PyMISP ile Otomasyon

PyMISP - MISP'e Erişmek İçin Python Kütüphanesi

PyMISP, MISP platformlarına Python programlama dili aracılığıyla REST API'leri kullanarak erişim sağlayan bir kütüphanedir. Bu kütüphane, MISP platformları ile etkileşimi kolaylaştırır ve otomasyon için bir arayüz sunar.

PyMISP'nin Sağladığı Yetenekler:

PyMISP, MISP platformlarındaki olaylara ve verilere erişimi sağlar ve çeşitli işlemleri gerçekleştirmenizi sağlar. Bu yetenekler arasında şunlar bulunur:

- Etkinliklerin eklenmesi, alınması, güncellenmesi, yayımlanması ve silinmesi
- Etiketlerin eklenmesi veya kaldırılması
- Dosya özniteliklerinin eklenmesi: karma, kayıt defteri anahtarı, desenler, kanal, muteks
- Ağ özniteliklerinin eklenmesi: IP hedefi/kaynağı, ana bilgisayar adı, etki alanı, URL, UA, ...
- E-posta özniteliklerinin eklenmesi: kaynak, hedef, konu, ek, ...
- Örneklerin yüklenmesi/indirilmesi
- Görüntülenmelerin güncellenmesi
- Tekliflerin eklenmesi, düzenlenmesi, kabul edilmesi ve silinmesi
- Tam metin araması ve niteliklere göre arama
- STIX etkinliklerinin alınması
- İstatistiklerin dışa aktarılması ve daha fazlası (api.py dosyasına bakınız)

Kurulum:

PyMISP'yi pip kullanarak veya GitHub deposundan en son sürümü alarak yükleyebilirsiniz. Kurulum talimatlarına aşağıdaki şekillerde ulaşabilirsiniz:

- Pip ile kurulum: `pip install pymisp`
- GitHub'dan en son sürümü yükleme: `git clone https://github.com/MISP/PyMISP.git && cd PyMISP` ve `python setup.py install`

PyMISP kütüphanesini kullanabilmek için MISP örneğinizde bir Kimlik Doğrulama Anahtarı'na ihtiyacınız olacaktır.

Başlarken:

PyMISP'yi kullanmaya başlamadan önce, MISP otomasyon anahtarınızı almanız gerekmektedir. Otomasyon anahtarınızı MISP web arayüzündeki otomasyon bölümünde veya profilinizde bulabilirsiniz.

PyMISP kütüphanesini kullanarak örnekler çalıştırmak için, `git clone https://github.com/MISP/PyMISP.git` komutunu kullanarak depoyu klonlayabilir ve örnekler klasöründeki `keys.py` dosyasını düzenleyerek MISP örneğinizin URL'sini ve otomasyon anahtarınızı belirtebilirsiniz.

PyMISP Kullanımı:

PyMISP'nin kullanımını daha iyi anlamak için mevcut örneklerden birine bakalım: `add_named_attribute.py`. Bu komut dosyası, sadece türünü bildiğiniz bir özniteliği mevcut bir etkinliğe eklemenizi sağlar (kategori varsayılan olarak belirlenir).

Revision #1
Created 11 April 2024 15:38:58 by İlayda Durlanık
Updated 12 April 2024 12:09:13 by İlayda Durlanık