Konteyner Güvenliği

Konteyner güvenliği, konteynerleri ve uygulamalarını güvenlik tehditlerine karşı korumaya odaklanan bir BT uygulamasıdır. Kuruluşlar, böyle bir ortamda sağlam güvenlik önlemleri uygulayarak hem konteynerlerin hem de içerdikleri uygulamaların kullanımına ilişkin görünürlük elde edebilirler.

Konteynerler, uygulama kodu, çalışma zamanı ve bağımlılıklarla hafif, izole ortamlar sunar. Hem şirket içinde hem de bulutta uygulamaları dağıtmak ve ölçeklendirmek için yaygın olarak kullanılırlar. Konteyner uygulamaları ve altyapı daha popüler hale geldikçe, bunları olası tehditlerden korumak önemli hale gelir.

Konteyner güvenliği için Wazuh

Wazuh, Docker ve Kubernetes gibi konteyner platformlarıyla entegre olur ve konteyner çalışma zamanı olaylarını, uygulama günlüklerini ve genel konteyner sağlığını etkin bir şekilde izler. Wazuh, konteyner günlüklerini önceden tanımlanmış kurallara göre değerlendirerek anormallikleri belirler. Ayrıca, konteynerleştirilmiş bir ortamda yetkisiz etkinlikleri tespit etmek için konteyner motoru eylemlerinin bir kaydını tutar. Ayrıca, bir kuruluşta performans darboğazlarını önlemek için sağlık ölçümlerini de izler.

Wazuh konteyner güvenlik özellikleri, konteyner çalışma zamanlarını izleme, konteynerleştirilmiş uygulama günlüklerini takip etme, konteyner kaynak kullanımını izleme, merkezi günlük kaydı ve konteyner uyarı bildirimlerini içerir. Bu kapsamlı yetenekler seti güvenliği artırır ve olay yanıtını kolaylaştırır.

Konteyner çalışma zamanı izleme

Kuruluşlar, konteyner olaylarını izleyerek konteynerleştirilmiş uygulamalarının güvenliğini artırabilir. Önceden tanımlanmış kurallar tarafından tetiklenen uyarılara derhal yanıt vererek beklenmeyen davranışları proaktif bir şekilde ele alabilirler. Wazuh ayrıca konteyner motoru etkileşimlerine ilişkin içgörü sağlar ve konteynerleştirilmiş uygulamalardaki düzensizlikleri tespit eder.

Konteyner motorunun izlenmesi

Wazuh, Docker dinleyici modülü aracılığıyla Docker motoru tarafından gerçekleştirilen gerçek zamanlı olayları yakalar . Bu, hiçbir önemli Docker olayının veya işleminin algılanmadan kalmamasını sağlar.

Kullanıcının Docker kaynaklarıyla etkileşiminin izlenmesi, Wazuh'un konteyner motorunun konteynerler ve görüntülerle etkileşimlerine ilişkin görünürlüğü nasıl artırdığını göstermektedir.



Docker konteyner kullanıcı etkileşimi uyarıları

Wazuh ayrıca yetkisiz eylemleri ve olası güvenlik ihlallerini belirlemeye yardımcı olmak için Kubernetes kümelerindeki kaynakların oluşturulmasını ve yok edilmesini de izliyor.

Wazuh ile Kubernetes Denetleme blog yazısı, Kubernetes kaynak etkileşimlerinin Wazuh ile nasıl izleneceğini göstermektedir.



Kubernetes kaynak etkileşim uyarıları

Konteynerleştirilmiş uygulama günlüklerinin izlenmesi

Wazuh, kuruluşların konteynerize edilmiş uygulamaları izlemesine olanak tanır. Konteynerde bulunan uygulamalara görünürlük sağlar. Uygulama olayları Wazuh yöneticisine iletildiğinde, Güvenlik mühendisleri kuruluşlarının benzersiz gereksinimleriyle uyumlu özel kurallar oluşturabilir. Bu, konteynerlere ve barındırdıkları uygulamalara genel görünürlüğü artıran oldukça kişiselleştirilmiş bir yaklaşımı kolaylaştırır.

Konteyner çalışma zamanını izleme belgeleri, konteynerleştirilmiş uygulama günlüklerinin izlenmesi hakkında daha fazla bilgi içerir.



Konteynerleştirilmiş uygulama günlüklerinin izlenmesi

Wazuh ile konteyner kaynak kullanımını izleyin

Wazuh, konteynerleştirilmiş uygulamaların kaynak tüketimini izler ve analiz eder. Konteynerlerin CPU, bellek ve ağ kullanım istatistiklerine ilişkin içgörüler sağlayarak performans darboğazlarının belirlenmesine yardımcı olur.

Wazuh, kuruluşların alışılmadık kaynak artışlarını veya tüketim modellerini tespit edip proaktif bir şekilde yanıt vermesini sağlayan özelleştirilebilir uyarılar ve bildirimler sunar.

Wazuh ile Docker konteyner güvenliği izleme hakkındaki blog yazısı, Wazuh'un konteynerleştirilmiş bir ortamda ağ kullanımını nasıl izlediğini göstermektedir.



Konteynerleştirilmiş bir ortamda ağ kullanımının izlenmesi

Konteyner olaylarının merkezi olarak kaydedilmesi ve görselleştirilmesi

Wazuh, konteyner olay günlüğü tutma ve görselleştirmeyi merkezileştirir. Ölçeklenebilir dizinleyicisi, günlükleri güçlü bir arama ve analiz motorunda toplayarak gerçek zamanlı içgörüler sağlar. Bu dizinleyici, olay akışını yönetirken günlük tutma politikaları gibi uyumluluk ihtiyaçlarını da destekler.

Wazuh, kuruluşların konteyner günlüklerini özelleştirilmiş bir panodan görüntülemesini sağlar. Güvenlik uzmanları, ortaya çıkan faaliyetleri takip edip analiz edebilir, tehditleri ve yetkisiz eylemleri hızla belirleyebilir. Bu erken tespit, güvenlik uzmanlarının güvenlik olaylarına ortaya çıktıkça hızla yanıt vermesini sağlayarak riskleri en aza indirmek için aktif bir yaklaşım oluşturur.

Aşağıdaki görselde Wazuh'un özelleştirilmiş konteyner kontrol paneli gösterilmektedir. Burada tüm konteynerlerden gelen etkinlikler sergilenmektedir.



Özelleştirilmiş konteyner gösterge paneli

Wazuh ile konteyner uyarı bildirimi

Wazuh, e-posta ve Slack gibi mesajlaşma platformlarıyla entegre olur . Ayrıca, olay yanıtlama ve gerçek zamanlı uyarılar için Jira gibi vaka yönetimi çözümleriyle de entegre olur . Bu, konteynerleştirilmiş ortamlarda olası tehditler veya yetkisiz eylemler meydana geldiğinde güvenlik ekiplerinin derhal bilgilendirilmesini sağlar.

Harici API entegrasyonuna ilişkin dokümantasyon, Integrator daemon'un Wazuh'un harici API'lere ve PagerDuty gibi vaka yönetim sistemleri araçlarına bağlanmasına nasıl olanak sağladığını açıklar .



Harici API'lere ve vaka yönetim sistemlerine bağlanın

Revision #4
Created 6 December 2023 18:04:39 by LastGuard
Updated 11 December 2024 16:47:22 by Ayşegül Sarıkaya