İzleme Örnekleri

Wazuh aracısı platformlar arası uyumludur, yani Windows, Linux, Solaris, BSD ve macOS dahil olmak üzere çeşitli işletim sistemlerinde çalışabilir. Farklı sistemler ve uygulamalar hakkında veri toplar ve örneğin Dosya Bütünlüğü İzleme (FIM) ve Güvenlik Yapılandırma Değerlendirmesi (SCA) gibi diğer Wazuh yeteneklerinden yararlanmasını sağlar. Bu veriler şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla Wazuh sunucusuna gönderilir. Benzersiz önceden paylaşılmış anahtar kayıt işlemi bu güvenli kanalı oluşturur.

Microsoft Azure ortamınızdaki sanal makinelere Wazuh aracısını yükleyebilirsiniz. Wazuh aracısını kullanarak bulut sanal makinelerini izlemek faydalıdır çünkü kapsamlı güvenlik ve performans denetimi sağlayarak dinamik bulut ortamlarında olası tehditlerin ve operasyonel sorunların erken tespitini sağlar.

Wazuh aracıları hakkında daha fazla bilgi edinmek için Wazuh agent kurulum ve kayıt belgelerini inceleyin . Ayrıca, Wazuh SIEM ve XDR yetenekleri ve bunların yapılandırması hakkında yetenekler belgelerimizde okuyun.

Revision #1
Created 30 December 2024 16:17:14 by Ayşegül Sarıkaya
Updated 30 December 2024 16:19:30 by Ayşegül Sarıkaya