Bulut Güvenliği

Wazuh, AWS, Microsoft Azure veya GCP gibi en kapsamlı ve yaygın olarak benimsenen bulut platformlarından bazılarının güvenliğini artırmaya yardımcı olur. Aşağıdaki bölümlerde Wazuh Cloud güvenliği hakkında daha fazla bilgi edinin:

- Amazon Web Hizmetlerini (AWS) İzleme
  - AWS Örneklerini İzleme
  - AWS Tabanlı Hizmetlerin İzlenmesi
- Microsoft Azure'u Wazuh ile İzleme
  - İzleme Örnekleri
  - Azure Platformunu ve Hizmetlerini İzleme
  - Microsoft Azure Günlük Analizi
  - Microsoft Graph Servislerini Wazuh İle İzleme
  - Microsoft Azure Depolama
  - Microsoft Grafiği
- Google Cloud'u İzleme
  - Google Cloud Örneklerini İzleme
  - Google Cloud Hizmetlerini İzleme
  - Bulut Güvenlik Durum Yönetimi
- Office 365'i İzleme
  - Office 365 Denetim Günlüklerinin İzlenmesi
- GitHub'ı İzleme
  - GitHub Denetim Günlüklerinin İzlenmesi

Amazon Web Hizmetlerini (AWS) İzleme

Amazon Web Services (AWS), Amazon tarafından sağlanan yaygın olarak kullanılan bir bulut bilişim platformudur. İşlem gücü, depolama, veritabanları, makine öğrenimi, analiz, güvenlik ve daha fazlası dahil olmak üzere geniş bir hizmet yelpazesi sunar. AWS, bireylerin, işletmelerin ve kuruluşların fiziksel altyapıya yatırım yapma ve bakımını yapma ihtiyacı olmadan işlem kaynaklarına erişmesini ve bunları kullanmasını sağlar. Açık kaynaklı bir güvenlik platformu olan Wazuh, AWS altyapınızın güvenliğini izlemek ve iyileştirmek için kapsamlı bir özellik paketi sunar. EC2 örneklerinize Wazuh aracıları yükleyebilir veya AWS için Wazuh modülünü desteklenen AWS hizmetleriyle entegre edebilirsiniz. Bu, olayları analiz etmenizi ve AWS altyapınızdaki anormallikler için neredeyse gerçek zamanlı uyarılar almanızı sağlar. Aşağıdaki bölümlerde AWS altyapınızı nasıl izleyeceğinizi öğrenebilirsiniz:

AWS Örneklerini İzleme

AWS EC2 örneklerinize Wazuh aracısını yükleyerek bu örneklerdeki içgörüler elde edebilir ve etkinlikleri izleyebilirsiniz.

Wazuh aracısı bir EC2 örneğinde hizmet olarak çalışır ve şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla sistem, güvenlik ve uygulama verilerini toplar ve Wazuh sunucusuna iletir.

AWS Tabanlı Hizmetlerin İzlenmesi

AWS için Wazuh modülü, bu hizmetlerin günlüklerini toplayarak ve günlükleri Wazuh kural setiyle analiz ederek çeşitli AWS hizmetlerinin izlenmesini sağlar. Bu, Wazuh'un EC2 örneği yapılandırmasına, kullanıcıların ve sistemlerin yetkisiz davranışlarına, S3'te depolanan verilere ve daha fazlasına dayalı uyarıları tetiklemesini sağlar. Böylece AWS altyapısı içindeki etkinlikler hakkında ayrıntılı bilgi sağlanır.

Aşağıdaki her bölüm, desteklenen tüm AWS hizmetlerini yapılandırmak ve kurmak için ayrıntılı talimatlar ve ayrıca bu hizmetlerden günlükleri toplamak için gereken Wazuh yapılandırmasını içerir. Ayrıca karşılaşabileceğiniz yaygın sorunları çözmek için adımlar da içerir.

Microsoft Azure'u Wazuh ile İzleme

Microsoft Azure, Microsoft'un bilgi işlem gücü, depolama seçenekleri ve ağ yetenekleri gibi çok çeşitli hizmetler sunan bir bulut bilişim platformudur. Sanal bilgi işlem, analiz, depolama ve ağ gibi çeşitli uygulamalar için çözümler sunar ve işletmelerin ve geliştiricilerin çeşitli ihtiyaçlarını karşılar. Bulut örneğinizi güvence altına almak, Microsoft Azure gibi bulut sağlayıcıları tarafından sunulan bulut hizmetlerini kullanan şirketler için önemli bir husustur. Açık kaynaklı bir güvenlik izleme platformu olan Wazuh, Microsoft Azure ortamlarında güvenlik ve çalışma zamanı olayları tarafından oluşturulan verileri toplamak ve analiz etmek için çözümler sunar. Wazuh'u Microsoft Azure ile entegre etmek, Azure dağıtımlarının güvenlik duruşunu iyileştirir ve düzenleyici standartlara ve operasyonel bütünlüğe uyumu sağlar.

İzleme Örnekleri

Wazuh aracısı platformlar arası uyumludur, yani Windows, Linux, Solaris, BSD ve macOS dahil olmak üzere çeşitli işletim sistemlerinde çalışabilir. Farklı sistemler ve uygulamalar hakkında veri toplar ve örneğin Dosya Bütünlüğü İzleme (FIM) ve Güvenlik Yapılandırma Değerlendirmesi (SCA) gibi diğer Wazuh yeteneklerinden yararlanmasını sağlar. Bu veriler şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla Wazuh sunucusuna gönderilir. Benzersiz önceden paylaşılmış anahtar kayıt işlemi bu güvenli kanalı oluşturur.

Microsoft Azure ortamınızdaki sanal makinelere Wazuh aracısını yükleyebilirsiniz. Wazuh aracısını kullanarak bulut sanal makinelerini izlemek faydalıdır çünkü kapsamlı güvenlik ve performans denetimi sağlayarak dinamik bulut ortamlarında olası tehditlerin ve operasyonel sorunların erken tespitini sağlar.

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

Azure Platformunu ve Hizmetlerini İzleme

Azure Monitor Logs, Azure hizmetleri, sanal makineler ve uygulamalar dahil olmak üzere izlenen kaynaklardan günlükleri ve performans verilerini toplar ve düzenler. Bu içgörü, Azure Log Analytics REST API'sini kullanarak veya doğrudan bir Microsoft Azure Storage hesabının içeriklerine erişerek Wazuh'a gönderilir. Azure için Wazuh modülü, Wazuh dağıtımınızdan Microsoft Azure ortamlarınızın merkezi günlük kaydını, tehdit algılamasını ve uyumluluk yönetimini sağlar.

Azure için Wazuh modülü, Microsoft Azure günlüklerinize erişmek için bağımlılıklar ve kimlik bilgileri gerektirir. Bu bağımlılıklar varsayılan olarak Wazuh yöneticisinde mevcuttur, ancak entegrasyon için bir Wazuh aracısı kullandığınızda bunları yüklemeniz gerekir. Devam etmeden önce Önkoşullar bölümüne bir göz atın.

Ön koşullar

Bağımlılıkları Yükleme

Wazuh modülünü Azure için Wazuh yöneticisinde veya bir Wazuh aracısında yapılandırabilirsiniz. Bu seçim tamamen ortamınızda Azure altyapınıza nasıl eriştiğinize bağlıdır.

Azure ile entegrasyonu bir Wazuh aracısında yapılandırırken yalnızca bağımlılıkları yüklemeniz gerekir. Wazuh yöneticisi zaten gerekli tüm bağımlılıkları içerir.

Python

Azure için Wazuh modülü Python 3.8–3.12 ile uyumludur. Daha sonraki Python sürümleri de çalışmalı ancak uyumlu olduklarını garanti edemeyiz. Python 3 zaten yüklü değilse, izlenen uç noktanızda aşağıdaki komutu çalıştırın.

Yum

```
yum update && yum install python3
```

APT

```
apt-get update && apt-get install python3
```

Gerekli modülleri Python paket yöneticisi Pip ile kurabilirsiniz. Çoğu UNIX dağıtımının yazılım depolarında bu araç mevcuttur. Zaten kurulu değilse, uç noktanıza pip'i kurmak için aşağıdaki komutu çalıştırın.

Yum

```
yum update && yum install python3-pip
```

APT

```
apt-get update && apt-get install python3-pip
```

Bağımlılıkların kurulumunu kolaylaştırmak için Pip 19.3 veya üzerini kullanmanızı öneririz. Pip sürümünüzü kontrol etmek için bu komutu çalıştırın.

```
pip3 --version
```

Örnek çıktı aşağıdaki gibidir.

Output

```
pip 22.0.2 from /usr/lib/python3/dist-packages/pip (python 3.10)
```

Eğer pip versiyonunuz 19.3'ten düşükse, versiyonu yükseltmek için aşağıdaki komutu çalıştırın.

Python 3.8–3.10

```
pip3 install --upgrade pip
```

Python 3.11–3.12

```
pip3 install --upgrade pip --break-system-packages
```

> Not: Bu komut, varsayılan harici olarak yönetilen Python ortamını değiştirir. Daha fazla bilgi için PEP 668 açıklamasına bakın.
>
> Değişikliği önlemek için sanal bir ortamda çalışabilirsiniz . Python betiğinin shebang'ini

> sanal ortamınızdaki yorumlayıcıyla güncellemelisiniz . Örneğin, .`pip3 install --upgrade pip` `/var/ossec/wodles/azure/azure-logs#!/path/to/your/virtual/environment/bin/python3`

Python İçin Azure Storage İstemci Kitaplığı

Wazuh aracı uç noktanızı kurmak ve Microsoft Azure platformunuzu ve hizmetlerinizi izlemek için aşağıdaki komuttaki kütüphanelere ihtiyacınız var.

Python 3.8–3.10

```
pip3 install azure-storage-blob==12.20.0 azure-storage-common==2.1.0 azure-common==1.1.25 cryptography==3.3.2 cffi==1.14.4 pycparser==2.20 six==1.14.0 python-dateutil==2.8.1 requests==2.25.1 certifi==2022.12.07 chardet==3.0.4 idna==2.9 urllib3==1.26.18 SQLAlchemy==2.0.23 pytz==2020.1
```

Python 3.11–3.12

```
pip3 install --break-system-packages azure-storage-blob==12.20.0 azure-storage-common==2.1.0 azure-common==1.1.25 cryptography==3.3.2 cffi==1.14.4 pycparser==2.20 six==1.14.0 python-dateutil==2.8.1 requests==2.25.1 certifi==2022.12.07 chardet==3.0.4 idna==2.9 urllib3==1.26.18 SQLAlchemy==2.0.23 pytz==2020.1
```

> Not: Eğer sanal ortam kullanıyorsanız `--break-system-packages`yukarıdaki komuttan parametreyi kaldırın.

Azure Kimlik Bilgilerini Yapılandırma

Azure için Wazuh modülünün Azure'a başarılı bir şekilde bağlanabilmesi için erişim kimlik bilgilerine sahip olması gerekir. Gereken kimlik bilgileri izleme türüne göre değişir. Bunlar şunları içerir:

- Microsoft Graph ve Azure Log Analytics için erişim kimlik bilgileri
- Microsoft Azure Storage için erişim kimlik bilgileri

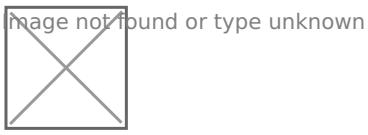
Aşağıdaki bölümlerde bu kimlik bilgilerini nasıl oluşturabileceğinize dair genel bir bakış sunulmaktadır.

Microsoft Graph ve Azure Log Analytics İçin Erişim Kimlik Bilgilerini Alma

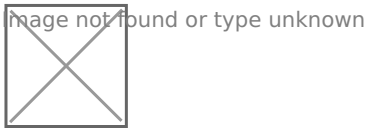
Azure için Wazuh modülünden gelen bağlantıyı doğrulamak için geçerli application_id ve application_key değerlerine ihtiyacınız var.

`application_id`ve elde etmek için aşağıdaki adımları izleyin `application_key`:

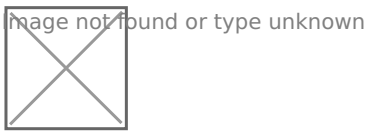
1. Microsoft Entra ID'ye gidin ve kayıtlı uygulamaya gidin.



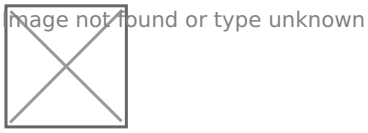
2. **Seçtiğiniz uygulamanın Sertifikalar ve sırlar** bölümüne gidin , ardından **Yeni istemci sırrı'nı** seçerek bir gizli anahtar oluşturun .



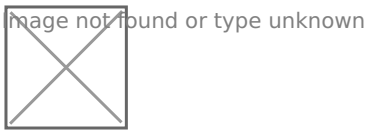
3. Anahtara açıklayıcı bir ad verin ve anahtarın etkin kalacağı süreyi belirtin, ardından **Ekle'yi** seçin.



4. `Value`ve 'yi kopyalayın . Bu değerleri güvenli bir şekilde sakladığınızdan emin olun, çünkü bunları yalnızca bir kez görüntüleyebilirsiniz. ' dir .`Secret ID``Value``application_key`



5. `application_id`Kayıtlı uygulamanızın değerini **Genel Bakış** bölümünden kopyalayın.



Microsoft Azure Storage İçin Erişim Kimlik Bilgilerini Alma

Microsoft Azure Storage geçerli `account_name`ve değerleri gerektirir. Bunları Azure ortamınızdaki **Storage hesaplarının Erişim anahtarları** bölümünden `account_key`edinebilirsiniz . Bir depolama hesabı oluşturmak için Microsoft kılavuzunu izleyin .

Aşağıdaki bölüm Microsoft Azure Depolama hesabı anahtarının alınmasına ilişkin adımları göstermektedir.

1. Microsoft Azure ortamınızın **Depolama hesapları** bölümüne gidin ve ilgilendiğiniz hesabı seçin.

Image not found or type unknown

2. ve değerlerine erişmek için sol bölmede bulunan **Erişim tuşlarına** gidin .`account_name` `account_key`

Image not found or type unknown

Wazuh Azure Kimlik Doğrulama Dosyası

Microsoft Azure ortamınızı Wazuh'ta kimlik doğrulamak için kimlik bilgilerinizi biçimini kullanarak bir dosyada saklamanız gerekir .`field = value`

Kimlik bilgileri dosyasında bulunması beklenen alanlar, izlediğiniz hizmet veya etkinliğin türüne bağlıdır.

Microsoft Azure Log Analitiği ve Grafiği

Dosya sadece iki satırdan oluşmalıdır, biri için `application_id`, diğeri ise `application_key`daha önce elde edilenler için:

```
application_id = <YOUR_APPLICATION_ID>
application_key = <YOUR_APPLICATION_KEY>
```

Microsoft Azure Depolama

Dosya sadece iki satırdan oluşmalıdır, biri için `account_name`ve diğeri `account_key`daha önce elde edilen için:

```
account_name = <YOUR_ACCOUNT_NAME>
account_key = <YOUR_ACCOUNT_KEY>
```

İzlediğiniz hizmet veya etkinlikten bağımsız olarak, yapılandırma dosyasında kimlik doğrulama dosyasını etiketi `/var/ossec/etc/ossec.conf`kullanarak belirtin. Aşağıdaki örneğe bir göz atın:`<auth_path>`

```
<wodle name="azure-logs">
  <disabled>no</disabled>
  <run_on_start>yes</run_on_start>

  <log_analytics>
    <auth_path>/var/ossec/wodles/credentials/log_analytics_credentials</auth_path>
     <tenantdomain>wazuh.com</tenantdomain>
     <request>
        <query>AzureActivity</query>
        <workspace>12345678-90ab-cdef-1234-567890abcdef</workspace>
```

```
        <time_offset>1d</time_offset>
      </request>
  </log_analytics>

  <graph>
    <auth_path>/var/ossec/wodles/credentials/graph_credentials</auth_path>
     <tenantdomain>wazuh.com</tenantdomain>
     <request>
        <query>auditLogs/directoryAudits</query>
        <time_offset>1d</time_offset>
     </request>
  </graph>

<storage>
    <auth_path>/var/ossec/wodles/credentials/storage_credentials</auth_path>
     <container name="insights-activity-logs">
        <blobs>.json</blobs>
        <content_type>json_inline</content_type>
        <time_offset>24h</time_offset>
     </container>
  </storage>
</wodle>
```

`request`Aynı yapılandırmada aynı anda birden fazla blok eklemek mümkündür. Azure için Wazuh modülü her isteği sırayla işler. Yukarıdaki yapılandırma bir örnektir. Microsoft Azure Log Analytics, Graph ve Storage yapılandırma bloklarını içerir.

Yeniden Çözümlemek

> Uyarı: Bu `reparse`seçenek başlangıç tarihinden bugüne kadar tüm günlükleri getirecek ve işleyecektir. Bu işlem yinelenen uyarılar üretebilir.

Daha eski Azure günlüklerini getirmek ve işlemek için, seçeneğini kullanarak Azure için Wazuh modülünü çalıştırmanız gerekir `--reparse`.
Değer `la_time_offset`, başlangıç noktası için bir ofset olarak zamanı ayarlar. Bir değer sağlamazsanız `la_time_offset`, Azure için Wazuh modülü ilk dosyayı işlediği tarihe döner.

Aşağıdaki kod bloğu, Wazuh yöneticisinde Azure için Wazuh modülünün şu `--reparse`seçenek kullanılarak çalıştırılmasına ilişkin bir örneği göstermektedir:

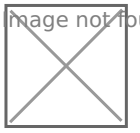
```
/var/ossec/wodles/azure/azure-logs --log_analytics --la_auth_path credentials_example --la_tenant_domain 'wazuh.example.domain' --la_tag azure-activity --la_query "AzureActivity" --workspace example-workspace --la_time_offset 50d --debug 2 --reparse
```

Parametre ayrıntılı bir çıktı alır. Bu çıktı, özellikle büyük miktarda veri işlenirken betiğin çalıştığını göstermek için yararlıdır.`--debug 2`

Microsoft Azure Günlük Analizi

Microsoft Azure Log Analytics, Microsoft Azure altyapınızı izleyen ve verilerinize özel gelişmiş aramalar yapmanıza olanak tanıyan sorgu yetenekleri sunan bir hizmettir.

Azure Log Analytics çözümü, tüm Azure aboneliklerinizdeki Azure etkinlik günlüklerini analiz etmenize ve aramanıza yardımcı olur ve aboneliklerinizin kaynaklarıyla gerçekleştirilen işlemler hakkında bilgi sağlar.



Microsoft Entra ID kimlik doğrulama şemasını kullanan Azure Log Analytics REST API'sini kullanarak Log Analytics tarafından toplanan verileri sorgulayabilirsiniz. Azure Log Analytics REST API'sini kullanmak için nitelikli bir uygulamaya veya istemciye ihtiyacınız vardır. Bunu Microsoft Azure portalında manuel olarak yapılandırmanız gerekir. Aşağıdaki bölüm uygulamanın nasıl kurulacağını gösterir ve bir kullanım örneği verir:

- Uygulamanın kurulumu
- Azure Log Analytics kullanım örneği

Yapılandırma

Azure

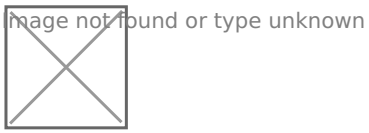
Uygulamanın kurulumu

Aşağıdaki işlem Azure Log Analytics REST API'sini kullanarak bir uygulama oluşturmayı ayrıntılı olarak açıklamaktadır. Mevcut bir uygulamayı yapılandırmak da mümkündür. Zaten mevcut bir uygulamanız varsa lütfen Uygulama oluşturma adımını atlayın.

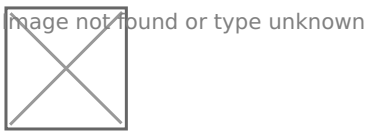
Uygulamanın oluşturulması

Azure Log Analytics için yeni bir uygulama oluşturmak üzere Microsoft Azure portalındaki Microsoft Entra ID paneline gidiyoruz.

1. **Microsoft Entra ID** panelinden **Uygulama kayıtları** seçeneğini seçin . Ardından, **Yeni kayıt** seçeneğini seçin.

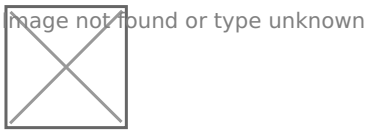


2. Uygulama için kullanıcıya dönük görüntü adını tanımlayın ve **Kaydet'i** seçin .

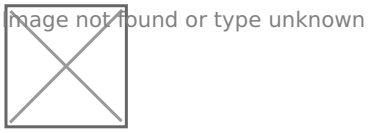


Uygulamaya İzinlerin Verilmesi

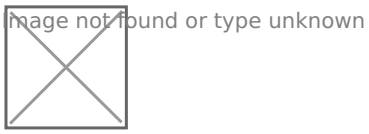
1. **Uygulama kaydından** Tüm **uygulamaları** seçin ve yenileyin. Yeni uygulama görünecektir. Bizim durumumuzda, görünen ad **LogAnalyticsApp'dir**.



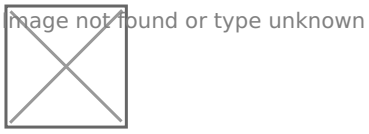
2. **Genel Bakış** bölümüne gidin ve **Uygulama (istemci) kimliğini** daha sonraki kimlik doğrulaması için kaydedin.



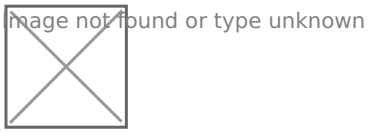
3. **API izinleri** bölümüne gidin ve uygulamaya **Data.Read** iznini ekleyin.



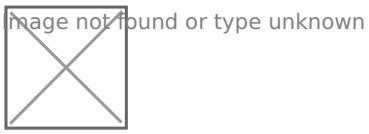
4. **Log Analytics API'yi** arayın .



5. Uygulamalar izinlerinden **Log Analytics verilerini oku iznini** seçin.

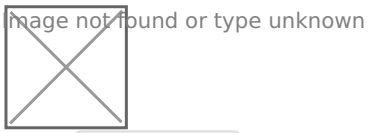


6. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.

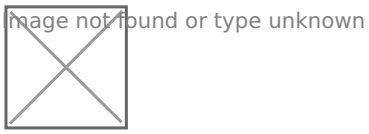


Uygulamaya Azure Log Analytics API'sine Erişim İzni Verme

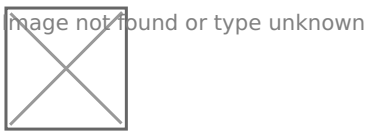
1. **Log Analytics çalışma alanlarına** erişin ve yeni bir çalışma alanı oluşturun veya mevcut bir çalışma alanını seçin.



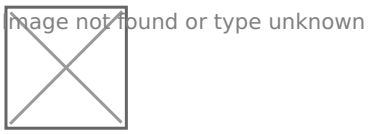
2. **Genel Bakış** bölümünden değeri kopyalayın .Workspace ID



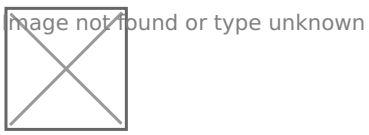
3. **Erişim denetimi (IAM)** bölümüne gidin , **Ekle'ye** tıklayın ve uygulamaya gerekli rolü eklemek için **Rol ataması ekle'yi** seçin .



4. **İş fonksiyonları rol sekmesinden Log Analytics Okuyucu** rolünü seçin.



5. **Üyeler** sekmesinden **Kullanıcı, grup veya hizmet sorumlusunu** seçin . **Üyeleri seç'e** tıklayın ve daha önce oluşturulan Uygulama kaydını bulun.

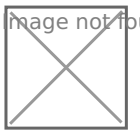


6. Bitirmek için **Gözden Geçir + Ata'ya** tıklayın .

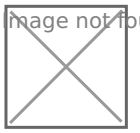
Günlükleri Çalışma Alanına gönderme

Önceki adımlarda oluşturulan Azure Log Analytics Çalışma Alanına günlükleri toplamak ve göndermek için bir tanılama ayarı oluşturmanız gerekir.

1. **Microsoft Entra ID'ye** geri dönün , sol menü çubuğunu aşağı kaydırın ve **Tanılama ayarları** bölümünü seçin.
2. **Tanılama ayarı ekle'ye** tıklayın.



3. **Kategoriler** altında toplamak istediğiniz günlük kategorilerini seçin . **Hedef ayrıntıları** altında **Log Analytics çalışma alanına gönder** seçeneğini işaretleyin. Önceki adımlarda oluşturduğunuz **Log Analytics Çalışma Alanını** seçin .



4. **Kaydet'e** tıklayın .

Azure Log Analytics, seçili kategorileri çalışma alanınıza aktaracaktır.

Wazuh, Azure Log Analytics'ten günlükleri çekmek için geçerli kimlik bilgileri gerektirir. Uygulama kaydına erişmek için bir istemci sırrının nasıl oluşturulacağını öğrenmek için kimlik bilgileri bölümüne bakın.

Wazuh Sunucusu veya Aracısı

Azure Log Analytics'inize erişmek için Wazuh modülünü Azure için yetkilendirmeniz gerekir. Yetkilendirmeyi ayarlama hakkında daha fazla bilgi için Azure kimlik bilgilerini yapılandırma bölümüne bakın.

1. `/var/ossec/etc/ossec.conf`Aşağıdaki yapılandırmayı Wazuh sunucusunun veya aracısının yerel yapılandırma dosyasına uygulayın . Bu, Wazuh modülünü Azure için nerede yapılandırdığınıza bağlı olacaktır:

```
<wodle name="azure-logs">
  <disabled>no</disabled>
  <run_on_start>no</run_on_start>

  <log_analytics>
    <auth_path>/var/ossec/wodles/credentials/log_analytics_credentials</auth_path>
    <tenantdomain>wazuh.com</tenantdomain>

    <request>
      <tag>azure-auditlogs</tag>
      <query>AuditLogs</query>
      <workspace>d6b...efa</workspace>
      <time_offset>1d</time_offset>
    </request>

  </log_analytics>
</wodle>
```

   Nerede:

- `<auth_path>`çalışma alanı gizli anahtarının saklandığı tam yoldur.
- `<tenantdomain>`kiracı etki alanı adıdır. Bunu Microsoft Entra ID'deki Genel Bakış bölümünden edinebilirsiniz.
- `<workspace>`kimlik doğrulaması için ihtiyaç duyduğunuz çalışma alanı kimliğidir.
- `<time_offset>`geriye doğru tarihlenen zaman dilimidir. Bu durumda, 24 saatlik bir zaman dilimi içindeki tüm günlükler indirilecektir.

2. Azure için Wazuh modülünü nerede yapılandırdığınıza bağlı olarak Wazuh sunucunuzu veya aracınızı yeniden başlatın.

   Wazuh temsilcisi:

   ```
   systemctl restart wazuh-agent
   ```

   Wazuh sunucusu:

   ```
   systemctl restart wazuh-manager
   ```

yukarıdaki yapılandırma, Wazuh'un tanımlayıcı olarak `tag` değeri kullanarak herhangi bir sorguyu aramasına olanak tanır .

Azure için Wazuh modülü hakkında daha fazla bilgi için referansı inceleyin .

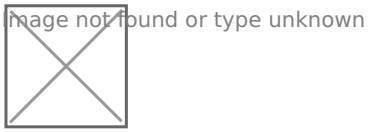
Use Case

Daha önce oluşturulmuş Azure uygulamasını kullanarak altyapı etkinliğinin izlenmesine dair bir örnek aşağıda verilmiştir.

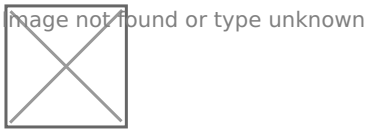
Bir Kullanıcı Oluşturma

Microsoft Entra ID'de kullanıcı oluşturmak için aşağıda belirtilen adımları izleyin:

1. **Entra ID'ye** gidin ve **Tüm kullanıcılar'ı** seçin.
2. **Yeni Kullanıcı'ya** tıklayın.

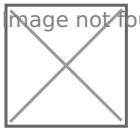


3. **Yeni kullanıcı oluştur** seçeneğini seçin.



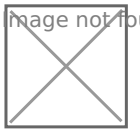
4. Oluşturmak istediğiniz kullanıcı için gerekli bilgileri girin ve ardından **Oluştur** seçeneğini

seçerek oluşturma işlemini tamamlayın.



Wazuh Dashboard Olayların Görselleştirilmesi

Kurulum tamamlandıktan sonra sonuçları Wazuh kontrol panelinden kontrol edebilirsiniz.



Microsoft Graph Servislerini Wazuh İle İzleme

Microsoft Graph API, Microsoft 365, Azure, Dynamics 365 ve diğer çeşitli Microsoft bulut bileşenleri dahil ancak bunlarla sınırlı olmamak üzere Microsoft bulut hizmetlerinin tüm paketindeki verilere erişim sağlayan kapsamlı bir API sistemidir. Microsoft Bulut ekosisteminden yapılandırılmış verilere, içgörülere ve zengin ilişkilere erişim için bir uç noktadır.

Bu bölümde, Microsoft Graph için Wazuh modülünü kullanarak kuruluşunuzun Microsoft Graph API kaynaklarını ve ilişkilerini izlemeye yönelik talimatlar verilmektedir.

Şu anda Microsoft Graph için Wazuh modülü Wazuh ile aşağıdakileri izlemenize olanak sağlıyor:

- Microsoft Entra Kimlik Koruması
- Microsoft 365 Savunucusu
- Bulut Uygulamaları için Microsoft Defender
- Microsoft Defender Uç Nokta İçin
- Kimlik için Microsoft Defender
- Office 365 için Microsoft Defender
- Microsoft Kapsamı eKeşif
- Microsoft Kapsamı Veri Kaybını Önleme (DLP)

Bunlar güvenlik kaynağı için temel olsa da, Microsoft Graph API'sini kullanarak birçok ek kaynağı izleyebilirsiniz. Daha fazla bilgi edinmek için Microsoft Graph belgelerine Genel Bakış'a bakın.

> Not: Güvenlik kaynağı, önceden oluşturulmuş kurallarla test edildiği için olgun olarak kabul edilebilir. Ancak, kuruluşunuz günlükleri diğer kaynaklardan Wazuh dağıtımınıza alabilir.

İçerik alınıyor

Microsoft Graph'tan bir dizi günlük almak için `GET`aşağıdaki URL'yi kullanarak bir istekte bulunun:

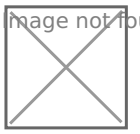
```
GET https://graph.microsoft.com/{version}/{resource}/{relationship}?{query-parameters}
```

Microsoft Graph API'nin mevcut üretim sürümünün açıklaması Microsoft Graph'a Genel Bakış'ta bulunabilir .

Alternatif olarak, API doğrudan Microsoft Graph Explorer aracılığıyla denenebilir .

Microsoft Azure Depolama

Microsoft Azure Storage, Microsoft Azure bulut depolama çözümünü ifade eder. Bu hizmet, veri nesneleri için büyük ölçüde ölçeklenebilir bir nesne deposu, güvenilir mesajlaşma için bir mesajlaşma deposu, bulut için bir dosya sistemi hizmeti ve bir NoSQL deposu sağlar.



Azure Log Analytics REST API'sine alternatif olarak Wazuh, bir Microsoft Azure Depolama hesabına erişim sunar. Microsoft Azure altyapısının etkinlik günlüklerini depolama hesaplarına aktarabilirsiniz.

Bu bölümde, Microsoft Azure etkinlik günlüklerinizi bir depolama hesabında arşivlemek için Azure portalının nasıl kullanılacağı açıklanmaktadır.

Yapılandırma

Azure

Etkinlik Günlüğü Dışa Aktarımını Yapılandırma

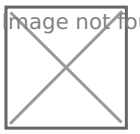
1. **Microsoft Entra ID** içerisindeki **İzleme bölümünden Denetim Günlükleri** seçeneğini seçin ve **Veri Ayarlarını Dışa Aktar'a** tıklayın.



2. **Tanılama ayarı ekle'ye** tıklayın.

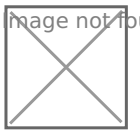


3. **Denetim Günlükleri'ni** seçin ve **Depolama hesabına arşivleyin** onay kutusunu seçin , ardından açılır menüden günlükleri dışa aktarmak istediğiniz aboneliği ve Depolama hesabını seçin.



Wazuh Sunucusu veya Agent

`account_name`Depolama hesabının ve'sini kimlik doğrulaması için ayarlamak önemlidir `account_key`. Aşağıdaki görüntü önceden yapılandırılmış bir depolama hesabını gösterir.



Microsoft Azure Depolama kimlik bilgilerini yapılandırma konusunda rehberlik için kimlik bilgileri bölümünü kontrol edin .

1. `/var/ossec/etc/ossec.conf`Aşağıdaki yapılandırmayı Wazuh sunucusunun veya aracısının yerel yapılandırma dosyasına uygulayın . Bu, Wazuh modülünü Azure için nerede yapılandırdığınıza bağlı olacaktır:

```
<wodle name="azure-logs">

  <disabled>no</disabled>
  <interval>1d</interval>
  <run_on_start>yes</run_on_start>

  <storage>

      <auth_path>/home/manager/Azure/storage_auth.txt</auth_path>
      <tag>azure-activity</tag>

      <container name="insights-activity-logs">
        <blobs>.json</blobs>
        <content_type>json_inline</content_type>
        <time_offset>24h</time_offset>
        <path>info-logs</path>
      </container>

  </storage>
</wodle>
```

Nerede

- `<auth_path>`çalışma alanı gizli anahtarının saklandığı tam yoldur.
- `<container>`blog depolama içeriklerini getirirken yararlı parametreler içerir.
- `<container name="insights-activity-logs">`Akışı yapılacak günlük kabı.
- `<blobs>.json</blobs>`indirilecek blob formatıdır.
- `<time_offset>`geriye doğru tarihlenen zaman dilimidir. Bu durumda, 24 saatlik bir zaman dilimi içindeki tüm günlükler indirilecektir.
- `<content_type>`blob'ların içeriğinin depolanması için kullanılan formattır.

2. Azure için Wazuh modülünü nerede yapılandırdığınıza bağlı olarak Wazuh sunucunuzu veya aracınızı yeniden başlatın.

   Wazuh temsilcisi:

   ```
   systemctl restart wazuh-agent
   ```

   Wazuh sunucusu:

   ```
   systemctl restart wazuh-manager
   ```

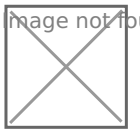
Kullanım Durumu

Yukarıdaki yapılandırmayı kullanarak Microsoft Entra ID etkinlik izleme örneğini aşağıda bulabilirsiniz.

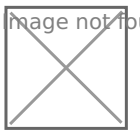
Yeni Bir Kullanıcı Oluştur

Microsoft Entra ID kullanarak Microsoft Azure ortamınızda yeni bir kullanıcı oluşturun. Kullanıcıyı oluşturduktan birkaç dakika sonra, `insights-activity-logs`Activity log export'u yapılandırılırken belirtilen Storage hesabının içinde adlandırılan bir kapsayıcıda yeni bir günlük kullanılabilir olacaktır.

Lütfen Azure Log Analytics kullanım örneği altında kullanıcı oluşturma bölümüne bakın .



Sonuçları Wazuh panelinden kontrol edebilirsiniz.



Microsoft Grafiği

Bu bölümde, Microsoft Graph REST API'yi kullanarak Microsoft Entra ID etkinliğinizi nasıl izleyeceğinizi öğreneceksiniz. Bu bölüm şunları içerir:

- Azure yapılandırması
- Wazuh yapılandırması
- Microsoft Entra ID kullanım örneği

Aşağıda Microsoft Entra ID'deki denetim ve izleme faaliyetleriyle ilgili Microsoft Graph REST API'sindeki uç noktalar yer almaktadır.

Rapor türü	**Sorgu**
Dizin denetimleri	`auditLogs/directoryaudits`
Oturum açmalar	`auditLogs/signIns`
Tedarik	`auditLogs/provisioning`

Bu uç noktalar, yöneticilerin ve geliştiricilerin güvenlik, uyumluluk ve operasyonel amaçlar doğrultusunda Microsoft Entra ID içindeki etkinlikleri izlemesine ve denetlemesine olanak tanır.

Wazuh, yukarıdaki uç noktaları kullanarak Microsoft Entra ID etkinlik raporlarını işleyebilir. Her biri farklı bir sorgu yürütmenizi gerektirir. Bu sorguları Azure yapılandırması için Wazuh modülünüzün komut bloğuna yerleştireceksiniz .

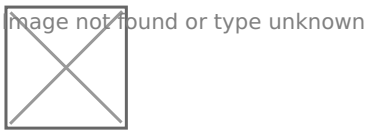
Yapılandırma

Azure

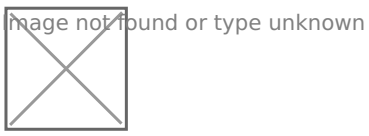
Uygulamanın Oluşturulması

Bu bölüm Azure Log Analytics REST API'sini kullanarak bir uygulama oluşturmayı açıklar. Ancak, mevcut bir uygulamayı yapılandırmak da mümkündür. Bu durumda, bu adımı atlayın.

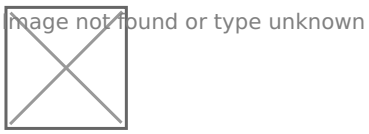
1. **Microsoft Entra ID** panelinde , **Uygulama kayıtları'nı** seçin . Ardından, **Yeni kayıt'ı** seçin.



2. Uygulamaya açıklayıcı bir ad verin, uygun **hesap türünü** seçin ve **Kaydol'a** tıklayın.

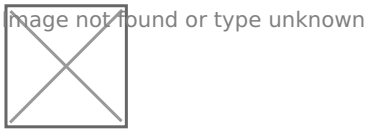


Uygulama artık kayıtlı.

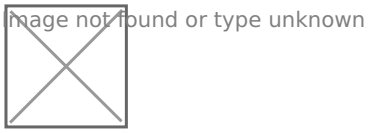


Uygulamaya İzinlerin Verilmesi

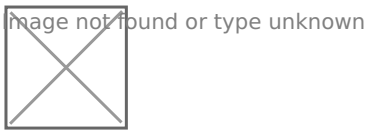
1. Uygulamaya tıklayın, **Genel Bakış** bölümüne gidin ve daha sonraki kimlik doğrulaması için **Uygulama (istemci) Kimliğini** kaydedin.



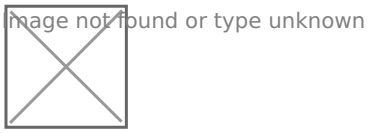
2. **API izinleri** bölümünde **İzin ekle** seçeneğini belirleyin.



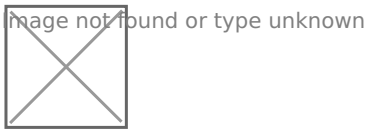
3. "*Microsoft Graph*"ı arayın ve API'yi seçin.



4. **Uygulamalar** izinlerinde altyapınızla uyumlu izinleri seçin . Bu durumda `AuditLog.Read.All` izinler verilecektir. Ardından **İzinleri ekle'ye** tıklayın.



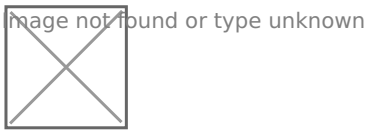
5. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.



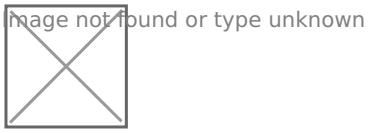
Kimlik Doğrulama İçin Uygulama Anahtarının Alınması

Log Analytics API'yi günlükleri almak için kullanmak üzere, Log Analytics API'yi doğrulamak için bir uygulama anahtarı üretmeliyiz. Uygulama anahtarını üretmek için aşağıdaki adımları izleyin.

1. **Sertifikalar ve sırlar'ı** seçin , ardından bir anahtar oluşturmak için **Yeni istemci sırrı'nı seçin.**

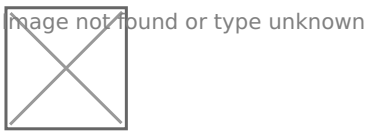


2. Uygun bir **açıklama** girin , anahtar için tercih edilen süreyi ayarlayın ve ardından **Ekle'ye** tıklayın.



3. Anahtar **değerini** kopyalayın . Bu daha sonra kimlik doğrulama için kullanılacaktır.

> Not: Bu sayfadan çıkmadan önce anahtarı kopyalayın, çünkü yalnızca bir kez görüntülenecektir. Sayfadan çıkmadan önce kopyalamazsanız, yeni bir anahtar oluşturmanız gerekecektir.



Wazuh Sunucusu veya Agent

Burada önceki adımlarda kaydedilen uygulamanın ve'sini `key`kullanacaksınız . Bu durumda, her iki alan da kimlik doğrulama için bir dosyaya kaydedildi. Bu konu hakkında daha fazla bilgi için Azure kimlik bilgilerini yapılandırma bölümüne bakın.`ID`

1. `/var/ossec/etc/ossec.conf`Aşağıdaki yapılandırmayı Wazuh sunucusunun veya aracısının yerel yapılandırma dosyasına uygulayın . Bu, Wazuh modülünü Azure için nerede yapılandırdığınıza bağlı olacaktır:

```
<wodle name="azure-logs">
  <disabled>no</disabled>
  <wday>Monday</wday>
```

```
  <time>2:00</time>
  <run_on_start>no</run_on_start>

  <graph>
    <auth_path>/var/ossec/wodles/azure/credentials</auth_path>
    <tenantdomain>wazuh.com</tenantdomain>
    <request>
       <tag>microsoft-entra_id</tag>
       <query>auditLogs/directoryAudits</query>
       <time_offset>1d</time_offset>
    </request>
  </graph>

</wodle>
```

Nerede:

- `<auth_path>`çalışma alanı gizli anahtarının saklandığı tam yoldur.
- `<tenantdomain>`kiracı etki alanı adıdır. Bunu Microsoft Entra ID'deki **Genel Bakış** bölümünden edinebilirsiniz
- `<wday>`tarama için planlanan haftanın günü nedir
- `<query>`Denetim günlüklerinin saklandığı yoldur.
- `<time>`tarama için planlanan zamandır.
- `<time_offset>`' a ayarlandığında `1d`, yalnızca son güne ait günlük verileri ayrıştırılır.

2. Azure için Wazuh modülünü nerede yapılandırdığınıza bağlı olarak Wazuh sunucunuzu veya aracınızı yeniden başlatın.

   Wazuh temsilcisi:

   ```
   systemctl restart wazuh-agent
   ```

   Wazuh sunucusu:

   ```
   systemctl restart wazuh-manager
   ```

Farklı kullanılabilir parametreleri kullanma hakkında daha fazla bilgi için Azure referansı için Wazuh modülünü kontrol edin . Microsoft Entra kimliğinizi izlemek için kimlik bilgilerini nasıl ayarlayacağınıza dair rehberlik için lütfen Wazuh Azure kimlik doğrulama dosyası bölümüne bakın.

> Uyarı: Alan zorunludur. Bunu **Microsoft Entra ID'deki Genel Bakış** bölümünden `tenantdomain`edinebilirsiniz .

Kullanım Durumu

Microsoft Entra ID'yi İzleme

Microsoft Entra ID, temel dizin hizmetlerini, uygulama erişim yönetimini ve kimlik korumasını tek bir çözümde birleştiren kimlik ve dizin yönetim hizmetidir.

Wazuh, Microsoft Graph REST API tarafından sağlanan etkinlik raporlarını kullanarak Microsoft Entra ID (ME-ID) hizmetini izleyebilir . Microsoft Graph API, Microsoft Entra ID uygulamalarındaki dizin verileri ve nesneler üzerinde okuma işlemleri gerçekleştirebilir.

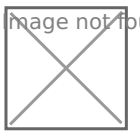


Yukarıdaki yapılandırmayı kullanarak Microsoft Entra ID etkinlik izleme örneğini aşağıda bulabilirsiniz.

Yeni Bir Kullanıcı Oluştur

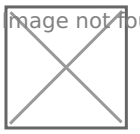
Azure'da yeni bir kullanıcı oluşturun. Başarılı bir kullanıcı oluşturma etkinliği bunu yansıtacak bir günlük üretecektir. Bu günlüğü auditLogs/directoryAudits sorgusunu kullanarak alabilirsiniz.

1. **Kullanıcılar** > **Tüm kullanıcılar'a** gidin , **Yeni kullanıcı** > **Yeni kullanıcı oluştur'u** seçin.

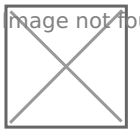


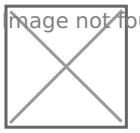
2. Gerekli bilgileri girin ve **İncele + oluştur'a** tıklayın . Kullanıcı artık oluşturuldu.

Başarılı kullanıcı oluşturma sonucunu **Microsoft Entra ID'nin Denetim günlükleri** bölümünden kontrol edebilirsiniz .



Entegrasyon çalışmaya başladığında, sonuçlar **Wazuh panosunun** Güvenlik **Olayları** sekmesinde mevcut olacaktır.





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

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
   Image not found or type unknown

   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
   Image not found or type unknown

   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
   Image not found or type unknown

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
   Image not found or type unknown

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
   Image not found or type unknown

   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 aktarmaları yapılandırın
   Image not found or type unknown

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.



Duruş Yönetimi Sonucu

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



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.

Office 365'i İzleme

Office 365, Microsoft tarafından sunulan, Word, Excel, PowerPoint, Outlook, OneDrive, Teams ve SharePoint gibi uygulamalar dahil olmak üzere bir dizi üretkenlik ve işbirliği aracına erişim sağlayan bulut tabanlı bir hizmettir. İzleme Office 365, araç paketinde gerçekleşen eylemlere ilişkin görünürlük ve veri görselleştirmesi sağlar.

Office 365 Denetim Günlüklerinin İzlenmesi

Office 365 denetim günlüğü, kuruluş yöneticilerinin kuruluşunuzun üyeleri tarafından gerçekleştirilen eylemleri hızla incelemesine olanak tanır. Oturum açan kullanıcı, eylemi kimin gerçekleştirdiği, gerçekleştirilen eylemin türü ve eylemin gerçekleştirildiği zaman gibi ayrıntıları içerir.

Bu bölüm, kuruluşunuz için Office 365 denetim günlüğünü izleme talimatları sağlar. Denetim günlüğü, Office 365 ortamında gerçekleşen değişiklikler ve kullanıcı etkinlikleri hakkında bilgi sağlar. Wazuh, Office 365'te aşağıdaki etkinlikleri izlemenize olanak tanır:

- SharePoint Online ve OneDrive İş'teki kullanıcı etkinliği.
- Exchange Online'daki kullanıcı etkinliği (Exchange posta kutusu denetim günlüğü).
- SharePoint Online'da yönetici etkinliği.
- Azure Active Directory'deki (Office 365 için dizin hizmeti) yönetici etkinliği.
- Exchange Online'daki yönetici etkinliği (Exchange yönetici denetim günlüğü).
- Güvenlik ve uyumluluk merkezinde eKeşif faaliyetleri.
- Kullanıcı ve yönetici etkinliği:
  - Güç BI.
  - Microsoft Teams.
  - Dinamikler 365.
  - Yavşak.
  - Microsoft Power Otomatikleştirin.
  - Microsoft Stream.
  - Microsoft İşyeri Analitiği.
  - Microsoft Güç Uygulamaları.
  - Microsoft Formları.
- SharePoint Online veya Microsoft Teams kullanan siteler için hassasiyet etiketlerine ilişkin kullanıcı ve yönetici etkinliği.
- Briefing e-postasında ve MyAnalytics'te yönetici etkinliği.

Office 365 Yönetim Etkinliği API'si

Office 365 Yönetim API'leri, hizmet iletişimleri, güvenlik, uyumluluk, raporlama ve denetim dahil olmak üzere çeşitli yönetim görevleri için bir platform sağlar. Office 365 ortamından denetim günlükleri toplamak için bir arayüz sunar. Wazuh, bu arayüzü kullanarak Office 365'ten denetim

günlükleri toplar.

Office 365 Yönetim Etkinliği API'si, eylemleri ve olayları her kuruluşun Office 365 ortamına göre uyarlanmış yapılandırılmış veriler olan kiracıya özgü içerik blob'larında toplar. Bu içerik blob'ları, bilgileri içerdikleri içeriğin türüne ve kaynağına göre sınıflandırır ve kuruluşların güvenlik denetimi, uyumluluk izleme ve diğer yönetim amaçları için Office 365 kiracılarındaki eylemleri ve olayları izlemelerine ve analiz etmelerine olanak tanır.

Planlara Dayalı Etkinlik API İşlemleri

Office 365 Yönetim Etkinliği API'si, kuruluşların farklı Office 365 hizmetlerinden denetim günlüklerine ve etkinlik verilerine erişmesini ve bunları bütünleştirmesini sağlayan bir RESTful API'dir. Etkinlikleri ilişkili hizmetlerine göre kategorilere ayırır ve Office 365 paketindeki geniş bir hizmet yelpazesini kapsar. Kullanılabilir belirli etkinlikler, Office 365 abonelik planınıza ve etkinleştirdiğiniz hizmetlere bağlıdır.

Tüm API işlemleri tek bir kiracıyla sınırlıdır ve API'nin kök URL'si kiracı bağlamını belirten bir kiracı kimliği içerir. Kullandığınız API uç noktasının URL'si, kuruluşunuz için Office 365 abonelik planının türüne dayanır. İşte kullanılabilir planların listesi ve bunlara karşılık gelen API uç noktası URL'leri.

- İşletme planı

  `https://manage.office.com/api/v1.0/{tenant_id}/activity/feed/{operation}`

- Hükümet Topluluk Bulutu (GCC) hükümet planı

  `https://manage-gcc.office.com/api/v1.0/{tenant_id}/activity/feed/{operation}`

- Hükümet Topluluk Bulutu (GCC) Yüksek hükümet planı

  `https://manage.office365.us/api/v1.0/{tenant_id}/activity/feed/{operation}`

- Savunma Bakanlığı (DoD) hükümet planı

  `https://manage.protection.apps.mil/api/v1.0/{tenant_id}/activity/feed/{operation}`

Office 365 abonelik planları farklı özellikler ve hizmetler içerebilir, bu nedenle kullanılabilir etkinlikler belirli planınıza göre değişebilir. Ortak Office 365 planlarına ve hizmetlerine bağlı olarak Office 365 Yönetim API'sinde bulabileceğiniz bazı etkinlik kategorileri şunlardır:

- **Azure Active Directory (Azure AD) etkinlikleri** - Azure AD'de kullanıcıların ve grupların oluşturulması, değiştirilmesi veya silinmesiyle ilgili olaylar. Bu, oturum açmaları, kimlik doğrulama olaylarını ve rol atamalarını ve değişikliklerini de içerir.
- **Exchange Online etkinlikleri** : Bunlara e-postayla ilgili etkinlikler, posta kutusu izin değişiklikleri ve e-posta özelliklerinde, eklerde ve klasörlerde yapılan değişiklikler dahildir.
- **SharePoint Online etkinlikleri** : Bu kategori, belge ve site paylaşımı, kullanıcı erişim hakları ve izin değişiklikleri ve dosya ve klasör işlemleriyle ilgili etkinlikleri içerir.

- **Microsoft Teams etkinlikleri** : Kanal ve ekip yönetimi, mesaj ve sohbet işlemleri ve toplantıyla ilgili etkinliklerle ilgili etkinlikler.
- **Güvenlik ve Uyumluluk Merkezi etkinlikleri** : Bu kategori, uyumluluk politikaları ve veri kaybı önleme (DLP) ile ilgili olayları içerir. Ayrıca politika ihlalleri ve eDiscovery etkinlikleri için uyarıları da içerir.
- **Genel aktiviteler** : Belirli hizmet kategorilerine girmeyen etkinlikler. Bu kategori genel değişiklikleri ve idari aktiviteleri içerebilir.

Office 365 Yönetim Etkinlik API'si çeşitli işlemleri destekler. Bunlar arasında bildirimleri almak için bir abonelik başlatmak, bir kiracı için etkinlik verilerini almak ve bir kiracı için veri alımını durdurmak için bir aboneliği durdurmak yer alır. Etkinlik API'sini kullanarak geçerli abonelikleri, kullanılabilir içeriği ve karşılık gelen içerik URL'lerini listeleyebilirsiniz. Ayrıca içerik URL'sini kullanarak içerik alabilirsiniz.

Aşağıda, Activity API'nin kullanılabilir içerikleri listelemek ve içerik işlemlerini almak için nasıl kullanılacağını gösteriyoruz.

- **Mevcut içerik listeleniyor**
  Belirli bir içerik türü için şu anda alınabilecek içeriği listeleyebilirsiniz. Bu içerik, bir Office 365 ortamında gerçekleşen eylem ve olayların bir koleksiyonunu oluşturur. Kullanılabilir içeriği almak için Microsoft, bir Office 365 kurumsal planı kullanırken verileri almak için aşağıdaki API uç noktasını sağlar:
  `Get https://manage.office.com/api/v1.0/<Tenant_ID>/activity/feed//subscriptions/content?contentType=<Cor`

  Nerede:
  - Değişken `<Tenant_ID>`, aboneliğin kiracı kimliğidir.
  - Değişken `<ContentType>`içerik türünü belirtir. Örneğin, `Audit.AzureActiveDirectory`ve `Audit.General`.
  - `<START_TIME>`ve değişkenleri, `<END_TIME>`içeriğin ne zaman kullanılabilir hale geldiğine bağlı olarak döndürülecek içeriğin zaman aralığını belirtir (tarih biçimi: YYYY-AA-GG).

  Aşağıdaki adımları izleyerek belirtilen içerik türü için şu anda alınabilecek içerikleri manuel olarak listeleyebilirsiniz.
  1. Aşağıdaki PowerShell betiğini kullanarak bir erişim belirteci oluşturun. Bir dosya oluşturun `AccessToken.ps1`, ardından aşağıdaki içerikleri oluşturulan dosyaya kopyalayıp yapıştırın. `<YOUR_APPLICATION_ID>`, `<YOUR_CLIENT_SECRET>`, ve `<YOUR_TENANT_ID>`değerlerini uygulama kaydı sırasında toplanan doğru değerlerle değiştirin:

     ```
     $clientId = "<YOUR_APPLICATION_ID>"
     $clientSecret = "<YOUR_CLIENT_SECRET>"
     $tenantId = "<YOUR_TENANT_ID>"
     $resource = "https://manage.office.com"

     $tokenEndpoint = "https://login.microsoftonline.com/$tenantId/oauth2/token"
     $tokenRequestBody = @{
        grant_type    = "client_credentials"
        client_id     = $clientId
     ```

```
    client_secret = $clientSecret
    resource      = $resource
}

$tokenResponse = Invoke-RestMethod -Uri $tokenEndpoint -Method POST -Body $tokenRequestBody
$MyToken = $tokenResponse.access_token
echo $MyToken
```

2. `AccessToken.ps1`Normal bir PowerShell terminali açın ve önceki adımda oluşturulan PowerShell betiğini çalıştırmak için aşağıdaki komutları çalıştırın :

```
> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
> $accessToken = <PATH>/AccessToken.ps1
```

> Not: `Set-ExecutionPolicy RemoteSigned -Scope CurrentUser` komudu yerel betiklerin yürütülmesine izin vermek için kullanılır. PowerShell betiğinin `<PATH>` dosya yoluyla değiştirin.

3. Aynı PowerShell terminalinde aşağıdaki komutu çalıştırarak bir içerik türü için şu anda mevcut olan içeriklerin listesini alabilirsiniz:

```
Invoke-RestMethod -Uri "https://manage.office.com/api/v1.0/<TENANT_ID>/activity/feed/subscriptions/con
```

   Yer değiştirmek:
   - `<TENANT_ID>`Geçerli kiracı kimliğine sahip değişken .
   - Geçerli bir içerik türüne sahip değişken `<CONTENT_TYPE>`. Örneğin `Audit.AzureActiveDirectory`
   - `<START_TIME>`ve tarih aralığına sahip değişkenler `<END_TIME>`(biçim: YYYY-AA-GG)

   Output

```
contentUri       : https://manage.office.com/api/v1.0/<Tenant_ID>/activity/feed/audit/2024012907324710
contentId        : 20240129073247100003384$20*********081955691028239$audit_azureactivedirectory$
contentType      : Audit.AzureActiveDirectory
contentCreated   : 2024-01-29T08:19:55.691Z
contentExpiration : 2024-02-05T07:32:47.100Z
...
```

- **İçerik alınıyor**
  Bir içerik blob'unu almak için, kullanılabilir içerik listesinde bulunan ilgili içerik URI'sine karşı bir GET isteği yapın. Döndürülen içerik, JSON biçiminde bir veya daha fazla eylem veya olayın bir koleksiyonu olacaktır.

```
GET <CONTENT_URI>
```

  `<CONTENT_URI>`Değişkeni, kullanılabilir içerik listesinde bulunan bir içerik URI'sinin değeriyle değiştirin .

Office 365 Yönetim API belgeleri, kullanılabilir uç noktalar ve yanıt biçimleri hakkında ayrıntılar sağlar. Daha fazla bilgi için belgelere başvurabilirsiniz.

Office 365 API Gereksinimleri

Wazuh'un analiz için denetim günlüklerini bağlamak ve çekmek için Office 365 Yönetim API'sine kimlik doğrulaması yapması gerekir. Bu işlem, gerekli kimlik bilgilerini almak için bir uygulamayı Microsoft Azure portalına kaydederek gerçekleştirilir.

Office 365 with Wazuh'un denetim günlüklerine erişmek için aşağıdaki gereksinimlere ihtiyacınız var:

- **Uygulama (istemci) kimliği** : Office 365'ten günlükleri çekmek için Microsoft Azure portalında oluşturulan uygulamanın benzersiz kimliği.
- **Dizin (kiracı) kimliği** : Kuruluş kimliğiyle aynı olan kiracı kimliği, uygulamanın hangi Azure Active Directory örneğinin altında bulunduğunu tanımlar.
- **İstemci sırrı** : Hem uygulama hem de yetkilendirme sunucusunun bildiği paylaşılan bir sır.

Office 365'i İzleme İçin Ayarlama

Office 365 API, Office 365'teki denetim günlüklerine erişim için bir uç nokta sağlar. Microsoft API'sine erişmek için doğru izinlere sahip bir uygulamaya ihtiyacınız var. Aşağıdaki liste, Wazuh ile bütünleşmek için Microsoft Azure'da gerçekleştirmeniz gereken adımların bir özetini sunar:

- **Microsoft Azure portalı üzerinden bir uygulama kaydetme** : Bu adım, kuruluşunuzda benzersiz kimlik bilgileriyle (istemci kimliği, kiracı kimliği ve istemci sırrı) bir uygulama oluşturmayı içerir.
- **Sertifikalar ve sırlar oluşturma** : Oluşturulan uygulamanın güvenliği sağlamak için Office 365 Yönetim API'sine kimlik doğrulaması yapması gerekir. Bu adım, uygulama için sertifikaların ve sırların nasıl oluşturulacağını gösterir.
- **API izinlerini etkinleştirme** : Oluşturulan uygulamanın Office 365 etkinlik olaylarını istemek için belirli API izinlerine ihtiyacı vardır. Bu adım, Office 365 Yönetim API'sinden günlükleri çekmek için gereken uygun izinlerin nasıl atanacağını gösterir.

Azure Portalı Üzerinden Bir Uygulamayı Kaydetme

Microsoft kimlik platformu uç noktasıyla kimlik doğrulaması yapmak için Azure portalınızda bir uygulama kaydetmeniz gerekir .

1. Azure portalınızda oturum açın .

2. Microsoft Azure portal uygulaması kayıtları bölümünde **Yeni kayıt'a** tıklayın.

Azure yeni uygulama kaydı

3. Başvurunuzun adını girin, istediğiniz hesap türünü seçin ve **Kayıt Ol** butonuna tıklayın.

Azure - Uygulamayı kaydet

   Bu noktada başvurunuz kayıt altına alınmış olur.

4. Uygulamaları ve ID'leri görüntülemek ve kopyalamak için menüdeki **Genel Bakış** sekmesine tıklayın . `client` `tenant`

Azure - Genel bakışta istemci ve kiracı kimlikleri

Sertifikalar ve Sırlar Oluşturma

Uygulama, kimlik doğrulama işlemi sırasında bir sertifika ve gizli bilginin kullanılmasını gerektirir.

1. **Sertifikalar ve sırlar** menüsüne gidin ve **Yeni istemci sırrı** düğmesine tıklayın . Ardından, **İstemci sırrı ekle** bölümünün altındaki yeni sırrın **Açıklama** ve **Son Kullanma Tarihi** alanlarını doldurun.

Azure - Sertifikalar ve sırlar

2. Gizli bilginin değerini **İstemci gizli bilgileri** bölümünün altına kopyalayıp kaydedin.

Azure - İstemci sırları değeri

> Not: Bunu mutlaka not edin çünkü web arayüzü daha sonra kopyalamanıza izin vermeyecektir.

API İzinlerini Etkinleştirme

Uygulamanın Office 365 etkinlik olaylarını istemek için belirli API izinlerine ihtiyacı vardır.

Uygulama izinlerini yapılandırmak için aşağıdaki adımları izleyin:

1. **API izinleri** menüsüne gidin ve **İzin ekle'yi** seçin .
   - **Office 365 Yönetim API'lerini** seçin ve **Uygulama izinleri'ne** tıklayın .
   - **ActivityFeed** grubunun altına aşağıdaki izinleri ekleyin :
     - `ActivityFeed.Read`: Kuruluşunuza ait etkinlik verilerini okuyun.
     - `ActivityFeed.ReadDlp`: Tespit edilen hassas veriler de dahil olmak üzere DLP politika olaylarını okuyun.

- **İzinleri ekle** butonuna tıklayın.

Azure – API izinlerini isteyin



> Not: API izin değişiklikleri için yönetici onayı gereklidir.

Azure – API izin değişiklikleri için yönetici onayı



Office 365 İzleme İçin Wazuh'u Kurma

Bu bölüm, Office 365 ortamlarının etkili bir şekilde izlenmesi için Wazuh'un yapılandırılmasında yer alan süreçleri ele alır. Yapılandırma sürecinin çeşitli yönleri arasında günlük toplama için Office 365 API'leriyle entegrasyon, Office 365 olayları için pano görselleştirme modülünün etkinleştirilmesi ve kuralların ilişkilendirilmesi yer alır.

Wazuh'u Office 365 API'leriyle Yapılandırma

Office 365 için Wazuh modülü, analiz ve kural ilişkilendirmesi için Office 365 API'lerinden denetim günlüklerini çeker. Modülü Wazuh sunucusunda veya Wazuh aracısında yapılandırabilirsiniz. Wazuh sunucusundaki iş yükünü azaltmak ve böylece izleme altyapınızın performansını iyileştirmek için Wazuh aracısında yapılandırmanız önerilir.

Office 365 ortamından denetim günlüklerini çekmek üzere Wazuh sunucusunu yapılandırmak için aşağıdaki adımları uygulayın.

1. Aşağıdaki yapılandırmayı dosyaya ekleyin `/var/ossec/etc/ossec.conf`. Yapılandırma yalnızca . `Audit.SharePoint`aralığındaki olay türlerini çeker `1m`.

```
<ossec_config>
  <office365>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID></tenant_id>
      <client_id><YOUR_CLIENT_ID></client_id>
      <client_secret><YOUR_CLIENT_SECRET></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <subscriptions>
      <subscription>Audit.SharePoint</subscription>
    </subscriptions>
  </office365>
```

```
</ossec_config>
```

Nerede:

- `<enabled>`Office 365 için Wazuh modülünü etkinleştirir. Bu seçenek için izin verilen değerler `yes`ve'dir `no`.
- `<interval>`Office 365 için Wazuh modülünün her yürütülmesi arasındaki zaman aralığını tanımlar. İzin verilen değer, `s`(saniye), `m`(dakika), `h`(saat) ve `d`(gün) gibi bir zaman birimini belirten bir sonek karakteri içeren herhangi bir pozitif sayıdır. Belirtilmezse modül yürütmesi için varsayılan aralık `10m`.
- `<curl_max_size>b/B`Microsoft API yanıtı için izin verilen maksimum boyutu belirtir. İzin verilen değer , (bayt), `k/K`(kilobayt), `m/M`(megabayt) ve (gigabayt) gibi bir boyut birimini belirten bir sonek karakteri içeren herhangi bir pozitif sayıdır `g/G`. Varsayılan değer `1M`.
- `<only_future_events>`Office 365 için Wazuh modülünü, değer olarak ayarlandığında yalnızca Wazuh yöneticisini başlattıktan sonra oluşturulan olayları toplayacak şekilde belirtir `yes`. Değer olarak ayarlandığında hayır, Wazuh yöneticisini başlatmadan önce oluşturulan önceki olayları toplar. Varsayılan değer 'dir `yes`ve izin verilen değerler `yes` ve'dir `no`.
- Blok , kimlik doğrulaması için kimlik bilgilerini Office 365 REST API ile yapılandırır. , , ve `<api_auth>`etiketleri, içindeki yapılandırma etiketleridir .`<tenant_id>` `<client_id>``<client_secret>``<api_type>``<api_auth>`
  - `<tenant_id>`Azure'da kayıtlı uygulamanın kiracı kimliğini belirtir. İzin verilen değer herhangi bir dizedir. Değişkeni, `<YOUR_TENANT_ID>`Azure'da kayıtlı uygulamanızın kiracı kimliğiyle değiştirin.
  - `<client_id>`Azure'da kayıtlı uygulamanın istemci kimliğini belirtir. İzin verilen değer herhangi bir dizedir. Değişkeni, `<YOUR_CLIENT_ID>`Azure'da kayıtlı uygulamanızın istemci kimliğiyle değiştirin.
  - `<client_secret>`Azure'da kayıtlı uygulamanın istemci gizli değerini belirtir. Değişkeni, `<YOUR_CLIENT_SECRET>`Azure'da kayıtlı uygulamanızın istemci gizli değeriyle değiştirin.
  - `<api_type>`kiracı tarafından kullanılan Office 365 abonelik planının türünü belirtir. İzin verilen abonelikler `commercial`, `gcc`, ve 'dir `gcc-high`.
- Blok `<subscriptions>`, Office 365 REST API'sindeki dahili seçenekleri yapılandırır.
  - `<subscription>`Wazuh'un denetim günlüklerini topladığı içerik türlerini belirtir. Yapılandırılabilen abonelik türleri`Audit.AzureActiveDirectory` arasında , `Audit.Exchange`, `Audit.SharePoint`, `Audit.General`ve bulunur `DLP.All`.

Yapılandırma seçenekleri hakkında daha fazla bilgi edinmek için lütfen Office 365 için Wazuh modülü başvuru kılavuzunu inceleyin.

2. Değişiklikleri uygulamak için Wazuh yönetici hizmetini yeniden başlatın:

```
systemctl restart wazuh-manager
```

Birden Fazla Kiracıyı Yapılandırma

`<tenant_id>`Wazuh'u, kuruluşun kimlik bilgilerini (, `<client_id>`, `<client_secret>`, ve `<api_type>`) ayrı bloklarda belirterek bir kuruluştaki birden fazla kiracıyı izleyecek şekilde yapılandırabilirsiniz `<api_auth>`.

Örneğin, aşağıdaki yapılandırma bir kuruluştaki iki kiracıyı izler:

```
<ossec_config>
  <office365>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID_1></tenant_id>
      <client_id><YOUR_CLIENT_ID_1></client_id>
      <client_secret><YOUR_CLIENT_SECRET_1></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID_2></tenant_id>
      <client_id><YOUR_CLIENT_ID_2></client_id>
      <client_secret><YOUR_CLIENT_SECRET_2></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <subscriptions>
      <subscription>Audit.AzureActiveDirectory</subscription>
      <subscription>Audit.General</subscription>
    </subscriptions>
  </office365>
</ossec_config>
```

Yer değiştirmek:

- `<YOUR_TENANT_ID_1>`, `<YOUR_CLIENT_ID_1>`, ve `<YOUR_CLIENT_SECRET_1>`kiracı 1'in kuruluş bilgileriyle birlikte.
- `<YOUR_TENANT_ID_2>`, `<YOUR_CLIENT_ID_2>`, ve `<YOUR_CLIENT_SECRET_2>`kiracı 2'nin kuruluş bilgileriyle birlikte.

Birden Fazla Aboneliği Yapılandırma

Wazuh, Office 365'teki aşağıdaki abonelik türlerinden denetim günlüklerini çeker:

- **Audit.AzureActiveDirectory** : Kullanıcı kimliği yönetimi.
- **Audit.Exchange** : E-posta ve takvim sunucusu.
- **Audit.SharePoint** : Web tabanlı işbirliği platformu.
- **Denetim.Genel** : Önceki içerik türlerinde yer almayan diğer tüm iş yüklerini içerir.
- **DLP.All** : Veri kaybını önleme iş yükleri.

`<subscription>`Aynı bloktaki ayrı etiketlerde abonelik türünü belirterek Wazuh'u bir kuruluş kiracısındaki birden fazla aboneliği izleyecek şekilde yapılandırabilirsiniz `<subscriptions>`.

Örneğin, aşağıdaki yapılandırma yalnızca bir kuruluştaki bir kiracı içindeki olayların `Audit.AzureActiveDirectory`ve türlerini çeker:`Audit.General`

```
<ossec_config>
  <office365>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID></tenant_id>
      <client_id><YOUR_CLIENT_ID></client_id>
      <client_secret><YOUR_CLIENT_SECRET></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <subscriptions>
      <subscription>Audit.AzureActiveDirectory</subscription>
      <subscription>Audit.General</subscription>
    </subscriptions>
  </office365>
</ossec_config>
```

`<YOUR_TENANT_ID>`, `<YOUR_CLIENT_ID>`, ve `<YOUR_CLIENT_SECRET>`ifadelerini kiracıya ait kuruluş kimlik bilgileriyle değiştirin.

Office 365 Etkinliğini Görselleştirme

Wazuh panosu, Office 365'te gerçekleşen olaylar hakkında ayrıntılı bilgi ve içgörüler sağlayan bir Office 365 modülüne sahiptir. Modül üç görselleştirme seçeneği sunar.

- **Dashboard**
- **Panel**
- **Events**

Bunlardan herhangi birini seçmek için Wazuh panosunun **Bulut güvenliği** bölümündeki **Office 365 sekmesine gidin.**

Dashboard

Pano görselleştirme seçeneği, izlenen bir Office 365 ortamında gerçekleştirilen eylemlerin kapsamlı bir görünümünü sağlar. Bu bilgiler, aşağıdaki görüntüde görüldüğü gibi şüpheli indirmeleri, Tam Erişim İzinlerini, Kimlik Avı ve Kötü Amaçlı Yazılımları, Zamana göre önem sırasına göre Olayları, Kullanıcılara göre IP adresini, Coğrafi konum haritasını ve daha fazlasını içerir.



Office 365 panosu görselleştirme seçeneği

Panel

Bu görselleştirme seçeneği, hizmetin en önemli kullanıcıları, hizmeti kullanan en önemli istemci IP adresleri, tetiklenen en önemli kurallar ve Office 365'te gerçekleştirilen en önemli işlemler dahil olmak üzere gerçekleşen olay hakkında ayrıntılı bilgi sağlar.



Office 365 modül paneli

Events

Olay görselleştirme seçeneği, Office 365 ortamında meydana gelen olaylar tarafından oluşturulan uyarıları gösterir. Burada, aracı adı, bir kullanıcının gerçekleştirdiği işlem, bir eylemi gerçekleştiren kullanıcı, uyarının açıklaması, uyarının kural düzeyi ve daha fazla alan gibi ayrıntıları görebilirsiniz.

Bu görselleştirme ayrıca şunları içeren ek işlevler de sunar:

- Kural kimlikleri, kural grupları, IP adresleri ve diğerleri gibi belirli alanlara dayalı olay filtreleme.
- Yapılandırılmış sorgulara dayalı dinamik aramalar.
- Oluşturulan uyarının tam günlüğü, eşleşen kod çözücü ve diğerleri dahil olmak üzere tam ayrıntıları.



Office 365 etkinlik görselleştirme seçeneği

Aşağıdaki görselde gösterildiği gibi, uyarıyı tetikleyen olay hakkında ek bilgileri görüntülemek için her uyarı girişini genişletebilirsiniz.



Office 365 etkinlik görselleştirme seçeneği – Uyarıyı genişlet
Image not found or type unknown
Office 365 etkinlik görselleştirme seçeneği – Uyarıyı genişlet

Use Case'ler

Microsoft Azure AD'de Kullanıcı Oturum Açmanın Algılanması

Bir kullanıcı Microsoft Azure AD'de oturum açtığında, eylem bir olay oluşturur. Aşağıdaki eylemleri gerçekleştirerek Wazuh'u bu olayları izleyecek ve görselleştirecek şekilde yapılandırabilirsiniz:

1. Aşağıdaki yapılandırmayı `/var/ossec/etc/ossec.conf`Wazuh sunucusundaki dosyaya ekleyin:

```
<ossec_config>
  <office365>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID></tenant_id>
      <client_id><YOUR_CLIENT_ID></client_id>
      <client_secret><YOUR_CLIENT_SECRET></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <subscriptions>
      <subscription>Audit.AzureActiveDirectory</subscription>
    </subscriptions>
  </office365>
</ossec_config>
```

   Yer değiştirmek:
   - `<YOUR_TENANT_ID>`Microsoft Azure'da kayıtlı uygulamanızın kiracı kimliğinin bulunduğu değişken .
   - `<YOUR_CLIENT_ID>`Microsoft Azure'da kayıtlı uygulamanızın istemci kimliğinin bulunduğu değişken .
   - `<YOUR_CLIENT_SECRET>`Microsoft Azure'da kayıtlı uygulamanızın istemci sırrını içeren değişken .

2. Değişiklikleri uygulamak için Wazuh yönetici hizmetini yeniden başlatın:

```
systemctl restart wazuh-manager
```

3. Azure portalınıza giriş yapın .
4. Wazuh panosunu ziyaret edin ve **Office 365'e** gidin, ardından oluşturulan uyarıları görüntülemek için **Etkinlikler** sekmesine tıklayın.

Office 365 oturum açma uyarıları oluşturuldu

Image not found or type unknown

Oluşturulan uyarının JSON formatı aşağıdadır.


```
{
 "_index": "wazuh-alerts-4.x-2024.01.29",
 "_id": "vNQjVI0B9LTh695MXIMn",
 "_version": 1,
 "_score": null,
 "_source": {
  "input": {
   "type": "log"
  },
  "agent": {
   "name": "wazuh-server",
   "id": "000"
  },
  "manager": {
   "name": "wazuh-server"
  },
  "data": {
   "integration": "office365",
   "office365": {
    "AzureActiveDirectoryEventType": "1",
    "UserKey": "5a4603e7-100d-4fab-83c0-8dac779b2628",
    "ActorIpAddress": "102.244.157.118",
    "Operation": "UserLoggedIn",
    "OrganizationId": "0fea4e03-8146-453b-b889-54b4bd11565b",
    "ExtendedProperties": [
     {
      "Value": "Redirect",
      "Name": "ResultStatusDetail"
     },
     {
      "Value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
      "Name": "UserAgent"
     },
     {
      "Value": "OAuth2:Authorize",
      "Name": "RequestType"
     }
    ],
    "IntraSystemId": "aa9ef67e-5237-49e0-9d45-587d8afc1f00",
    "Target": [
     {
      "Type": 0,
      "ID": "5f09333a-842c-47da-a157-57da27fcbca5"
     }
    ],
    "RecordType": "15",
    "Version": "1",
    "ModifiedProperties": [],
```

```
    "Actor": [
     {
      "Type": 0,
      "ID": "5a4603e7-100d-4fab-83c0-8dac779b2628"
     },
     {
      "Type": 5,
      "ID": "XXXXXXX@wazuh.com"
     }
    ],
    "DeviceProperties": [
     {
      "Value": "Windows10",
      "Name": "OS"
     },
     {
      "Value": "Chrome",
      "Name": "BrowserType"
     },
     {
      "Value": "80ce5b15-c485-4128-a9ea-f9c0cdfb663d",
      "Name": "SessionId"
     }
    ],
    "Subscription": "Audit.AzureActiveDirectory",
    "ActorContextId": "0fea4e03-8146-453b-b889-54b4bd11565b",
    "ResultStatus": "Success",
    "ObjectId": "5f09333a-842c-47da-a157-57da27fcbca5",
    "ErrorNumber": "0",
    "ClientIP": "102.244.157.118",
    "Workload": "AzureActiveDirectory",
    "UserId": "XXXXXXX@wazuh.com",
    "TargetContextId": "0fea4e03-8146-453b-b889-54b4bd11565b",
    "CreationTime": "2024-01-29T07:29:21",
    "Id": "aa9ef67e-5237-49e0-9d45-587d8afc1f00",
    "InterSystemsId": "e0e158a5-202d-4e1f-bb93-873be484222d",
    "ApplicationId": "89bee1f7-5e6e-4d8a-9f3d-ecd601259da7",
    "UserType": "0"
   },
   "aws": {
    "accountId": "",
    "region": ""
   }
  },
  "rule": {
   "firedtimes": 1,
   "mail": false,
   "level": 3,
   "hipaa": [
    "164.312.a.2.I",
    "164.312.b",
    "164.312.d",
```

```
      "164.312.e.2.II"
     ],
     "pci_dss": [
      "8.3",
      "10.6.1"
     ],
     "description": "Office 365: Secure Token Service (STS) logon events in Azure Active Directory.",
     "groups": [
      "office365",
      "AzureActiveDirectoryStsLogon"
     ],
     "id": "91545"
    },
    "location": "office365",
    "decoder": {
     "name": "json"
    },
    "id": "1706513609.3469",
    "GeoLocation": {
     "city_name": "Sangmelima",
     "country_name": "Cameroon",
     "region_name": "South",
     "location": {
      "lon": XX.XX33,
      "lat": XX.XX33
     }
    },
    "timestamp": "2024-01-29T07:33:29.195+0000"
   },
   "fields": {
    "timestamp": [
     "2024-01-29T07:33:29.195Z"
    ]
   },
   "highlight": {
    "manager.name": [
     "@opensearch-dashboards-highlighted-field@wazuh-server@/opensearch-dashboards-highlighted-field@"
    ],
    "rule.groups": [
     "@opensearch-dashboards-highlighted-field@office365@/opensearch-dashboards-highlighted-field@"
    ]
   },
   "sort": [
    1706513609195
   ]
  }
```


Microsoft Azure AD'de Kullanıcı Hesaplarının Oluşturulmasını ve Silinmesini Algılama

Bu kullanım örneği, bir kullanıcı hesabının oluşturulması ve silinmesi de dahil olmak üzere Microsoft Azure AD'de (Office 365 için dizin hizmeti) yönetici etkinliklerinin nasıl izleneceğini gösterir.

Wazuh Sunucusu

Microsoft Azure AD'de yönetici etkinliklerini izlemek için Wazuh sunucusunu yapılandırmak üzere aşağıdaki adımları uygulayın.

1. Aşağıdaki yapılandırmayı `/var/ossec/etc/ossec.conf`Wazuh sunucusundaki dosyaya ekleyin:

```
<ossec_config>
  <office365>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <tenant_id><YOUR_TENANT_ID></tenant_id>
      <client_id><YOUR_CLIENT_ID></client_id>
      <client_secret><YOUR_CLIENT_SECRET></client_secret>
      <api_type>commercial</api_type>
    </api_auth>
    <subscriptions>
      <subscription>Audit.AzureActiveDirectory</subscription>
    </subscriptions>
  </office365>
</ossec_config>
```

   Yer değiştirmek:
   - `<YOUR_TENANT_ID>`Microsoft Azure'da kayıtlı uygulamanızın kiracı kimliğini içeren değişken .
   - `<YOUR_CLIENT_ID>`Microsoft Azure'da kayıtlı uygulamanızın istemci kimliğini içeren değişken .
   - `<YOUR_CLIENT_SECRET>`Microsoft Azure'da kayıtlı uygulamanızın istemci sırrını içeren değişken .

2. Değişiklikleri uygulamak için Wazuh yönetici hizmetini yeniden başlatın:

```
systemctl restart wazuh-manager
```

Microsoft Azure Portal

Wazuh'un panoda izleyip görüntüleyebileceği bir etkinlik oluşturmak için Microsoft Azure AD'de bir kullanıcı hesabı oluşturuyoruz ve siliyoruz.

Bir test kullanıcı hesabı oluşturmak ve silmek için aşağıdaki işlemleri gerçekleştirin.

1. Azure Active Directory artık Microsoft Entra ID'dir. Azure portalının Arama çubuğuna yazın ve AD'nize erişmek için üzerine tıklayın.Microsoft Entra ID
2. Yan menüden **Kullanıcılar'a** gidin ve **Yeni kullanıcı** > **Yeni kullanıcı oluştur'a** tıklayın .

Azure yeni kullanıcı oluştur

3. Kullanıcının bilgilerini doldurun ve **İncele + oluştur** butonuna tıklayarak kullanıcıyı oluşturun.

Azure İnceleme + Yeni kullanıcı oluştur

4. **Görünen adı seçip Sil** butonuna tıklayarak kullanıcıyı silin .

Azure kullanıcıyı sil

Wazuh Dashboard

Modüller > **Office 365'e** gidin ve oluşturulan uyarıları görüntülemek için **Etkinlikler** sekmesine tıklayın.

Azure hesap oluşturma/silme uyarıları

Aşağıda kullanıcı ekleme etkinliğinin JSON formatındaki örnek uyarısı yer almaktadır.


```
{
 "_index": "wazuh-alerts-4.x-2024.01.29",
 "_id": "0NRwVY0B9LTh695MClSi",
 "_version": 1,
 "_score": null,
 "_source": {
  "input": {
   "type": "log"
  },
  "agent": {
   "name": "wazuh-server",
   "id": "000"
  },
  "manager": {
   "name": "wazuh-server"
  },
  "data": {
   "integration": "office365",
   "office365": {
    "AzureActiveDirectoryEventType": "1",
    "ResultStatus": "Success",
    "ObjectId": "testuser@wazuh.com",
```

```
"UserKey": "10032002120F5B41@wazuh.com",
"Operation": "Add user.",
"OrganizationId": "0fea4e03-8146-453b-b889-54b4bd11565b",
"ExtendedProperties": [
  {
    "Value": "{}",
    "Name": "additionalDetails"
  },
  {
    "Value": "User",
    "Name": "extendedAuditEventCategory"
  }
],
"Workload": "AzureActiveDirectory",
"IntraSystemId": "db6d1058-438e-452a-8de2-82650855e986",
"Target": [
  {
    "Type": 2,
    "ID": "User_f1937c88-f4f2-43b3-a753-e324345e39e4"
  },
  {
    "Type": 2,
    "ID": "f1937c88-f4f2-43b3-a753-e324345e39e4"
  },
  {
    "Type": 2,
    "ID": "User"
  },
  {
    "Type": 5,
    "ID": "testuser@wazuh.com"
  },
  {
    "Type": 3,
    "ID": "100320034A719856"
  }
],
"RecordType": "8",
"Version": "1",
"ModifiedProperties": [
  {
    "OldValue": "[]",
    "NewValue": "[\r\n  true\r\n]",
    "Name": "AccountEnabled"
  },
  {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"testuser\"\r\n]",
    "Name": "DisplayName"
  },
  {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"Test\"\r\n]",
```

```
    "Name": "GivenName"
   },
   {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"testuser\"\r\n]",
    "Name": "MailNickname"
   },
   {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"2024-01-29T13:19:12Z\"\r\n]",
    "Name": "StsRefreshTokensValidFrom"
   },
   {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"User\"\r\n]",
    "Name": "Surname"
   },
   {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"testuser@wazuh.com\"\r\n]",
    "Name": "UserPrincipalName"
   },
   {
    "OldValue": "[]",
    "NewValue": "[\r\n  \"Member\"\r\n]",
    "Name": "UserType"
   },
   {
    "OldValue": "",
    "NewValue": "AccountEnabled, DisplayName, GivenName, MailNickname, StsRefreshTokensValidFrom, Sur
    "Name": "Included Updated Properties"
   }
  ],
  "UserId": "XXXXXXX@wazuh.com",
  "TargetContextId": "0fea4e03-8146-453b-b889-54b4bd11565b",
  "Actor": [
   {
    "Type": 5,
    "ID": "XXXXXXX@wazuh.com"
   },
   {
    "Type": 3,
    "ID": "10032002120F5B41"
   },
   {
    "Type": 2,
    "ID": "User_046e51c3-4029-44c0-b57a-e80d39e4970e"
   },
   {
    "Type": 2,
    "ID": "046e51c3-4029-44c0-b57a-e80d39e4970e"
   },
   {
```

```
        "Type": 2,
        "ID": "User"
       }
     ],
     "CreationTime": "2024-01-29T13:19:12",
     "Id": "0c620dac-5a11-4478-a8fe-4c8f35d89517",
     "InterSystemsId": "1f9afa31-170c-4862-8655-5b48b00cc368",
     "Subscription": "Audit.AzureActiveDirectory",
     "UserType": "0",
     "ActorContextId": "0fea4e03-8146-453b-b889-54b4bd11565b"
   },
   "aws": {
     "accountId": "",
     "region": ""
   }
 },
 "rule": {
   "firedtimes": 1,
   "mail": false,
   "level": 6,
   "hipaa": [
     "164.312.a.2.I",
     "164.312.b"
   ],
   "pci_dss": [
     "8.1.2",
     "10.6.2"
   ],
   "description": "Office 365: Added user",
   "groups": [
     "office365",
     "AzureActiveDirectory"
   ],
   "mitre": {
     "technique": [
       "Valid Accounts",
       "Additional Cloud Credentials"
     ],
     "id": [
       "T1078",
       "T1098.001"
     ],
     "tactic": [
       "Defense Evasion",
       "Persistence",
       "Privilege Escalation",
       "Initial Access"
     ]
   },
   "id": "91709"
 },
 "location": "office365",
 "decoder": {
```

```
      "name": "json"
    },
    "id": "1706535414.239597",
    "timestamp": "2024-01-29T13:36:54.168+0000"
  },
  "fields": {
    "timestamp": [
      "2024-01-29T13:36:54.168Z"
    ]
  },
  "highlight": {
    "manager.name": [
      "@opensearch-dashboards-highlighted-field@wazuh-server@/opensearch-dashboards-highlighted-field@"
    ],
    "rule.groups": [
      "@opensearch-dashboards-highlighted-field@office365@/opensearch-dashboards-highlighted-field@"
    ]
  },
  "sort": [
    1706535414168
  ]
}
```

GitHub'ı İzleme

GitHub Denetim Günlüklerinin İzlenmesi

Kurumsal yöneticiler, kuruluşları içindeki üyeler tarafından gerçekleştirilen eylemleri incelemek için proaktif olarak GitHub denetim günlüklerini kullanır. Eylemi gerçekleştiren kullanıcı, eylemin niteliği ve yürütme zaman damgası gibi ayrıntıları içerir. GitHub için Wazuh modülü, API'si aracılığıyla GitHub'dan denetim günlüklerinin toplanmasını sağlar. Wazuh, denetim günlüklerini toplamak için GitHub API uç noktasına bir HTTP GET isteği başlatır . Daha fazla ayrıntı için GitHub REST API `/orgs/{org}/audit-log` belgelerine başvurabilirsiniz .

GitHub Denetim Günlüklerinin İzlenmesine İlişkin Gereksinimler

Wazuh ile denetim günlüklerine erişebilmek için GitHub'da aşağıdaki gereksinimlere sahip olmanız gerekir.

- **GitHub organizasyonu** : Yalnızca GitHub organizasyonlarına ait denetim günlüklerini görüntüleyebilirsiniz.
- **GitHub Enterprise Cloud aboneliği** : Yalnızca GitHub Enterprise Cloud aboneliği olan kuruluşlar GitHub denetim günlüğü REST API'sini kullanabilir.

GitHub'da Kişisel Erişim Belirteci Oluşturma

Gerekli kişisel erişim belirtecini oluşturmak için GitHub'da aşağıdaki adımları izleyin:

1. Kuruluş sahibine ait bir hesapla GitHub'a giriş yapın.
2. Yeni bir kişisel erişim belirteci oluşturmak için https://github.com/settings/tokens/new adresine gidin .
3. Kişisel erişim belirteci için açıklayıcı bir not ekleyin ve bir son kullanma tarihi seçin.

GitHub yeni kişisel erişim belirteci

Image not found or type unknown

4. Aşağı kaydırın, **audit_log** öğesini seçin ve **Jeton oluştur öğesine** tıklayın.

GitHub token üret

Image not found or type unknown

5. Yeni oluşturulan kişisel erişim belirtecini kopyalayın.



GitHub kopyası oluşturulan belirteç

Wazuh'u GitHub Günlüklerini Çekecek Şekilde Yapılandırın

Wazuh'un GitHub denetim günlüklerini izlemesine, toplamasına ve analiz etmesine izin vermek için aşağıdaki adımları gerçekleştirin. Wazuh modülünü GitHub için Wazuh sunucusunda veya Wazuh aracısında yapılandırabilirsiniz.

1. Aşağıdaki yapılandırmayı `/var/ossec/etc/ossec.conf` Wazuh sunucusundaki dosyaya ekleyin.

```
<ossec_config>
  <github>
    <enabled>yes</enabled>
    <interval>1m</interval>
    <time_delay>1m</time_delay>
    <curl_max_size>1M</curl_max_size>
    <only_future_events>yes</only_future_events>
    <api_auth>
      <org_name><ORG_NAME></org_name>
      <api_token><API_TOKEN></api_token>
    </api_auth>
    <api_parameters>
      <event_type>all</event_type>
    </api_parameters>
  </github>
</ossec_config>
```

   Nerede:

   - `<enabled>`: GitHub için Wazuh modülünü etkinleştirir. İzin verilen değerler `yes` ve 'dir `no`.
   - `<interval>`: GitHub için Wazuh modülünün her yürütülmesi arasındaki zaman aralığını tanımlar. Varsayılan değer 'dir `10m` ve izin verilen değer, s (saniye), m (dakika), h (saat) ve d (gün) gibi bir zaman birimini belirten bir sonek karakteri içeren herhangi bir pozitif sayıdır.
   - `<time_delay>`: Taramanın geçerli zamana göre gecikme süresini belirtir. Varsayılan değer 'dir `30s` ve izin verilen değer, s (saniye), m (dakika), h (saat) ve d (gün) gibi bir zaman birimini belirten bir sonek karakteri içeren herhangi bir pozitif sayıdır.
   - `<curl_max_size>`: GitHub API yanıtı için izin verilen maksimum boyutu belirtir. Varsayılan değer 'dir `1M` ve izin verilen değer, b/B (bayt), k/K (kilobayt), m/M (megabayt) ve g/G (gigabayt) gibi bir boyut birimini belirten bir sonek karakteri içeren herhangi bir pozitif sayıdır.
   - `<only_future_events>`: Evet olarak ayarlandığında, GitHub için Wazuh modülü yalnızca Wazuh yöneticisini başlattıktan sonra oluşturulan olayları toplar. olarak

ayarlandığında `no`, Wazuh yöneticisini başlatmadan önce oluşturulan önceki olayları toplar. Varsayılan değer 'dir `yes`ve izin verilen değerler `yes`ve ' dir `no`.

- `<api_auth>`: Bu blok, GitHub REST API ile kimlik doğrulama için kimlik bilgilerini yapılandırır. Aşağıdaki etiketler `<org_name>`ve `<api_token>`, içindeki yapılandırma etiketleridir `<api_auth>`.
  - `<org_name>`: GitHub organizasyonunuzun adı. İzin verilen değer herhangi bir dizedir.
  - `<api_token>`: GitHub API ile kimlik doğrulaması yapmak için kişisel erişim belirteci. İzin verilen değer herhangi bir dizedir.
- `<api_parameters>`: Bu blok GitHub REST API'sindeki dahili seçenekleri yapılandırır. İçindeki bir alt yapılandırma `<api_parameters>`bloğu `<event_type>`.
  - `<event_type>`: Wazuh'un toplaması gereken olay türlerini belirtir. Kullanılabilir olay türleri web ve git olaylarıdır. Bu yapılandırma bloğu için varsayılan değer `all`, hem web hem de git olaylarını toplamaktır. İzin verilen değerler `all`, `web`, ve 'dir `git`.

Yapılandırma seçenekleri hakkında daha fazla bilgi edinmek için GitHub referansı için Wazuh modülüne bakın.

2. Değişiklikleri uygulamak için Wazuh yöneticisini veya aracı hizmetini yeniden başlatın:

   - **Wazuh yöneticisi**

     ```
     systemctl restart wazuh-manager
     ```

   - **Wazuh temsilcisi**

     ```
     systemctl restart wazuh-agent
     ```

Birden Fazla GitHub Organizasyonunu İzleyin

Wazuh ile birden fazla GitHub kuruluşunu, kuruluş kimlik bilgilerini ayrı bölümlerde belirterek izleyebilirsiniz `<api_auth>`. Örneğin, aşağıdaki yapılandırma `organization1`ve adlı iki kuruluşu izler `organization2`.

```
<github>
  <enabled>yes</enabled>
  <interval>1m</interval>
  <time_delay>1m</time_delay>
  <curl_max_size>1M</curl_max_size>
  <only_future_events>no</only_future_events>

  <api_auth>
    <org_name>organization1</org_name>
    <api_token><API_TOKEN></api_token>
  </api_auth>
```

```
  <api_auth>
    <org_name>organization2</org_name>
    <api_token><API_TOKEN></api_token>
  </api_auth>

  <api_parameters>
    <event_type>git</event_type>
  </api_parameters>
</github>
```

Nerede:

- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.

Kullanım Durumu

Gereksinimler

- GitHub aktivite izleme dokümanlarına göre Wazuh'u GitHub ile entegre edin .
- Curl yüklü bir Ubuntu 23.10 uç noktası.

GitHub

`admin:org`, `repo`, ve kapsamları içinde bir GitHub kişisel erişim belirteci oluşturun `delete_repo`. Bu belirteci, Wazuh'ta uyarıları tetikleyen kuruluşta eylemler gerçekleştirerek kullanım durumlarını test etmek için GitHub REST API'siyle kullanacağız. Belirteci oluşturmak için aşağıdaki adımları izleyin:

1. https://github.com/settings/tokens/new adresine gidin , token için bir not ekleyin, istediğiniz son kullanma tarihini seçin ve ardından `repo`ve `admin:org`kapsamlarını seçin.

GitHub yeni kişisel erişim belirteci
Image not found or type unknown

2. Sayfanın en altına gidin, ardından `delete_repo`kapsamı seçin ve **Jeton oluştur** düğmesine tıklayın.

GitHub Jeton oluştur
Image not found or type unknown

3. Yeni oluşturulan kişisel erişim belirtecini kopyalayın.

Oluşturulan belirteci kopyala
Image not found or type unknown

Ubuntu Uç Noktası

Örgüt Üyelerinin Manipülasyonlarını Tespit Edin

Bir Üyeyi Davet Et

Kuruluşunuza bir üye davet etmek için aşağıdaki adımları izleyin.

1. Ubuntu uç noktasında aşağıdaki komutu çalıştırın:

   ```
   # curl -L \
     -X POST \
     -H "Accept: application/vnd.github+json" \
     -H "Authorization: Bearer <API_TOKEN>" \
     -H "X-GitHub-Api-Version: 2022-11-28" \
     https://api.github.com/orgs/<ORG_NAME>/invitations \
     -d '{"email":"<USER_EMAIL>","role":"direct_member"'
   ```

   Nerede:
   - `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.
   - `<ORG_NAME>`kuruluşunuzun adıdır.
   - `<USER_EMAIL>`davet etmek istediğiniz kullanıcının e-posta adresidir.
2. Davet edilen üyenin posta kutusuna gidin ve daveti kabul edin.

Bir Üyeyi Yönetici Olarak Terfi Ettir

Kuruluşunuzdaki bir üyeyi yönetici rolüne yükseltmek için aşağıdaki komutu çalıştırın:

```
# curl \
  -u <ADMIN_USERNAME>:<API_TOKEN> \
  -X PUT \
  -H "Accept: application/vnd.github.v3+json" https://api.github.com/orgs/<ORG_NAME>/memberships/<MEMBER_
   -d '{"role":"admin"}'
```

Nerede:

- `<ADMIN_USERNAME>`geçerli bir yöneticinin kullanıcı adıdır. Örneğin, kuruluşun sahibinin kullanıcı adı.
- `<API_TOKEN>` kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.
- `<ORG_NAME>`kuruluşunuzun adıdır.
- `<MEMBER_USERNAME>`terfi ettirmek istediğiniz kullanıcının kullanıcı adıdır.

Yeni Bir Ekip Oluştur

Kuruluşunuzda yeni bir ekip oluşturmak için aşağıdaki komutu çalıştırın:

```
# curl -X POST \
    -H "Authorization: Bearer <API_TOKEN>" \
    -d '{"name": "<NEW_TEAM_NAME>"}' \
    "https://api.github.com/orgs/<ORG_NAME>/teams"
```

Nerede:

- `<NEW_TEAM_NAME>`yeni takımın adı.

- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.
- `<ORG_NAME>`kuruluşunuzun adıdır.

Aşağıdaki görsel, izlenen GitHub organizasyonunda yukarıdaki eylemleri gerçekleştirdikten sonra Wazuh panosunda oluşan uyarıları göstermektedir.

Bir Depoda Yapılan Değişiklikleri Algıla

Yeni Bir Depo Oluştur

Yeni bir depo oluşturmak için aşağıdaki komutu çalıştırın:

```
# curl -L \
  -X POST \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <API_TOKEN>" \
  -H "X-GitHub-Api-Version: 2022-11-28" \
  https://api.github.com/orgs/<ORG_NAME>/repos \
  -d '{"name":"<NEW_REPO_NAME>"}'
```

Nerede:

- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `repo`.
- `<ORG_NAME>`kuruluşunuzun adıdır.
- `<NEW_REPO_NAME>`oluşturmak istediğiniz deponun adıdır.

Deponuza Bir Takım Ekleyin

Takımları listelemek ve deponuza bir takım eklemek için aşağıdaki komutları çalıştırın:

1. Organizasyonunuzdaki takım kimliklerini listeleyin.

   ```
   # curl -H "Authorization: Bearer <API_TOKEN>" "https://api.github.com/orgs/<ORG_NAME>/teams"
   ```

2. Deponuza eklemek istediğiniz takımın ID'sini girin.

   ```
   # curl -X PUT \
       -H "Authorization: Bearer <API_TOKEN>" \
       -d '{"permission": "push"}' \
       "https://api.github.com/teams/<TEAM_ID>/repos/<ORG_NAME>/<REPO_NAME>"
   ```

   Nerede:
   - `<TEAM_ID>`Takım ID'sidir.
   - `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.
   - `<ORG_NAME>`kuruluşunuzun adıdır.
   - `<REPO_NAME>`Bir takımı eklemek istediğiniz deponun adıdır.

Ayrıcalıkları Yönet

Ekibinizdeki üyelere depoda yönetici ayrıcalıkları vermek için aşağıdaki komutu çalıştırın:

```
# curl \
-u <ADMIN_USERNAME>:<API_TOKEN> \
-X PUT \
-H "Accept: application/vnd.github.v3+json" https://api.github.com/orgs/<ORG_NAME>/teams/<TEAM_NAME>/repo
 -d '{"permission":"admin"}'
```

Nerede:

- `<ADMIN_USERNAME>`bir kullanıcıyı yönetici olarak yükseltme iznine sahip kullanıcının kullanıcı adıdır
- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.
- `<ORG_NAME>`kuruluşunuzun adıdır.
- `<REPO_NAME>`Ekibinin erişimini yönetmek istediğiniz deponun adıdır.
- `<TEAM_NAME>`deponuzdaki belirli takımın adıdır.

Depoyu Sil

Kuruluşunuzdaki bir deponun silinmesi için aşağıdaki komutu çalıştırın:

```
# curl -L \
  -X DELETE \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <API_TOKEN>" \
  -H "X-GitHub-Api-Version: 2022-11-28" \
  https://api.github.com/repos/<ORG_NAME>/<REPO_NAME>
```

Nerede:

- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `delete_repo`.
- `<ORG_NAME>`kuruluşunuzun adıdır.
- `<REPO_NAME>`kuruluşunuzdan silmek istediğiniz deponun adıdır.

Takımı Sil

Oluşturduğunuz takımı silmek için aşağıdaki komutu çalıştırın:

```
# curl -L \
  -X DELETE \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <API_TOKEN>" \
  https://api.github.com/orgs/<ORG_NAME>/teams/<TEAM_NAME>
```

Nerede:

- `<API_TOKEN>`kapsam dahilinde oluşturulan GitHub kişisel erişim belirtecidir `admin:org`.

- `<ORG_NAME>`kuruluşunuzun adıdır.
- `<TEAM_NAME>`deponuzdaki belirli takımın adıdır.

Aşağıdaki görsel, izlenen GitHub organizasyonunda yukarıdaki eylemleri gerçekleştirdikten sonra Wazuh panosunda oluşan uyarıları göstermektedir.

GitHub deposu izleme uyarıları panosu