Wazuh Server

Wazuh sunucu bileşeni, ajanlardan alınan verileri analiz ederek tehditler veya anormallikler algılandığında uyarıları tetikler. Ayrıca, ajan yapılandırmasını uzaktan yönetmek ve durumlarını izlemek için kullanılır.

Wazuh sunucusu, algılama yeteneklerini geliştirmek için tehdit istihbarat kaynaklarını kullanır. Ayrıca, MITRE ATT&CK çerçevesini ve PCI DSS, GDPR, HIPAA, CIS ve NIST 800-53 gibi düzenleyici uyumluluk gereksinimlerini kullanarak uyarı verilerini zenginleştirir ve güvenlik analitiği için yararlı bir bağlam sağlar.

Ek olarak, Wazuh sunucusu ServiceNow , Jira ve PagerDuty gibi bilet sistemleri ve Slack gibi anlık mesajlaşma platformları dahil olmak üzere harici yazılımlarla entegre edilebilir . Bu entegrasyonlar güvenlik operasyonlarını kolaylaştırmak için uygundur.

Sunucu Mimarisi

Wazuh sunucusu analiz motorunu, Wazuh RESTful API'sini, aracı kayıt hizmetini, aracı bağlantı hizmetini, Wazuh küme arka plan programını ve Filebeat'i çalıştırır. Sunucu bir Linux işletim sistemine kurulur ve genellikle bağımsız bir fiziksel makinede, sanal makinede, docker konteynerinde veya bulut örneğinde çalışır.

Aşağıdaki diyagram sunucu mimarisini ve bileşenlerini göstermektedir:

Wazuh sunucu mimarisi
Image not found or type unknown

Sunucu Bileşenleri

Wazuh sunucusu, yeni aracıları kaydetme, her bir aracının kimliğini doğrulama ve Wazuh aracısı ile Wazuh sunucusu arasındaki iletişimi şifreleme gibi farklı işlevlere sahip aşağıda listelenen birkaç bileşenden oluşur.

- **Aracı kayıt hizmeti:** Yeni aracıları kaydetmek için kullanılır. Bu hizmet her aracıya benzersiz kimlik doğrulama anahtarları sağlar ve dağıtır. İşlem bir ağ hizmeti olarak çalışır ve TLS/SSL sertifikaları aracılığıyla veya sabit bir parola sağlayarak kimlik doğrulamayı destekler.
- **Aracı bağlantı hizmeti:** Bu hizmet aracılardan veri alır. Her aracı kimliğini doğrulamak ve Wazuh aracısı ile Wazuh sunucusu arasındaki iletişimleri şifrelemek için kayıt hizmeti tarafından paylaşılan anahtarları kullanır. Ayrıca, bu hizmet merkezi yapılandırma yönetimi sağlayarak yeni aracı ayarlarını uzaktan göndermenize olanak tanır.

- **Analiz motoru:** Bu, veri analizini gerçekleştiren sunucu bileşenidir. İşlenen bilgi türünü (Windows olayları, SSH günlükleri, web sunucusu günlükleri ve diğerleri) belirlemek için kod çözücüleri kullanır. Bu kod çözücüler ayrıca günlük iletilerinden kaynak IP adresi, olay kimliği veya kullanıcı adı gibi ilgili veri öğelerini çıkarır. Daha sonra, motor kuralları kullanarak, uyarıları tetikleyebilecek ve hatta otomatik karşı önlemler (örneğin, bir IP adresini yasaklama, çalışan bir işlemi durdurma veya kötü amaçlı yazılım eserini kaldırma) gerektirebilecek kod çözülmüş olaylardaki belirli kalıpları belirler.
- **Wazuh RESTful API:** Bu hizmet, Wazuh altyapısıyla etkileşim kurmak için bir arayüz sağlar. Aracıların ve sunucuların yapılandırma ayarlarını yönetmek, altyapı durumunu ve genel sağlığı izlemek, Wazuh kod çözücülerini ve kurallarını yönetmek ve düzenlemek ve izlenen uç noktaların durumu hakkında sorgulama yapmak için kullanılır. Wazuh panosu da bunu kullanır.
- **Wazuh küme arka planı:** Bu hizmet, Wazuh sunucularını yatay olarak ölçeklendirmek ve bunları bir küme olarak dağıtmak için kullanılır. Bu tür bir yapılandırma, bir ağ yük dengeleyicisiyle birleştirildiğinde yüksek kullanılabilirlik ve yük dengeleme sağlar. Wazuh küme arka planı, Wazuh sunucularının birbirleriyle iletişim kurmak ve senkronize kalmak için kullandıkları şeydir.
- **Filebeat:** Wazuh dizinleyicisine olayları ve uyarıları göndermek için kullanılır. Wazuh analiz motorunun çıktısını okur ve olayları gerçek zamanlı olarak gönderir. Ayrıca, çok düğümlü bir Wazuh dizinleyici kümesine bağlandığında yük dengelemesi sağlar.

Revision #4
Created 6 December 2023 17:33:08 by LastGuard
Updated 11 December 2024 16:04:37 by Ayşegül Sarıkaya