aa teknoloji

Wazuh SIEM & XDR

Wazuh, siber güvenlik gücünü arttıran açık kaynaklı bir SIEM ve XDR platformudur. Tehditleri algılamak, uyumluluk gereksinimlerini karşılamak ve uç noktaları korumak isteyen BT ekipleri için kapsamlı bir izleme ve müdahale çözümü sunar. Wazuh Platinum Partner unvanımızla; Avrupa, Türkiye ve Orta Doğu (MEA) bölgelerinde uçtan uca teknik destek, kurulum ve yönetim hizmetleri sağlayan yetkin bir iş ortağıyız. Bölgesel uzmanlığımız ve güçlü operasyon altyapımızla, kurumların siber güvenlik altyapılarını en yüksek standartlarda destekliyoruz.

Modern Güvenlik Zorlukları

Kurumlar, dağıtık BT altyapıları üzerinde görünürlük sağlamakta ve karmaşık siber tehditleri yönetmekte zorlanmaktadır. Veri parçalanması ve manuel süreçler, tehdit tespitini geciktirirken siber güvenlik operasyonlarının verimliliğini ciddi ölçüde düşürmektedir. Güvenlik ekipleri, izole kalan log verileri ve reaktif müdahale yöntemleriyle aşırı yüklenmektedir. Dağınık yapıdaki uç noktalarda merkezi kontrol kaybı, tehditlerin tespit edilmesini ve engellenmesini güçleştirmektedir. KVKK ve ISO 27001 gibi yasal düzenlemelerin getirdiği sürekli izleme ve denetlenebilirlik baskısı, manuel yönetimi imkansız hale getirmektedir.

⚠ Hangi Sorunları Çözer?

- Dağınık BT ortamında görünürlük arayan ekipler için
- Manuel log inceleme yükü altında ezilen SOC ekipleri için
- KVKK ve GDPR uyumluluk süreçlerinde zorlanan kurumlar için
- Zafiyet tespiti ve yama yönetimini otomatize etmek isteyenler için

Temel İlkeler

Merkezi
Tüm verileri tek panelde birleştirir.

Otomatik
Tehditleri hızla ve otomatik algılar.

Bütünleşik
SIEM ve EDR yeteneklerini birleştirir.

Uyumlu
Regülasyon süreçlerine tam destek verir.

Teknik Özellikler

Bütünleşik Tehdit Algılama
- Gerçek zamanlı log korelasyonu yapar.
- Uç nokta etkinliklerini izler.
- Dosya bütünlüğü kontrolü sağlar.
- Kritik sistemleri sürekli tarar.

Uyumluluk ve Risk Yönetimi
- KVKK ve GDPR panelleri sunar.
- Sürekli denetim izleri oluşturur.
- Zafiyetleri otomatik belirler.
- Güvenlik açıklarını raporlar.

Esnek Kurulum Mimarisi
- On-premise kurulumu destekler.
- Hibrit bulut yapılarıyla uyumludur.
- İnternete kapalı ortamda çalışır.
- Yüksek erişilebilirlik sunar.

SOC Operasyon Desteği
- Windows, Linux, macOS desteği sağlar.
- SOAR platformlarıyla entegre olur.
- Merkezi ve tek panelden izler.
- Otomatik yanıt mekanizmaları sunar.

Tehdit Algılama ve Müdahale
- Dosya bütünlüğünü sürekli izler.
- Zararlı yazılımları anında tespit eder.
- Yetkisiz erişimleri engeller.
- Otomatik yanıt mekanizmaları kurar.

Wazuh Nasıl Çalışır?

Wazuh, kurumsal ortamınızdaki siber tehditleri tespit etmek, analiz etmek ve otomatize edilmiş yanıtlar üretmek için geliştirilmiş kapsamlı bir güvenlik platformudur. Sistemin çalışma mantığı, verilerin merkezi toplanmasından başlayarak, akıllı korelasyon analizi ve hızlı olay müdahalesini içeren üç aşamalı bir süreç üzerine kuruludur.

Çalışma Akışı

1. Veri Toplanması
- Uç noktalardan logları canlı toplar.
- Tüm bulut ve fiziksel veriyi işler.
- Ajanlar ile sürekli izleme sağlar.
- Farklı kaynakları tekte birleştirir.

→

2. Tehdit Analizi
- Kötü amaçlı yazılımları anında bulur.
- Sistem dosyalarını sürekli denetler.
- Yetkisiz erişim girişimlerini izler.
- Kural setleri ile anomali arar.

→

3. Yanıt ve Rapor
- Otomatik yanıt mekanizması çalıştırır.
- Yasal düzenlemelere uygun raporlar.
- Güvenlik açıklarını önceliklendirir.
- SOC panellerine anlık veri aktarır.

Sürekli İyileştirme

Wazuh, açık kaynak yapısı sayesinde ağır lisans maliyetleri olmaksızın kurumsal düzeyde güvenlik sağlar. On-premise, hibrit ve bulut ortamlarında yüksek erişilebilirlik ve kümeleme desteği ile altyapınızla birlikte büyür, operasyonel yükü azaltarak stratejik güvenlik odağınızı korumanıza yardımcı olur.

Avantajlar

Merkezi Güvenlik Görünürlüğü
Dağınık BT altyapılarındaki tüm uç noktalar, sunucular ve bulut uygulamalarından gelen verileri tek bir panelde birleştirerek izleme ve analiz süreçlerini hızlandırır.

Otomatik Tehdit Algılama
Yerleşik kural setleri ve gelişmiş tehdit istihbaratı sayesinde, kötü niyetli yazılım ve yetkisiz erişim girişimlerini anlık tespit ederek SOC ekiplerinin yükünü azaltır.

Dosya Bütünlüğü İzleme (FIM)
Kritik sistem dosyalarında ve kayıt defterlerinde yapılan tüm değişiklikleri sürekli takip ederek, rootkit faaliyetlerini ve yetkisiz müdahaleleri anında ortaya çıkarır.

Otomatik Uyumluluk Denetimi
KVKK, GDPR, PCI-DSS ve ISO 27001 gibi standartlar için önceden tanımlanmış paneller ve otomatik raporlama araçları ile yasal denetim süreçlerini kolaylaştırır.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.