

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 configuration interface. On the left, the 'Platform Management' sidebar is visible with tabs for License, Status, Branding, Cortex (selected), MISP, Authentication, SMTP, Global Endpoints, and LDAP. The main content area shows the 'General settings' for Cortex, including 'Max retries on error' (3), 'Refresh Delay' (5 seconds), and 'Frequency of status checks' (1 minute). Below these settings is a 'Servers' section with a '+ ' button to add new servers. On the right, a modal dialog titled 'Set up the new server' is open, showing fields for 'Server name', 'Server url', and 'API Key'. The 'Proxy' section has a 'Use default configuration' button and 'Enabled'/'Disabled' toggle. The 'SSL Settings' section includes 'Do not check Certificate Authority' and 'Disable hostname Verification' toggles. The 'Advanced settings' section has a 'Choose the filter on TheHive organisations' dropdown menu 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

Created 8 April 2024 18:03:17 by Güldeniz Akca
Updated 13 April 2024 15:09:33 by Güldeniz Akca