

Cortex

Varsayılan olarak, TheHive hiçbir Cortex sunucusuna bağlı değildir.

TheHive'i Cortex'e bağlayın ve Gözlemlenebilirler hakkında bilgi ve istihbarat toplamak için Analizörlerden yararlanın, ayrıca Aksiyonları etkinleştirerek ağınıza veya üçüncü taraf hizmetlerinde(TheHive ve Cortex'in dışında gelen ve bu platformlarla entegre olarak çalışabilen diğer yazılım veya servisler) işlemler çalıştırın.

Giriş

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

- Gözlemlenebilirler üzerinde ayrıntılar, bağlamsal bilgi, istihbarat elde etmek için Analizörler başlatılabilir.
- Yanıtlayıcılar, Araştırma ve Olay Yanıtı sırasında etkin işlemleri çalıştırmak için Vaka, Görevler, Gözlemlenebilirler, görev Günlükleri ve Uyarılar üzerinde başlatılabilir.

Bir veya daha fazla Cortex örneği TheHive'e bağlanabilir.

Cortex Bağlantılarını Yönetme

Yeni Bir Cortex Sunucusu Ekleyin

The screenshot displays the Cortex Platform Management interface. The main window is titled 'Platform Management / Cortex' and shows a sidebar with navigation options: License, Status, Branding, Cortex (selected), MISP, Authentication, SMTP, Global Endpoints, and LDAP. The main content area is divided into 'General settings' and 'Servers'. The 'General settings' section includes fields for 'Max retries on error' (set to 3), 'Refresh Delay' (set to 5 seconds), and 'Frequency of status checks' (set to 1 minute). The 'Servers' section shows a table with the header 'SERVER NAME' and a 'No Data' message. A modal dialog box titled 'Set up the new server' is open on the right side. It contains the following sections: 'General settings' with fields for 'Server name', 'Server url', and 'API Key'; 'Proxy' section with a 'Use default configuration' toggle (set to 'Disabled'); 'SSL Settings' with 'Do not check Certificate Authority' (set to 'Not recommended') and 'Disable hostname Verification' (set to 'Disabled'); and 'Advanced settings' with a 'Choose the filter on TheHive organisations' dropdown (set to 'Include all organisations').

Cortex bağlantısını belirtin:

- Bu bağlantı için bir isim, örneğin: Cortex1
- Bağlanılacak Cortex sunucusunun URL'si, örneğin: <https://cortex.mycompany.com>
- Ayrılmış Cortex hesabının API anahtarı
- Cortex ile bağlantı kurmak için gerekiyorsa Proxy ayarları

Gelişmiş Ayarlar

Advanced settings

Advanced settings

Choose the filter on TheHive organisations

Include selected organisations

Select the organisations to include

Search

☐

☐

☒

☐

☒


Cancel

Update



Cortex tarafından sunulan tüm Analizörler ve Yanıtlayıcılar TheHive'deki tüm organizasyonlar için kullanılabilir durumdadır. Ayrıca, 2 seçenek daha bulunmaktadır:

- Onları sadece TheHive'daki mevcut Organizasyonların bir alt kümesine kullanılabilir hale getirin.
- Onları TheHive'daki mevcut Organizasyonların bir alt kümesine kullanılamaz hale getirin.

Bir Bağlantıyı Sil



Platform Management / Cortex

 ENGLISH (UK)  DEFAULT ADMIN USER

Platform Management

License

Status

Branding

Cortex

MISP

Authentication

SMTP

Global Endpoints

LDAP servers

General settings

Max retries on error

3

Refresh Delay

5

seconds

Frequency of status checks

1

minute

Servers +

SERVER NAME

cortex

...

Cortex

...

1

Delete

Revision #4

Created 8 April 2024 18:03:17 by Güldeniz Akca

Updated 13 April 2024 15:09:33 by Güldeniz Akca