

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

ekebilir.

- **Blob Storage API** : Azure hizmetlerinden gelen gnlkler isteęe baęlı olarak Azure Blob Storage'a gnderilir.  zellikle, bir Azure hizmetini gnlkleri bu amala oluřturulmuř bir depolama hesabındaki bir kapsayıcıya aktaracak řekilde yapılandırmak mmkndr. Daha sonra, Wazuh aracı bu gnlkleri Blob Storage API ile entegrasyonu aracılıęıyla indirecektir.
- **Active Directory Graph API** : Azure Active Directory (AD) Graph API, REST API u noktaları aracılıęıyla AZURE AD'ye eriřim saęlar. Wazuh tarafından Active Directory olaylarını izlemek iin kullanılır (rneęin, yeni bir kullanıcı oluřturma, kullanıcı  zelliklerini gncelleme, kullanıcı hesaplarının devre dıřı bırakılması, vb.)

Google Bulut Platformu

Wazuh, olay alımı ve daęıtımı iin bir ara yazılım olan Google Pub/Sub mesajlařma hizmetinden olayları ekerek Google Cloud hizmetlerini izler. Bu entegrasyon, Google Cloud varlıklarınızı hedef alan tehditleri tespit etmeye yardımcı olur. Daha fazla bilgi iin ltfen [GCP hizmetlerini izlemek iin Wazuh'u kullanma](#) blmne bakın .

Office 365

Wazuh, Office 365 Ynetim Etkinlięi API'siyle etkileřim kurmak zere tasarlanmış  zel bir modl ierir. Bu modl, Office 365'ten gnlkleri almak ve bunları Wazuh platformu iinde analiz iin kullanılabilir hale getirmekten sorumludur. Ynetim Etkinlięi API'si, Office 365 iin denetim gnlklerinin kaynaęı olarak hizmet eder ve Office 365 ortamındaki eřitli eylemler ve olaylar hakkında bilgi ierir. Bu gnlkler, kiracıya  zg ierik blob'ları halinde dzenlenir ve ierik trlerine ve kaynaklarına gre sınıflandırılır. Wazuh, bu gnlkler zerinde analiz, uyarı ve raporlama gerekleřtirerek Office 365 ortamındaki gvenlik ve uyumluluk izleme yeteneklerini geliřtirir. Daha ayrıntılı bilgi iin ltfen [Office 365'i izlemek iin Wazuh'u kullanma](#) blmne bakın .

GitHub

Wazuh, GitHub API'sini kullanarak kuruluř yeleri tarafından gerekleřtirilen eylemler hakkında bilgi ieren GitHub denetim gnlklerini eken bir GitHub modlne sahiptir. Bu gnlk, eylemi bařlatan kullanıcı, eylemin nitelięi (rneęin, depo oluřturma, eriřim deęiřiklikleri, vb.), eylemin ne zaman gerekleřtięini gsteren zaman damgası ve dięerleri gibi temel ayrıntıları ierir. Wazuh bu gnlkleri toplar, iřler ve depolar, analiz, uyarı ve raporlamayı mmkn kılar. Daha fazla bilgi iin [GitHub'ı izlemek iin 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

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 içgörülerini güvenlik önlemlerini ince ayarlamak ve savunmalarını güçlendirmek için kullanabilir.

Tespit sonuçları

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.