Log Analizi

Günlük veri analizi, farklı sistemler, uygulamalar veya cihazlar tarafından oluşturulan günlük dosyalarını incelemeyi ve bunlardan değerli içgörüler çıkarmayı içeren önemli bir işlemdir. Bu günlükler, sorun giderme, güvenlik analizi ve izleme ve performansı optimize etme için yararlı bilgiler sağlayan olayların kayıtlarını içerir. Günlük veri analizi, güvenli, verimli ve güvenilir bir BT ekosistemine katkıda bulunan temel bir uygulamadır.

Wazuh, uç noktalardan, ağ aygıtlarından ve uygulamalardan günlükleri toplar, analiz eder ve depolar. İzlenen bir uç noktada çalışan Wazuh aracısı, analiz için sistem ve uygulama günlüklerini toplar ve Wazuh sunucusuna iletir. Ayrıca, syslog veya üçüncü taraf API entegrasyonları aracılığıyla günlük mesajlarını Wazuh sunucusuna gönderebilirsiniz.

Günlük veri toplama

Wazuh, BT ortamınızın çeşitli yönlerinin kapsamlı bir şekilde izlenmesini sağlayarak çok çeşitli kaynaklardan günlükler toplar. Wazuh'un izlenen uç noktalardan günlükleri nasıl topladığını ve analiz ettiğini daha iyi anlamak için Günlük veri toplama konusundaki belgelerimize göz atabilirsiniz. Wazuh tarafından desteklenen yaygın günlük kaynaklarından bazıları şunlardır:

- **İşletim sistemi günlükleri : Wazuh,** Linux , Windows ve macOS dahil olmak üzere çeşitli işletim sistemlerinden günlükleri toplar .
  Wazuh, Linux uç noktalarından syslog, auditd, uygulama günlükleri ve diğerlerini toplayabilir.
  Wazuh, Windows olay kanalı ve Windows olay günlüğü biçimini kullanarak Windows uç noktalarında günlükleri toplar. Varsayılan olarak, Wazuh aracısı Windows uç noktalarındaki Sistem, Uygulama ve Güvenlik Windows olay kanallarını izler. Wazuh aracısı diğer Windows olay kanallarını yapılandırma ve izleme esnekliği sunar .
  Wazuh, macOS uç noktalarındaki günlükleri toplamak için birleşik günlükleme sistemini (ULS) kullanır. macOS ULS, günlüklerin tüm sistem düzeylerinde yönetimini ve depolanmasını merkezileştirir.
  Aşağıdaki görüntü, `Microsoft-Windows-Sysmon/Operational` bir Windows uç noktasındaki olay kanalından toplanan bir olayı göstermektedir.

Sysmon operasyonel Olay kanalı uyarısı

- **Syslog olayları** : Wazuh, Linux/Unix sistemleri ve aracı kurulumunu desteklemeyen ağ cihazları da dahil olmak üzere çok çeşitli kaynakları kapsayan syslog etkinleştirilmiş

cihazlardan günlükleri toplar. Aşağıdaki görüntü, Linux uç noktasında yeni bir kullanıcı oluşturulduğunda tetiklenen bir uyarıyı ve günlük rsyslog aracılığıyla Wazuh sunucusuna iletildiğini gösterir.

Sistem uyarısına yeni kullanıcı eklendi

- **Aracısız izleme** : Wazuh aracısız izleme modülü, aracı kurulumunu desteklemeyen uç noktaları izler. Uç nokta ile Wazuh sunucusu arasında bir SSH bağlantısı gerektirir. Wazuh aracısız izleme modülü dosyaları, dizinleri veya yapılandırmaları izler ve uç noktada komutlar çalıştırır. Aşağıdaki görüntü, Wazuh panosundaki aracısız bir cihazdan gelen bir uyarıdır.

Aracısız cihaz uyarısı

- **Bulut sağlayıcı günlükleri** : Wazuh , EC2 örnekleri, S3 kovaları, Azure VM'leri ve daha fazlası gibi bulut hizmetlerinden günlükleri toplamak için AWS , Azure , Google Cloud ve Office 365 gibi bulut sağlayıcılarıyla entegre olur . Aşağıdaki görüntü , Wazuh panosundaki **BULUT GÜVENLİĞİ bölümünü gösterir.**

Bulut sağlayıcı modülleri

- **Özel günlükler : Wazuh'u** VirusTotal , Windows Defender ve ClamAV gibi çeşitli uygulamalardan ve üçüncü taraf güvenlik araçlarından günlükleri toplayıp ayrıştıracak şekilde yapılandırabilirsiniz . Aşağıdaki görüntü, Wazuh sunucusu tarafından işlenen VirusTotal'dan bir günlüğün uyarısını göstermektedir.

VirusTotal günlük uyarısı

Kurallar ve kod çözücüler

Wazuh kuralları ve kod çözücüleri, günlük veri analizi ve tehdit tespiti ve yanıtında temel bileşenlerdir. Wazuh, günlük veri analizi için güçlü bir platform sunarak kuruluşların potansiyel güvenlik tehditlerini derhal tespit edip yanıtlayarak güvenlik duruşlarını geliştirmelerine olanak tanır.

Wazuh kod çözücüleri, çeşitli kaynaklardan toplanan günlük verilerini ayrıştırmak ve normalleştirmekten sorumludur. Kod çözücüler, ham günlük verilerini çeşitli biçimlerde Wazuh'un etkili bir şekilde işleyebileceği birleşik ve yapılandırılmış bir biçime dönüştürmek için gereklidir. Wazuh, syslog, Windows olay kanalı, macOS ULS ve daha fazlası gibi yaygın günlük biçimleri için önceden oluşturulmuş kod çözücülere sahiptir. Ek olarak, Wazuh, benzersiz günlük biçimlerine sahip belirli uygulamalardan veya cihazlardan günlükleri ayrıştırmak için özel kod çözücüler tanımlamanıza olanak tanır. Wazuh, kod çözücüleri kullanarak günlük verilerini verimli bir şekilde

yorumlayabilir ve zaman damgaları, günlük düzeyleri, kaynak IP adresleri, kullanıcı adları ve daha fazlası gibi ilgili bilgileri çıkarabilir. Aşağıda gösterildiği gibi, Wazuh panosunun **Sunucu yönetimi** > **Kod çözücüler** bölümünde Wazuh'un kullanıma hazır ve özel kod çözücülerini görüntüleyebilirsiniz .

Wazuh panosundaki kod çözücüler

Wazuh kural seti günlük verilerindeki güvenlik olaylarını ve anormallikleri algılar. Bu kurallar belirli bir biçimde yazılır ve belirli koşullar karşılandığında uyarıları tetikler. Kurallar, güvenlik tehditlerini gösterebilecek belirli günlük girişleriyle eşleşmek için günlük alanları, değerler veya kalıplar gibi belirli ölçütlere göre tanımlanır. Wazuh, yaygın güvenlik kullanım durumlarını kapsayan çok çeşitli önceden oluşturulmuş kurallar sağlar. Ayrıca, yöneticiler kendi özel ortamlarına ve güvenlik gereksinimlerine göre uyarlanmış özel kurallar **oluşturabilir. Wazuh panosunun Sunucu yönetimi kategorisi, varsayılan ve özel Kuralları** görüntülemenizi sağlar.

Wazuh panosundaki kurallar

Örneğin, aşağıdaki kural, `match`kuralın aradığı deseni tanımlamak için kullanılan bir alanı içerir. Kural ayrıca, `level`sonuç uyarısının önceliğini belirten bir alana sahiptir. Ek olarak, kurallar olayları MITRE ATT&CK çerçevesinden gelen teknik tanımlayıcılarla zenginleştirir ve bunları düzenleyici uyumluluk kontrollerine eşler.

```
<rule id="5715" level="3">
  <if_sid>5700</if_sid>
  <match>^Accepted|authenticated.$</match>
  <description>sshd: authentication success.</description>
  <mitre>
    <id>T1078</id>
    <id>T1021</id>
  </mitre>
  <group>authentication_success,gdpr_IV_32.2,gpg13_7.1,gpg13_7.2,hipaa_164.312.b,nist_800_53_AU.14,nist_80
</rule>
```

Günlük verilerinin indekslenmesi ve depolanması

Wazuh dizinleyicisi, son derece ölçeklenebilir, dağıtılmış gerçek zamanlı bir arama ve analiz motorudur. Wazuh dizinleyicisi, Wazuh sunucusu tarafından oluşturulan uyarıları depolayıp dizinlediği için günlük analizinde kritik öneme sahiptir. Bu uyarılar JSON belgeleri olarak depolanır.

Wazuh dizinleyicisi, JSON belgelerini parçalar adı verilen birkaç kapsayıcıda depolayarak ve parçaları birden fazla düğüme dağıtarak yedekliliği garanti eder. Bu uygulama, donanım arızaları veya siber saldırılar meydana geldiğinde kesintiyi önler ve düğümler bir kümeye eklendikçe sorgu kapasitesini artırır.

Wazuh, çeşitli olay türlerini depolamak için dört endeks kullanır:

- **wazuh-alerts,** bir olay yeterince yüksek önceliğe sahip bir kuralı tetiklediğinde Wazuh sunucusu tarafından oluşturulan uyarıları depolar. Aşağıdaki görüntü, Wazuh panosunun **Discover**`wazuh-alerts-*` modülündeki uyarıları gösterir. Dizin deseni varsayılan olarak olarak ayarlanmıştır .



wazuh-alerts-* dizin desenindeki uyarılar

- **wazuh-archives** dizini, uyarı tetikleyip tetiklemediklerine bakılmaksızın Wazuh sunucusundan alınan tüm olayları depolar. Wazuh arşivleri, izlenen uç noktalarda gerçekleşen olaylara dair daha derin bir içgörü sunan günlük tutma ve sorgulama yeteneklerini etkinleştirmek için bu dizini kullanır. Wazuh arşivleri, tüm günlükleri depolamak için gereken büyük depolama gereksinimleri nedeniyle varsayılan olarak devre dışıdır. Aşağıdaki görüntü, dizin deseni olarak ayarlanmış Wazuh panosunun **Keşfet**`wazuh-archives-*` bölümündeki arşivlenmiş olayları gösterir.



wazuh-archives-* dizin desenindeki olaylar

- **wazuh-monitoring** dizini, belirli bir zaman dilimi boyunca Wazuh aracılarının durumuyla ilgili verileri depolar. Aracın durumu `Active`, `Disconnected`, veya olabilir . Bu bilgi, birkaç nedenden dolayı panoya rapor vermeyen ve araştırılması gereken Wazuh aracılarını izlemek için çok faydalıdır. Aşağıdaki görüntü, Wazuh panosundaki araçların bağlantı durumunu gösterir. Görüntüde gösterildiği gibi aracı bilgileri dizinden toplanır .`Never connected``wazuh-monitoring`



Wazuh monitoring dizininden ajan bilgisi

- **wazuh-statistics** endeksi, Wazuh sunucusuyla ilgili performans verilerini depolar. Bu bilgi, Wazuh sunucusunun mevcut bilgi işlem kaynaklarıyla en iyi şekilde performans göstermesini sağlamak için kritik öneme sahiptir. Aşağıdaki görüntü, Wazuh panosundaki performansla ilgili olayları gösterir.



Performansla ilgili etkinlikler

Günlük verilerinin sorgulanması ve görselleştirilmesi

Wazuh panosu, günlük veri sorgulama ve görselleştirme yetenekleri sunar. Panonun sezgisel arayüzünden yararlanarak Wazuh tarafından toplanan günlük verilerinden anlamlı içgörüler çıkarmak için karmaşık aramalar ve sorgular gerçekleştirebilirsiniz.

Wazuh, güvenlik izleme ve uyumluluk kullanım örneklerine özel olarak uyarlanmış, kullanıma hazır bir dizi önceden tanımlanmış pano ve görselleştirme sunar. Bu panolar, başarısız oturum açmalar, kötü amaçlı yazılım tespiti ve sistem anormallikleri gibi yaygın güvenlik olaylarına ilişkin içgörüler sağlar. Bu panoları özel ihtiyaçlarınıza ve gereksinimlerinize uyacak şekilde daha da özelleştirebilirsiniz. Aşağıda, **En İyi 5 PCI DSS Gereksinimi** , **En İyi 5 uyarı** ve **Uyarı grupları evrimi** gibi çeşitli ilginç bilgileri gösteren **Güvenlik olayı** panosunun örnek bir görüntüsü bulunmaktadır .

> Güvenlik olay panosu
> Image not found or type unknown

Wazuh panosu kullanıcıların günlük girişlerini gerçek zamanlı olarak incelemesini, çeşitli filtreler uygulamasını ve belirli olaylara veya zaman aralıklarına ayrıntılı olarak bakmasını sağlar. Bu esneklik, güvenlik analistlerinin ortamlarındaki eğilimleri, anormallikleri ve olası güvenlik olaylarını belirlemesine olanak tanır.

Wazuh, kullanıcıların temel performans göstergelerini, güvenlik ölçümlerini ve kritik sistemlerin ve uygulamaların gerçek zamanlı izlenmesini görüntüleyen özelleştirilmiş panolar oluşturmasına olanak tanır . Kullanıcılar, pasta grafikleri, çizgi grafikler ve ısı haritaları gibi birden fazla görselleştirmeyi tek bir panoda bir araya getirerek altyapılarının güvenlik duruşuna dair bütünsel bir görünüm sağlayabilir.

Revision #4
Created 6 December 2023 18:01:58 by LastGuard
Updated 23 December 2024 18:13:53 by Ayşegül Sarıkaya