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 .

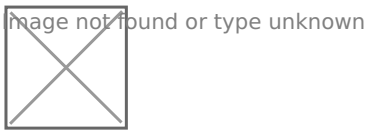
Yapılandırma

Azure

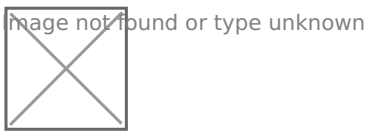
Uygulamanın Oluşturulması

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.

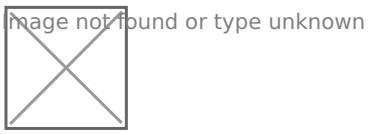
1. **Microsoft Entra ID** panelinde , **Uygulama kayıtları'nı** seçin . Ardından, **Yeni kayıt'ı** seçin.



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

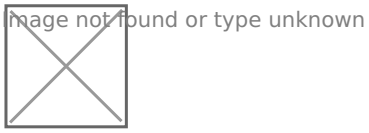


Uygulama artık kayıtlı.

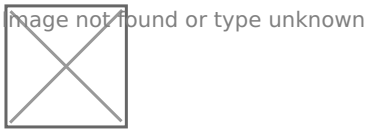


Uygulamaya İzinlerin Verilmesi

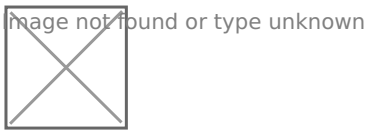
1. Uygulamaya tıklayın, **Genel Bakış** bölümüne gidin ve daha sonraki kimlik doğrulaması için **Uygulama (istemci) Kimliğini** kaydedin.



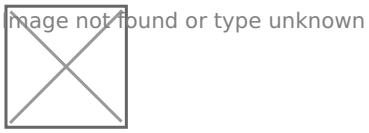
2. **API izinleri** bölümünde **İzin ekle** seçeneğini belirleyin.



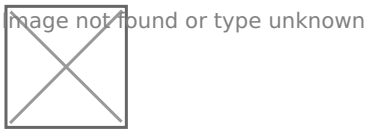
3. "*Microsoft Graph*"ı arayın ve API'yi seçin.



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



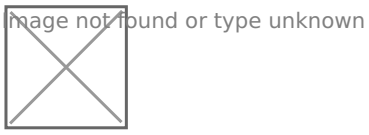
5. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.



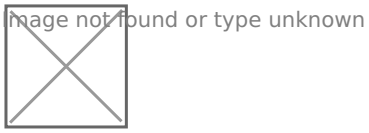
Kimlik Doğrulama İçin Uygulama Anahtarının Alınması

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.**

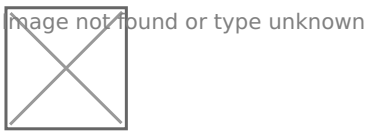


2. Uygun bir **açıklama** girin , anahtar için tercih edilen süreyi ayarlayın ve ardından **Ekle'ye** tıklayın.



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.

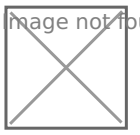
> Uyarı: Alan zorunludur. Bunu **Microsoft Entra ID'deki Genel Bakış** bölümünden `tenantdomain`edinebilirsiniz .

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.

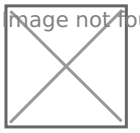


Yukarıdaki yapılandırmayı kullanarak Microsoft Entra ID etkinlik izleme örneğini aşağıda bulabilirsiniz.

Yeni Bir Kullanıcı Oluştur

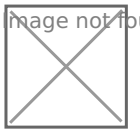
Azure'da yeni bir kullanıcı oluşturun. Başarılı bir kullanıcı oluşturma etkinliği bunu yansıtacak bir günlük üretecektir. Bu günlüğü auditLogs/directoryAudits sorgusunu kullanarak alabilirsiniz.

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



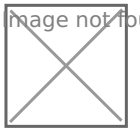
2. Gerekli bilgileri girin ve **İncele + oluştur'a** tıklayın . Kullanıcı artık oluşturuldu.

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



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





Revision #1
Created 31 December 2024 19:50:12 by Ayşegül Sarıkaya
Updated 31 December 2024 20:00:51 by Ayşegül Sarıkaya