğmaz; bütçe planlaması yalnızca sunucu ve depolama altyapısına odaklanır.
- **Tek Çatı Altında Çoklu Modül:** Günlük Analizi (Log Analysis), Dosya Bütünlük Denetimi (FIM), Güvenlik Yapılandırma Değerlendirmesi (SCA), Zafiyet Tespiti ve Tehdit Avcılığı (Threat Hunting) tek bir ajan üzerinden yönetilir.
- **Genişletilebilir Güvenlik Altyapısı:** Kural dışı veya şüpheli aktivitelerde yerel betikler ve güvenlik duvarı kuralları tetiklenerek proaktif güvenlik adımları kurgulanabilir.
- **Şeffaf Kural Mimarisi:** XML ve Regex tabanlı dekode/kural yapısı sayesinde kurumlar kendi iç yazılımlarını ve özel log formatlarını sisteme kolayca entegre edebilir.



Görsel 1: Wazuh Cluster ve Dağıtık Ajan (Agent) Mimarisi

Bölüm 3: Laboratuvar Mimarisi ve Kurulum

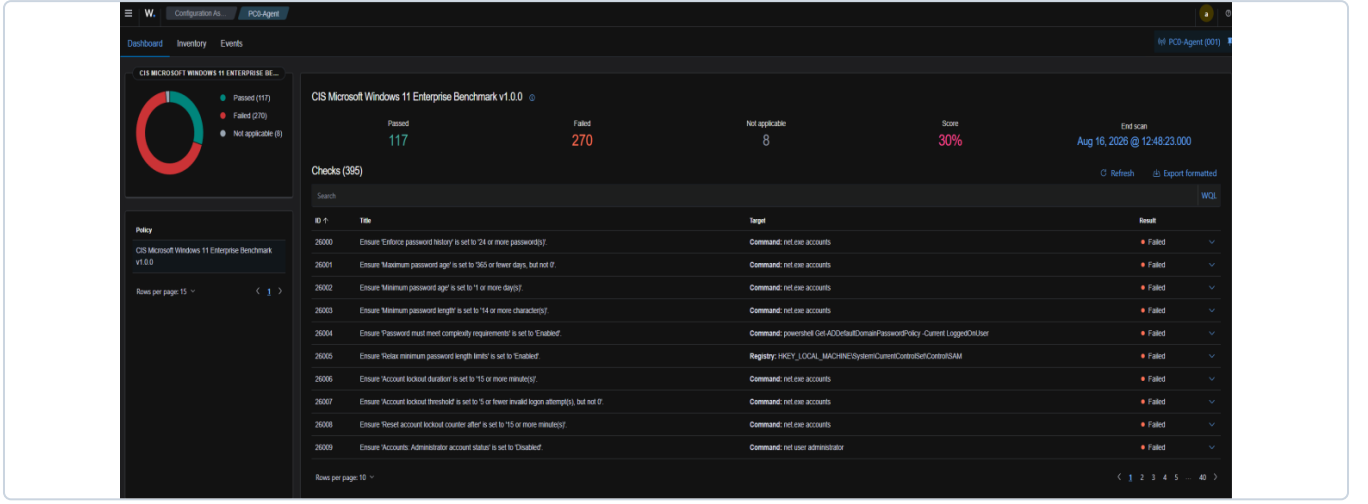
Çalışmada Wazuh'un tespit ve analiz yeteneklerini test etmek amacıyla izole bir test/analiz ortamı yapılandırılmıştır:

- **Merkezi Yönetim Katmanı (Wazuh Manager & Indexer):** Ubuntu Server üzerinde konuşlandırılmıştır. Uç noktalardan gelen telemetriyi toplar, dekode eder ve kural motorlarıyla analiz eder, OpenSearch tabanlı Indexer katmanında indeksleyerek Wazuh Dashboard üzerinden görselleştirir.
- **Uç Nokta Katmanı (Wazuh Agent):** Windows 11 Enterprise işletim sisteminde arka plan servisi olarak çalıştırılmıştır. Olay günlüklerini, dosya değişikliklerini ve sistem yapılandırmalarını gerçek zamanlı izler.
- **Haberleşme Güvenliği:** Ajan ile sunucu arasındaki tüm log ve komut trafiği TCP/1514 portu üzerinden çift taraflı TLS doğrulaması ile şifrelenmiştir.

Bölüm 4: Uygulamalı Tehdit Simülasyonu ve Olay Tespiti

4.1. Güvenlik Yapılandırma Değerlendirmesi (SCA & CIS Benchmark)

Ajan devreye alındıktan sonra sistem, **CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0** standartlarına göre otomatik bir sıkılaştırma (hardening) taraması gerçekleştirmiştir.



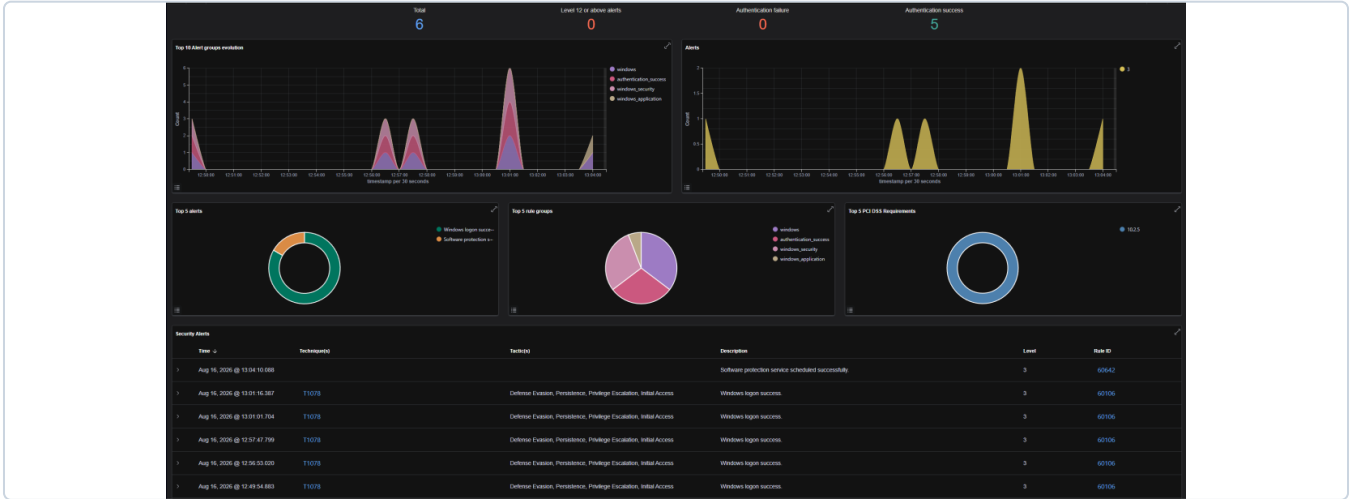
Görsel 2: Windows 11 Uç Noktası CIS Benchmark Sıkılaştırma Sonuçları (%30 Güvenlik Skoru)

SCA Bulguları ve Değerlendirme:

Taramada 117 kural başarılı (Passed), 270 kural ise başarısız (Failed) olarak işaretlenmiş ve sistem **%30 güvenlik skoru** almıştır. Başarısız kontroller incelendiğinde; parola geçmişi zorunluluğu, maksimum parola geçerlilik süresi, minimum parola uzunluğu ve hesap kilitleme eşiği gibi kritik ilkelerin işletim sisteminde varsayılan olarak tanımlanmadığı tespit edilmiştir. Wazuh, her kural için kayıt defteri (Registry) ve komut çıktılarını göstererek analiste doğrudan sıkılaştırma kılavuzu sunmuştur.

4.2. Tehdit Avcılığı ve Oturum Hareketleri Analizi

Wazuh Dashboard üzerindeki **Threat Hunting** modülü ile Windows uç noktadaki oturum açma, yetki kullanımı ve kimlik doğrulama olayları gerçek zamanlı olarak izlenmiştir.



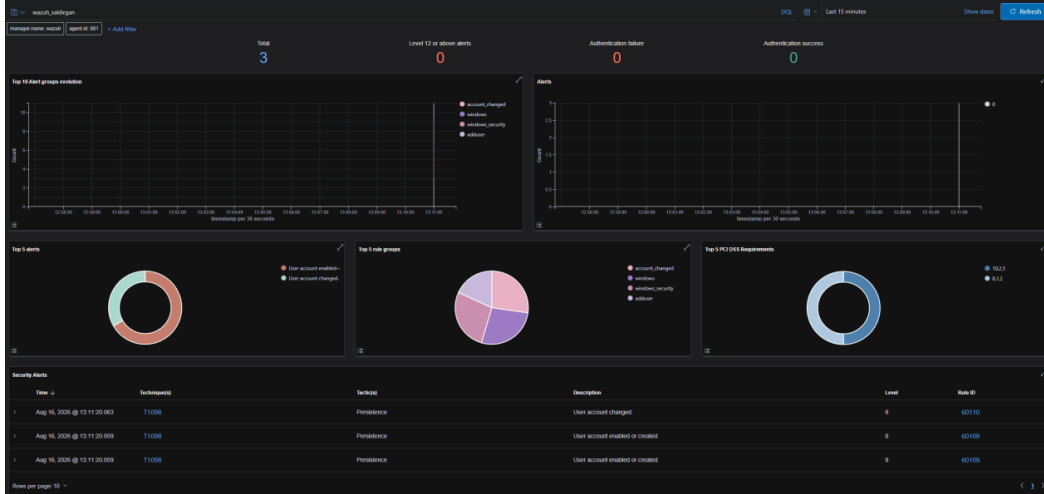
Görsel 3: Wazuh Threat Hunting Modülü - Uç Nokta Giriş Hareketleri ve MITRE ATT&CK (T1078 - Valid Accounts) Analizi

Windows Güvenlik Günlüklerinden toplanan Event ID 4624 (Başarılı Oturum Açma) ve Event ID 4672 (Özel Ayrıcalık Ataması) kayıtları; MITRE ATT&CK **T1078 (Valid Accounts)** tekniği altında korele edilmiş, kimlik doğrulama başarı/başarısızlık oranları ve ayrıcalıklı oturumlar analist ekranına anlık olarak yansıtılmıştır.

4.3. Yetkisiz Kullanıcı Açma ve Kalıcılık Tespiti (Persistence)

Saldırganların sistemde yetki elde ettikten sonra erişimlerini kaybetmemek adına başvurduğu en yaygın yöntemlerden biri yerel arka kapı hesabı oluşturmaktır. Bu senaryoyu simüle etmek amacıyla Windows uç noktasında komut satırından yetkisiz bir yerel kullanıcı oluşturulmuştur:

```
net user wazuh_saldirgan Sifre123! /add
```



Görsel 4: Yetkisiz Yerel Hesap Oluşturma Olayının (Rule ID: 60109 - Seviye 8 Alarm, MITRE T1098 Persistence) Anlık Tespiti

Olay Tespit ve Korelasyon Mekanizması:

1. Komutun çalıştırılmasıyla Windows Güvenlik Günlüğü'nde Event ID 4720 (A user account was created) kaydı üretmiştir.
2. Wazuh Ajansı bu telemetriyi yakalayarak merkezi sunucuya iletmış; Wazuh kural motoru logu **Rule ID 60109** (User account enabled or created) ve **Rule ID 60110** (User account changed) ile eşleştirmiştir.
3. Olay, **Level 8 (Yüksek Önem)** seviyesinde bir güvenlik alarmı olarak sınıflandırılmış ve MITRE ATT&CK **TA0003 (Persistence)** taktiği altındaki **T1098 (Account Manipulation)** tekniği ile otomatik olarak ilişkilendirilmiştir.

Bölüm 5: Maliyet Analizi, Çözüm Karşılaştırması ve Sonuç

Kurumsal SOC operasyonlarında platform seçimi yalnızca teknik kabiliyetlere değil, Toplam Sahip Olma Maliyeti (TCO) parametrelerine de doğrudan bağlıdır.

Özellik / Kriter	Wazuh (Açık Kaynak)	Splunk Enterprise	Microsoft Sentinel	IBM QRadar
Lisanslama Modeli	Ücretsiz / Açık Kaynak (GPLv2)	Günlük İndekslenen Veri (GB/Gün)	Alınan Veri Hacmi (GB/Gün)	Saniye Başı Olay Sayısı (EPS)
Yıllık Tahmini Maliyet (Orta Ölçek)	\$0 (Yazılım Lisansı)*	\$25.000 - \$70.000+	\$18.000 - \$50.000+	\$30.000 - \$80.000+
Uç Nokta (XDR/EDR) Desteği	Dahili ve Sınırsız Ajan Desteği	Ek Universal Forwarder / App gerekir	Defender for Endpoint (Ek Lisans)	WinCollect / Harici Entegrasyon
Sıkılaştırma (SCA / CIS)	Yerleşik, Otomatik ve Özelleştirilebilir	Ek eklentiler / Dashboard gerektirir	Defender / Azure Policy ile entegre	Ek modül / uyumluluk paketi
Kural ve Dekoder Esnekliği	Tamamen Şeffaf XML/Regex Mimarisi	SPL tabanlı / Üreticiye bağımlı	KQL tabanlı / Bulut bağımlı	AQL tabanlı / Katı kural yapısı

* Wazuh yazılım lisansı ücretsizdir; ancak sunucu donanımı, log depolama kapasitesi ve bakım/mühendislik eforu göz önünde bulundurulmalıdır.

Sonuç ve Genel Değerlendirme

Yapılan test ve analizler; açık kaynaklı Wazuh platformunun log yönetimi, uç nokta izleme (XDR), sıkılaştırma denetimi (SCA) ve tehdit avcılığı fonksiyonlarını tek bir mimaride başarıyla birleştirdiğini göstermiştir. Yetkisiz kullanıcı oluşturma testinde görüldüğü üzere sistem, Windows güvenlik olaylarını gecikmesiz yakalayarak MITRE ATT&CK matrisiyle korele edebilmektedir.

Wazuh; sıfır yazılım lisans maliyeti, veri egemenliği sağlaması ve tamamen özelleştirilebilir kural mimarisiyle özellikle KOBİ'ler ve bütçe kısıtı bulunan kurumlar için ticari çözümlere karşı güçlü, sürdürülebilir ve kurumsal seviyede bir SIEM/XDR alternatifi oluşturmaktadır.

Kaynakça

1. **Wazuh Documentation.** (2026). *Wazuh - Open Source Security Platform Architecture and Endpoint Capabilities*. <https://documentation.wazuh.com>
2. **Center for Internet Security (CIS).** (2026). *CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0*. CIS Security Standards.
3. **MITRE ATT&CK Framework.** (2026). *Technique T1098: Account Manipulation & Technique T1078: Valid Accounts*. <https://attack.mitre.org>
4. **Microsoft Learn TechDocs.** (2026). *Windows Security Log Event ID 4720 (A user account was created) & Event ID 4624 (Successful Logon)*.
5. **Gartner Research.** (2025/2026). *Magic Quadrant for Security Information and Event Management (SIEM)*.