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 .

Revision #1
Created 31 December 2024 19:21:51 by Ayşegül Sarıkaya
Updated 31 December 2024 19:23:19 by Ayşegül Sarıkaya