Amazon Web Hizmetlerini (AWS) İzleme

Amazon Web Services (AWS), Amazon tarafından sağlanan yaygın olarak kullanılan bir bulut bilişim platformudur. İşlem gücü, depolama, veritabanları, makine öğrenimi, analiz, güvenlik ve daha fazlası dahil olmak üzere geniş bir hizmet yelpazesi sunar. AWS, bireylerin, işletmelerin ve kuruluşların fiziksel altyapıya yatırım yapma ve bakımını yapma ihtiyacı olmadan işlem kaynaklarına erişmesini ve bunları kullanmasını sağlar. Açık kaynaklı bir güvenlik platformu olan Wazuh, AWS altyapınızın güvenliğini izlemek ve iyileştirmek için kapsamlı bir özellik paketi sunar. EC2 örneklerinize Wazuh aracıları yükleyebilir veya AWS için Wazuh modülünü desteklenen AWS hizmetleriyle entegre edebilirsiniz. Bu, olayları analiz etmenizi ve AWS altyapınızdaki anormallikler için neredeyse gerçek zamanlı uyarılar almanızı sağlar. Aşağıdaki bölümlerde AWS altyapınızı nasıl izleyeceğinizi öğrenebilirsiniz:

- AWS Örneklerini İzleme
- AWS Tabanlı Hizmetlerin İzlenmesi

AWS Örneklerini İzleme

AWS EC2 örneklerinize Wazuh aracısını yükleyerek bu örneklerdeki içgörüler elde edebilir ve etkinlikleri izleyebilirsiniz.

Wazuh aracısı bir EC2 örneğinde hizmet olarak çalışır ve şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla sistem, güvenlik ve uygulama verilerini toplar ve Wazuh sunucusuna iletir.

AWS Tabanlı Hizmetlerin İzlenmesi

AWS için Wazuh modülü, bu hizmetlerin günlüklerini toplayarak ve günlükleri Wazuh kural setiyle analiz ederek çeşitli AWS hizmetlerinin izlenmesini sağlar. Bu, Wazuh'un EC2 örneği yapılandırmasına, kullanıcıların ve sistemlerin yetkisiz davranışlarına, S3'te depolanan verilere ve daha fazlasına dayalı uyarıları tetiklemesini sağlar. Böylece AWS altyapısı içindeki etkinlikler hakkında ayrıntılı bilgi sağlanır.

Aşağıdaki her bölüm, desteklenen tüm AWS hizmetlerini yapılandırmak ve kurmak için ayrıntılı talimatlar ve ayrıca bu hizmetlerden günlükleri toplamak için gereken Wazuh yapılandırmasını içerir. Ayrıca karşılaşabileceğiniz yaygın sorunları çözmek için adımlar da içerir.