Wazuh Agent

Wazuh aracısı Linux, Windows, macOS, Solaris, AIX ve diğer işletim sistemlerinde çalışır. Dizüstü bilgisayarlara, masaüstü bilgisayarlara, sunuculara, bulut örneklerine, kapsayıcılara veya sanal makinelere dağıtılabilir. Aracı, tehdit önleme, algılama ve yanıt yetenekleri sağlayarak sisteminizi korumaya yardımcı olur. Ayrıca, şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla Wazuh sunucusuna ilettiği farklı türdeki sistem ve uygulama verilerini toplamak için kullanılır .

Aracı Mimarisi

Wazuh aracısı modüler bir mimariye sahiptir. Her bileşen, dosya sistemini izleme, günlük mesajlarını okuma, envanter verilerini toplama, sistem yapılandırmasını tarama ve kötü amaçlı yazılım arama gibi kendi görevlerinden sorumludur. Kullanıcılar, aracı modüllerini yapılandırma ayarları aracılığıyla yönetebilir ve çözümü kendi özel kullanım durumlarına uyarlayabilir.

Aşağıdaki diyagram, aracı mimarisini ve bileşenlerini göstermektedir:



Aracı mimarisi

Ajan Modülleri

Tüm aracı modülleri yapılandırılabilir ve farklı güvenlik görevleri gerçekleştirir. Bu modüler mimari, her bileşeni güvenlik ihtiyaçlarınıza göre etkinleştirmenize veya devre dışı bırakmanıza olanak tanır. Aşağıda tüm aracı modüllerinin farklı amaçları hakkında bilgi edinebilirsiniz.

- **Günlük toplayıcı:** Bu aracı bileşeni, işletim sistemi ve uygulama günlük mesajlarını toplayarak düz günlük dosyalarını ve Windows olaylarını okuyabilir. Windows olayları için XPath filtrelerini destekler ve Linux Denetim günlükleri gibi çok satırlı biçimleri tanır. Ayrıca JSON olaylarını ek meta verilerle zenginleştirebilir.
- **Komut yürütme:** Aracılar, yetkili komutları periyodik olarak çalıştırır, çıktılarını toplar ve daha fazla analiz için Wazuh sunucusuna geri bildirir. Bu modülü, kalan sabit disk alanını izlemek veya son oturum açan kullanıcıların listesini almak gibi farklı amaçlar için kullanabilirsiniz.
- **Dosya bütünlüğü izleme (FIM):** Bu modül, dosyalar oluşturulduğunda, silindiğinde veya değiştirildiğinde raporlama yaparak dosya sistemini izler. Dosya özniteliklerindeki, izinlerdeki, sahiplikteki ve içerikteki değişiklikleri takip eder. Bir olay meydana geldiğinde, gerçek zamanlı olarak kim, ne ve ne zaman ayrıntılarını yakalar. Ayrıca, FIM modülü izlenen dosyaların durumuyla bir veritabanı oluşturur ve korur ve sorguların uzaktan çalıştırılmasına olanak tanır.
- **Güvenlik yapılandırması değerlendirmesi (SCA):** Bu bileşen, İnternet Güvenliği Merkezi (CIS) kıyaslamalarına dayalı olarak kullanıma hazır kontrolleri kullanarak sürekli

yapılandırma değerlendirmesi sağlar. Kullanıcılar ayrıca güvenlik politikalarını izlemek ve uygulamak için kendi SCA kontrollerini oluşturabilirler.
- **Sistem envanteri:** Bu aracı modülü, işletim sistemi sürümü, ağ arayüzleri, çalışan işlemler, yüklü uygulamalar ve açık portların listesi gibi envanter verilerini toplayarak periyodik olarak taramalar çalıştırır. Tarama sonuçları, uzaktan sorgulanabilen yerel SQLite veritabanlarında saklanır.
- **Kötü amaçlı yazılım tespiti:** İmza tabanlı olmayan bir yaklaşım kullanarak, bu bileşen anormallikleri ve olası kök araç takımlarının varlığını tespit edebilir. Ayrıca, sistem çağrılarını izlerken gizli süreçleri, gizli dosyaları ve gizli bağlantı noktalarını arar.
- **Active Response:** Bu modül, tehditler algılandığında otomatik eylemler çalıştırır ve bir ağ bağlantısını engellemek, çalışan bir işlemi durdurmak veya kötü amaçlı bir dosyayı silmek için yanıtları tetikler. Kullanıcılar ayrıca gerektiğinde özel yanıtlar oluşturabilir ve örneğin bir ikili dosyayı bir sanal alanda çalıştırmak, ağ trafiğini yakalamak ve bir dosyayı bir antivirüsle taramak için yanıtları özelleştirebilir.
- **Konteyner güvenlik izleme:** Bu aracı modülü, konteynerleştirilmiş bir ortamda değişiklikleri izlemek için Docker Engine API ile entegre edilmiştir. Örneğin, konteyner görüntülerinde, ağ yapılandırmasında veya veri birimlerinde değişiklikleri algılar. Ayrıca, ayrıcalıklı modda çalışan konteynerler ve çalışan bir konteynerde komutları yürüten kullanıcılar hakkında uyarılar verir.
- **Bulut güvenliği izleme:** Bu bileşen, Amazon Web Services, Microsoft Azure veya Google GCP gibi bulut sağlayıcılarını izler. API'leriyle yerel olarak iletişim kurar. Bulut altyapısındaki değişiklikleri (örneğin, yeni bir kullanıcı oluşturulur, bir güvenlik grubu değiştirilir, bir bulut örneği durdurulur, vb.) tespit edebilir ve bulut hizmetleri günlük verilerini (örneğin, AWS Cloudtrail, AWS Macie, AWS GuardDuty, Azure Active Directory, vb.) toplayabilir.

Wazuh Sunucusuyla İletişim

Wazuh aracısı, toplanan verileri ve güvenlikle ilgili olayları iletmek için Wazuh sunucusuyla iletişim kurar . Ayrıca, aracı operasyonel verileri göndererek yapılandırmasını ve durumunu bildirir. Bağlandıktan sonra, aracı Wazuh sunucusundan uzaktan yükseltilebilir, izlenebilir ve yapılandırılabilir.

Aracının sunucuyla iletişimi güvenli bir kanal (TCP veya UDP) üzerinden gerçekleşir ve gerçek zamanlı olarak veri şifrelemesi ve sıkıştırması sağlar. Ek olarak, taşmayı önlemek, gerektiğinde olayları sıraya koymak ve ağ bant genişliğini korumak için akış kontrol mekanizmaları içerir.

Aracı ilk kez sunucuya bağlamadan önce kaydetmeniz gerekir. Bu işlem, aracıya kimlik doğrulama ve veri şifrelemesi için kullanılan benzersiz bir anahtar sağlar.

Revision #2
Created 6 December 2023 17:33:27 by LastGuard
Updated 11 December 2024 16:04:11 by Ayşegül Sarıkaya