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 .`clienttenant`

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 Microsoft Entra ID yazın ve AD'nize erişmek için üzerine tıklayın.
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": "0NRwVY0B9LTh695MCISi",
 "_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, Surı
   "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
  ]
}
```


Revision #2
Created 31 December 2024 18:17:00 by Ayşegül Sarıkaya
Updated 31 December 2024 18:34:51 by Ayşegül Sarıkaya