

MISP

Giriş

Bir bağlantı tanımlamak için MISP sunucusunda bir hesap ve bir API anahtarı gereklidir.

- Bir veya daha fazla MISP örneği TheHive'a bağlanabilir.
- Her biri için:
- MISP etkinlikleri, TheHive'da Uyarılar olarak içe aktarılabilir. İçe aktarılan etkinlikleri hassaslaştırmak için bir filtre seti kullanılabilir.
- Bir Vaka'da IOC olarak işaretlenmiş Gözlemlenebilirler, MISP'te yeni bir etkinlik olarak dışa aktarılabilir.

MISP bağlantılarını yönetme

Yeni bir MISP sunucusu ekleyin

The screenshot shows the MISP Platform Management interface. The main window displays the 'Platform Management' section with a sidebar containing icons for License, Status, Branding, Cortex, MISP, Authentication, SMTP, Global Endpoints, and LDAP. The 'MISP' tab is selected. The main content area shows 'General settings' with an 'Interval' dropdown set to '1' and 'hour'. Below this is a 'Servers' section with a '+ ' button and a table with the header 'SERVER NAME' and a 'No Data' message. A modal dialog titled 'Set up the new server' is open on the right. It contains the following sections: 'General settings' with fields for 'Server name', 'Server url', 'API Key', and 'Purpose'; 'Proxy' section with 'Use default configuration' (checked), 'Enabled', and 'Disabled' buttons; 'SSL Settings' section with 'Do not check Certificate Authority' (checked) and 'Disable hostname Verification' (checked) options; and 'Advanced settings'.

Bağlantı için şunları belirtin:

- Bu bağlantı için bir isim, örneğin: misp1
- Bağlanılacak MISP sunucusunun URL'si, örneğin: <https://misp.mycompany.com>
- Ayrılmış MISP hesabının API anahtarı

- Bu bağlantının amacı: Yalnızca İçer Aktar, Yalnızca Dışer Aktar veya İçer Aktar ve Dışer Aktar
- TheHive'in MISP ile bağlantı kurması için gerekiyorsa Proxy ayarları

Gelişmiş Ayarlar

Advanced settings

Choose the filter on TheHive organisations

Include all organisations



Tags



Export case tags



Export observables tags



Varsayılan olarak, TheHive'daki tüm organizasyonlar bu bağlantıdan faydalanır. Ek olarak, 2 seçenek daha bulunmaktadır:

- Bu bağlantıyı yalnızca TheHive'daki mevcut organizasyonların bir alt kümesine kullanılabilir hale getirin.
- Bu bağlantıyı TheHive'daki mevcut organizasyonların bir alt kümesine kullanılamaz hale getirin.

Ek seçenekler size şunları sağlar:

- MISP etkinliklerini içer aktardığınızda Uyarılara eklenen etiketleri tanımlayın
- IOC'leri MISP'te dışer aktardığınızda, yeni MISP etkinliğinde Vakadaki gözlemlenebilirlerden gelen etiketleri de dışer aktarın
- IOC'leri MISP'te dışer aktardığınızda, gözlemlenebilirlerden gelen etiketleri de dışer aktarın

Filtreler

Filter settings

Maximum age

minutes▼

Organisations to include

Organisations to exclude

Maximum number of attributes

List of allowed tags

+

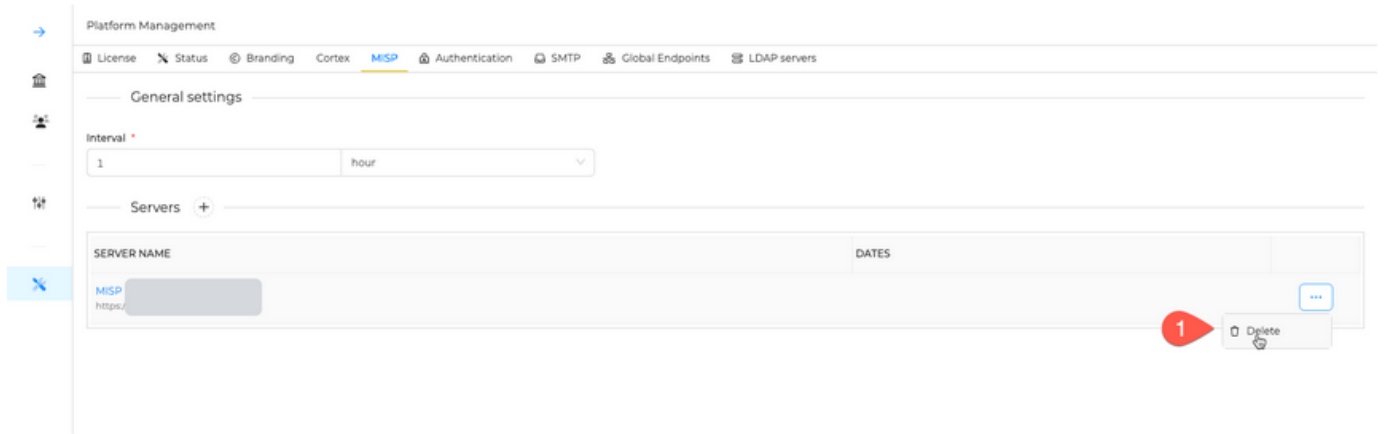
Prohibited tags list

+

MISP etkinliklerini TheHive Uyarıları olarak içe aktardığınızda, birkaç seçenek mevcuttur:

- İçe aktarılmasına izin verilen bir MISP etkinliğinin maksimum yaşını belirleyin
- İçe aktarılmasına izin verilen MISP etkinliklerinin sahibi olan organizasyonların bir listesini belirtin
- İçe aktarılmasına izin verilmeyen MISP etkinliklerinin sahibi olan organizasyonların bir listesini belirtin
- İçe aktarılması için MISP etkinliğine dahil edilecek gözlemlenebilirlerin (~ özniteliklerin) bir limitini belirleyin
- İçe aktarılması için MISP etkinliğinde bulunması gereken etiketlerin bir listesini belirtin
- İçe aktarılması için MISP etkinliğinde bulunması gereken etiketlerin bir listesini belirtin ve bunu görmezden gelin

Bir Bağlantıyı Sil



Revision #4

Created 8 April 2024 19:47:36 by Güldeniz Akca

Updated 13 April 2024 15:09:59 by Güldeniz Akca