Google Cloud'u İzleme

Google Cloud, Google tarafından sağlanan kapsamlı bir bulut bilişim hizmetleri paketidir. Çeşitli altyapı ve uygulama hizmetleri sunarak işletmelerin ihtiyaç duydukları uygulamaları verimli bir şekilde dağıtmalarını, oluşturmalarını ve ölçeklendirmelerini sağlar. Wazuh, Google Cloud altyapınızın güvenlik duruşunu geliştiren güvenlik izleme, olay yanıtlama ve düzenleyici uyumluluk yetenekleri sunar. Wazuh aracılarını Google Cloud örneklerinize yükleyebilir veya Wazuh modüllerini desteklenen Google Cloud hizmetleriyle entegre olacak şekilde yapılandırabilirsiniz. Bu, Google Cloud ortamınızdaki olayları analiz etmenizi ve anormallikler için gerçek zamanlı uyarılar almanızı sağlar.

- Google Cloud Örneklerini İzleme
- Google Cloud Hizmetlerini İzleme
- Bulut Güvenlik Durum Yönetimi

Google Cloud Örneklerini İzleme

Wazuh aracısını doğrudan Google Cloud sanal makinelerine veya Linux, Windows ve macOS işletim sistemleri için örneklere yükleyebilirsiniz. Yüklendikten sonra, Wazuh aracıları izlenen uç noktalardan güvenlik verilerini toplar ve analiz için Wazuh sunucusuna iletir. Güvenlik koruması, analize ve algılanan olaylara göre izlenen uç noktalara uygulanır.

Wazuh aracıları hakkında daha fazla bilgi edinmek için Wazuh aracısı kurulum ve kayıt belgelerini inceleyin . Ayrıca, Wazuh SIEM ve XDR yetenekleri ve bunların yapılandırması hakkında yetenekler belgelerimizde okuyun.

Google Cloud Hizmetlerini İzleme

Wazuh, Google Cloud Pub/Sub ve Google Cloud Storage kova hizmetleriyle entegre olan modüller sunar. Pub/Sub, bağımsız uygulamalar arasında iletişim sağlayan bir Google Cloud mesajlaşma hizmetidir; Cloud Storage ise verilerinizi Google Cloud'da depolamanıza ve dağıtmanıza olanak tanıyan yönetilen bir hizmettir. Google Cloud'u izlemek için kullanılan Wazuh modülleri, Google Cloud altyapınızdan veri erişimi, ayrıcalıklı etkinlikler, sistem etkinlikleri ve DNS sorguları gibi farklı etkinlikleri getirir.

Bu günlük toplama ve analiz yetenekleri, altyapıları için Google Cloud Platform'a güvenen kuruluşlara bulut ortamlarındaki faaliyetleri proaktif olarak izleme ve güvenlik olaylarına etkili bir şekilde yanıt verme olanağı sağlıyor.

Bulut Güvenlik Durum Yönetimi

Bulut Güvenlik Duruş Yönetimi (CSPM), bulut ortamlarının güvenliğini ve uyumluluğunu sağlamada önemlidir. Kuruluşların bulut kaynaklarını hızlı ve kolay bir şekilde sağlayabildiği, yapılandırabildiği ve değiştirebildiği bulut bilişimde güvenlik yanlış yapılandırmaları potansiyeli artar. Bu güvenlik sorunları, izinlerin yanlış yönetilmesi, ağ yapılandırmalarındaki boşluklar ve diğer çeşitli faktörler nedeniyle ortaya çıkabilir.

Bulut Güvenlik Duruş Yönetimi, yanlış yapılandırmaları, güvenlik açıklarını ve olası riskleri belirlemek için bulut iş yüklerini sürekli olarak izleyerek ve değerlendirerek bu zorluğun üstesinden gelir. Ayrıca olası güvenlik risklerini düzeltmek için düzeltme adımları sağlar ve böylece bulut ortamının genel güvenlik duruşunu iyileştirir.

Wazuh, bulut, şirket içi, konteynerleştirilmiş ve sanallaştırılmış ortamlar için kapsamlı koruma sağlayan ücretsiz, açık kaynaklı, kurumsal düzeyde bir güvenlik izleme platformudur. Bu bölüm, Google Cloud'da duruş güvenliğini incelemek için Wazuh'un nasıl kullanılacağını gösterir.

Wazuh'u Google Cloud İle Entegre Etme

Wazuh, Google Cloud yayıncı ve abone hizmetini (Google Cloud Pub/Sub) kullanarak Google Cloud ile entegre olur. Google Cloud Pub/Sub, uygulamalar arasında günlük verilerini göndermenize ve almanıza yardımcı olan bir mesajlaşma hizmetidir. Wazuh, Pub/Sub hizmetinden günlükleri alan Google Cloud için bir entegrasyon modülü sağlar.

Google Cloud Platform entegrasyonuna genel bakış

Google Bulut

Google Cloud Hesabını Yapılandırma

Yeni bir Google Cloud projesi ve Wazuh Google Cloud modülünün Google Pub/Sub hizmetinden günlük verilerini çekmesini sağlayan bir hizmet hesabı oluşturun. Bu yapıldıktan sonra Pub/Sub ve Sink hizmetlerini yapılandırın. Sink hizmeti, bulut güvenlik duruşu günlüklerini merkezi Google Cloud Logging hizmetinden Pub/Sub hizmetine yönlendirir.

Yapılandırmayı gerçekleştirmek için aşağıdaki adımları izleyin.

1. Yeni bir Google Cloud projesi oluşturun . Proje kimliğini not edin.

GCP projesi oluştur


   Nerede:
   - **Proje adı,** projeye verilen isimdir.
   - **Kuruluş,** Google Cloud kuruluşunun adıdır.

2. **IAM ve yönetici** açılır menüsüne gidin ve yeni bir hizmet hesabı oluşturmak için **Hizmet hesapları'nı** seçin . Hizmet hesapları oluşturma sayfasında, hesaba ve rollerini ekleyin.
Pub/Sub PublisherPub/Sub Subscriber

Hizmet hesabı oluştur


   Nerede:
   - **Hizmet hesabı adı** , Wazuh'un Google Cloud'a bağlanmak için kullandığı ayrıcalıklı hesaptır.
   - **Roller,** servis hesabına verilen haklardır.

3. Yeni oluşturulan hizmet hesabını açın ve JSON formatında özel bir anahtar oluşturun . Tarayıcınız anahtarı otomatik olarak indirir. Wazuh, Google Cloud projenizde kimlik doğrulaması yapmak için anahtarı kullanır.

JSON formatında özel bir anahtar oluşturun


4. Pub/SubSayfanın üst kısmındaki konsol arama alanından arayın ve seçin. **Konu Oluştur'a** tıklayın . **Konu Oluştur** sayfasında, **Konu Kimliğini** girin ve **Varsayılan abonelik ekle** onay kutusunun seçili olduğundan emin olun. Ardından, **Oluştur'a tıklayın.** Abonelik Kimliğini not edin .

Konu oluştur


5. Google Cloud konsolunda **Log Router'ı** arayın ve seçin. **Create Sink'e** tıklayın . Lavaboya bir ad verin ve **Next'e** tıklayın . **Sink hedef servisinde Cloud Pub/Sub konusunu** seçin . Sonra, yukarıda oluşturulan konu adını seçin. **Create Sink'e** tıklayın .

Günlük yönlendirme havuzunu oluştur


   Google Cloud projesindeki Log Router ve Sink hizmetleri sırasıyla log yönetimi ve log hedefi yönlendirmesinden sorumludur.
6. Google Cloud Findings hizmetinden Google Cloud Pub/Sub hizmetine sürekli günlük aktarımını yapılandırın.

Sürekli dışa aktarmalar yapılandırın


Wazuh Sunucusu

Aşağıdaki adımları uygulayarak Wazuh sunucusunu Google Cloud'dan günlük alacak şekilde yapılandırın.

> Not: Komutları root yetkisiyle çalıştırın.

1. `credentials.json`Şu dizinde bir dosya oluşturun `/var/ossec/wodles/gcloud/`:

   ```
   # touch /var/ossec/wodles/gcloud/credentials.json
   ```

2. Dosyayı daha önce indirilen JSON formatındaki özel anahtarın `/var/ossec/wodles/gcloud/credentials.json` içeriğiyle güncelleyin . Google Cloud Pub/Sub için Wazuh modülü, Google Cloud hesabınızı doğrulamak için anahtar dosyasını kullanır.

3. Yapılandırma dosyasına aşağıdaki içeriği ekleyin `/var/ossec/etc/ossec.conf`. Yapılandırma, Wazuh'un proje kimliğini, Google Cloud PubSub abonelik kimliğini ve bir kimlik bilgisini kullanarak Google Cloud'a nasıl bağlanacağını belirtir.

   ```
   <ossec_config>
     <gcp-pubsub>
       <pull_on_start>yes</pull_on_start>
       <interval>5m</interval>
       <project_id><PROJECT_ID></project_id>
       <subscription_name><SUBSCRIPTION_ID></subscription_name>
        <credentials_file>/var/ossec/wodles/gcloud/credentials.json</credentials_file>
     </gcp-pubsub>
   </ossec_config>
   ```

   Yapılandırmadaki değişkenleri uygun değerlerle değiştirin.
   Nerede:
   - `<PROJECT_ID>`Yukarıda oluşturulan Google Cloud projesinin kimliğidir .
   - `<SUBSCRIPTION_NAME>`Google Cloud Pub/Sub'ınızın abonelik kimliğinizdir .

4. `gcp_posture.xml`Dizin içinde bir kural dosyası oluşturun `/var/ossec/etc/rules/`ve Google Cloud duruş bulgularını algılamak için aşağıdaki özel kuralları ekleyin:

   ```
   <group name="gcp,">
     <!-- Misconfiguration detection -->
       <rule id="100200" level="10">
         <if_sid>65000</if_sid>
         <field name="gcp.finding.findingClass">MISCONFIGURATION</field>
         <description>A $(gcp.finding.findingClass) with $(gcp.finding.severity) severity has been discovered on
         <mitre>
           <id>T1562</id>
         </mitre>
       </rule>

     <!-- Threat detection -->
       <rule id="100201" level="10">
         <if_sid>65000</if_sid>
         <field name="gcp.finding.findingClass">THREAT</field>
         <description>A $(gcp.finding.findingClass) with $(gcp.finding.severity) severity has been discovered on
   ```

```
      <mitre>
        <id>T1562</id>
      </mitre>
    </rule>
</group>
```

Nerede:

- Wazuh bir Google Cloud hesabında yanlış yapılandırma tespit ettiğinde Kural Kimliği `100200`tetiklenir.
- Google Cloud bir tehdit algıladığında Kural Kimliği `100201`tetiklenir.

5. Yapılandırmayı uygulamak için Wazuh yöneticisini yeniden başlatın:

```
systemctl restart wazuh-manager
```

Bulut Güvenlik Duruşu Yönetimi Simülasyonu

Bulgular modülü **,** bir Google Cloud projesi genelindeki güvenlik yanlış yapılandırmalarını kaydeden bir Google Cloud Güvenlik Komuta Merkezi hizmetidir.

Ağ Yanlış Yapılandırmaları

Ağ yanlış yapılandırmasını simüle etmek için Google Cloud konsolunda aşağıdaki işlemleri gerçekleştirin.

1. **Compute Engine API'yi** etkinleştirin . Bu, dahili VPC güvenlik duvarını etkinleştirecektir.

Hesaplama motoru API'sini etkinleştirin
Image not found or type unknown

2. `verybadrule`Birden fazla ağ yanlış yapılandırmasını simüle etmek için Google Cloud ağ güvenliğinde bir güvenlik duvarı kuralı oluşturun . Güvenlik duvarı kuralı tüm IP adreslerinden ve bağlantı noktalarından gelen bağlantılara izin verir.

Güvenlik duvarı kuralı oluştur
Image not found or type unknown

3. `verybadrule`Google Cloud ağ güvenliğindeki kurallar listesinden güvenlik duvarı kuralını silin.

Güvenlik duvarı kuralını sil
Image not found or type unknown

Kimlik ve Erişim Yönetimi Anormal Etkinliği

1. Eğer henüz bir Gmail e-posta adresiniz yoksa, bir test adresi oluşturun.

2. **IAM ve Yönetici** açılır menüsüne gidin ve **IAM'ı seçin. Erişim** Ver'e tıklayın . Erişim Ver sayfasında, test kullanıcısının Gmail adresini **Yeni sorumlu** olarak girin . Ardından, rolü atayın, **Proje** > **Sahip** ve **Kaydet'e** tıklayın.



Test e-postasına erişim izni verin

Duruş Yönetimi Sonucu

Google Cloud duruş yönetimi sonuçlarını Threat Hunting'e giderek görselleştirin . Kural kimlikleri `100200`ve için filtre uygulayın `100201`.



GCP duruş yönetimi için Wazuh uyarıları

Yukarıdaki görselde Google Cloud ortamında keşfedilen hatalı yapılandırma ve tehditler gösterilmektedir.

> Not: Google Cloud'un güvenlik komuta merkezini ilk etkinleştirdiğinizde uyarılar Wazuh panosunda hemen görünmeyebilir. Bunun nedeni, etkinleştirme işleminin neden olduğu gecikmedir.