Bulut Altyapı Koruması

Wazuh güvenlik platformu, şirket içi, bulut ve hibrit ortamlar için tehdit algılama, yapılandırma uyumluluğu ve sürekli izleme sağlar. Altyapıyı iki düzeyde izleyerek bulut iş yüklerini korur:

- **Uç nokta düzeyi :** Hafif Wazuh aracısını kullanarak bulut örneklerini veya sanal makineleri izleme .
- **Bulut altyapısı düzeyi** : sağlayıcı API'sinden veri toplayıp analiz ederek bulut hizmeti etkinliğini izleme. Wazuh, Amazon AWS, Microsoft Azure ve Google Cloud'u destekler.

Güvenlik operasyonlarını geliştirmek, bulut tabanlı uygulamaları korumak ve güvenli bir bulut ortamı için uyumluluk çabalarını kolaylaştırmak amacıyla Wazuh'un kullanılmasının bazı avantajlarını açıklıyoruz.

Bulut Günlük Veri Analizi ve Saklama

Bulut ortamları, güvenlik olaylarını tanımlamak için hayati önem taşıyan büyük miktarda günlük verisi üretir. Wazuh kuralları ve kod çözücüleri, anormal olayları tespit etmek için günlük verilerini ayrıştırmaktan ve analiz etmekten sorumludur. Wazuh, AWS, Azure, Google Cloud, Office 365 ve GitHub gibi çeşitli bulut platformlarından ve hizmetlerinden günlük verilerini toplar ve analiz eder.

Aşağıdaki görsel, bulut altyapısından toplanan olayların eğilimini gösteren Wazuh'taki bir AWS panosunun örneğidir.

Wazuh'taki AWS panosu

Wazuh, buluttaki etkinlikleri izler ve kaydeder ve tüm bulut altyapısındaki kullanıcı eylemlerinin merkezi bir görünümünü sağlar. Wazuh, şüpheli veya yetkisiz etkinlikleri tespit etmek için kullanıma hazır kurallara sahiptir. Kullanıcılar, yerleşik kurallara ek olarak tehdit tespitini birleştirmek için özel kurallar oluşturabilir .

Amazon Web Servisleri

Wazuh, AWS bulut altyapısını izlemek ve güvence altına almak için özel modüllere sahiptir . Wazuh'un izlediği AWS hizmetlerinden bazıları şunlardır:

- **Amazon Guardduty,** kötü amaçlı faaliyetleri ve yetkisiz davranışları sürekli olarak izleyen ve AWS hesaplarının, iş yüklerinin ve Amazon S3'te depolanan verilerin korunmasını sağlayan bir tehdit algılama hizmetidir.
- **Amazon Inspector,** AWS'de dağıtılan uygulamaların güvenliğini ve uyumluluğunu iyileştirmeye yardımcı olan otomatik bir güvenlik değerlendirme hizmetidir.
- **Amazon Key Management Service (KMS),** AWS servisleri genelinde şifreleme anahtarı yönetimi için kullanılır.
- **Amazon Macie,** tamamen yönetilen bir veri güvenliği ve gizlilik hizmetidir. Şifrelenmemiş S3 kovalarını, herkese açık kovaları ve harici AWS hesaplarıyla paylaşılan kovaları otomatik olarak algılar.
- **Amazon Sanal Özel Bulut (VPC),** AWS kaynaklarının kullanıcı tarafından tanımlanan sanal bir ağ üzerinde başlatılabileceği AWS Bulutunun mantıksal olarak izole edilmiş bir bölümünü sağlar.
- **AWS Config,** AWS kaynaklarınızın yapılandırmalarını değerlendirir, denetler ve değerlendirir. Kullanıcıların AWS kaynakları arasındaki yapılandırmalardaki değişiklikleri ve ilişkileri incelemesine yardımcı olur.
- **AWS Cloudtrail** , AWS hesabınızın yönetimini, uyumluluğunu, operasyonel denetimini ve risk denetimini sağlar. CloudTrail ile AWS altyapınızdaki eylemlerle ilgili hesap etkinliğini kaydedebilir, sürekli olarak izleyebilir ve saklayabilirsiniz.
- **AWS Trusted Advisor,** kullanıcıların AWS ortamlarını optimize ederek maliyetleri düşürmelerine, performansı artırmalarına ve güvenliği iyileştirmelerine yardımcı olur. Kullanıcıların kaynaklarını AWS en iyi uygulamalarını izleyerek sağlamalarına yardımcı olmak için gerçek zamanlı rehberlik sağlar.
- **AWS Web Uygulama Güvenlik Duvarı (WAF),** web uygulamalarınızı veya API'lerinizi, kullanılabilirliği etkileyebilecek, güvenliği tehlikeye atabilecek veya aşırı kaynak tüketebilecek yaygın web saldırılarına karşı korumaya yardımcı olur.

Microsoft Azure

Wazuh, Azure platformundan günlükleri çeken ve izleyen özel bir modüle sahiptir . Bu modül, aşağıdakiler de dahil olmak üzere kritik Azure hizmetlerinden veri alır:

- **Log Analytics API** : Log Analytics API, Azure Monitor hizmetinin temel bir bileşenidir ve günlük verilerini toplamak ve analiz etmek için kullanılır. Bu tür verilerin kaynakları bulut uygulamaları, işletim sistemleri ve Azure kaynaklarıdır. Azure için Wazuh modülü, Log Analytics API'sini sorgulayabilir ve Azure Monitor hizmeti tarafından toplanan günlükleri

çekebilir.

- **Blob Storage API** : Azure hizmetlerinden gelen günlükler isteğe bağlı olarak Azure Blob Storage'a gönderilir. Özellikle, bir Azure hizmetini günlükleri bu amaçla oluşturulmuş bir depolama hesabındaki bir kapsayıcıya aktaracak şekilde yapılandırmak mümkündür. Daha sonra, Wazuh aracısı bu günlükleri Blob Storage API ile entegrasyonu aracılığıyla indirecektir.
- **Active Directory Graph API** : Azure Active Directory (AD) Graph API, REST API uç noktaları aracılığıyla AZURE AD'ye erişim sağlar. Wazuh tarafından Active Directory olaylarını izlemek için kullanılır (örneğin, yeni bir kullanıcı oluşturma, kullanıcı özelliklerini güncelleme, kullanıcı hesaplarının devre dışı bırakılması, vb.)

Google Bulut Platformu

Wazuh, olay alımı ve dağıtımı için bir ara yazılım olan Google Pub/Sub mesajlaşma hizmetinden olayları çekerek Google Cloud hizmetlerini izler. Bu entegrasyon, Google Cloud varlıklarınızı hedef alan tehditleri tespit etmeye yardımcı olur. Daha fazla bilgi için lütfen GCP hizmetlerini izlemek için Wazuh'u kullanma bölümüne bakın .

Office 365

Wazuh, Office 365 Yönetim Etkinliği API'siyle etkileşim kurmak üzere tasarlanmış özel bir modül içerir. Bu modül, Office 365'ten günlükleri almak ve bunları Wazuh platformu içinde analiz için kullanılabilir hale getirmekten sorumludur. Yönetim Etkinliği API'si, Office 365 için denetim günlüklerinin kaynağı olarak hizmet eder ve Office 365 ortamındaki çeşitli eylemler ve olaylar hakkında bilgi içerir. Bu günlükler, kiracıya özgü içerik blob'ları halinde düzenlenir ve içerik türlerine ve kaynaklarına göre sınıflandırılır. Wazuh, bu günlükler üzerinde analiz, uyarı ve raporlama gerçekleştirerek Office 365 ortamındaki güvenlik ve uyumluluk izleme yeteneklerini geliştirir. Daha ayrıntılı bilgi için lütfen Office 365'i izlemek için Wazuh'u kullanma bölümüne bakın .

GitHub

Wazuh, GitHub API'sini kullanarak kuruluş üyeleri tarafından gerçekleştirilen eylemler hakkında bilgi içeren GitHub denetim günlüklerini çeken bir GitHub modülüne sahiptir. Bu günlük, eylemi başlatan kullanıcı, eylemin niteliği (örneğin, depo oluşturma, erişim değişiklikleri, vb.), eylemin ne zaman gerçekleştiğini gösteren zaman damgası ve diğerleri gibi temel ayrıntıları içerir. Wazuh bu günlükleri toplar, işler ve depolar, analiz, uyarı ve raporlamayı mümkün kılar. Daha fazla bilgi için GitHub'ı izlemek için Wazuh'u kullanma konusuna bakın.

Bulut Tabanlı Uygulamaları Koruyun

Wazuh, bulut tabanlı uygulamalar için güvenlik tehditlerine ve güvenlik açıklarına karşı koruma sağlayarak koruma sağlar. Kubernetes ve Docker gibi konteyner düzenleme platformlarıyla entegre olur ve konteyner etkinliğini gerçek zamanlı olarak izlemesine ve analiz etmesine olanak tanır. Wazuh, şüpheli konteyner davranışlarını, yetkisiz görüntü değişikliklerini ve olası güvenlik yanlış yapılandırmalarını tespit ederek konteynerleştirilmiş uygulamaların genel bütünlüğünü garanti eder.

Aşağıdaki görüntü izlenen bir Docker altyapısından üretilen uyarıları göstermektedir.

Docker altyapı uyarıları

Image not found or type unknown

Bulutta Güvenlik Operasyonlarını Destekleyin

Wazuh, güvenlik ekiplerinin tehditleri tespit edip yanıtlamalarına, hasarları azaltmalarına ve bulut altyapısı üzerindeki genel etkiyi azaltmalarına olanak tanıyarak bulut ortamlarındaki güvenlik operasyonlarını teşvik eder. Ayrıca Wazuh, kırmızı ve mavi takım faaliyetlerini kolaylaştırır. Platformun özelleştirilebilir kuralları, kuruluşların saldırıları simüle etmelerini ve güvenlik savunmalarını test etmelerini sağlar. Mavi takımlar, kırmızı takım faaliyetlerinden Wazuh'ta elde edilen içgörüleri güvenlik önlemlerini ince ayarlamak ve savunmalarını güçlendirmek için kullanabilir.

Tespit sonuçları

Image not found or type unknown

Wazuh'un merkezi günlük kaydı ve raporlama yetenekleri, bulut ortamlarında uyumluluk yönetimini basitleştirir. Denetim izlerini yakalayıp depolayarak, hesap verebilirliği sağlayarak ve güvenlik olaylarının araştırılmasını kolaylaştırarak kuruluşların düzenleyici gereklilikleri karşılamalarına yardımcı olur. Wazuh'un analiz, raporlama ve uyumluluk çabalarına nasıl yardımcı olduğu hakkında daha fazla bilgi için Wazuh dashboard belgelerine bakın.

Revision #4
Created 6 December 2023 18:05:11 by LastGuard
Updated 23 December 2024 19:44:38 by Ayşegül Sarıkaya