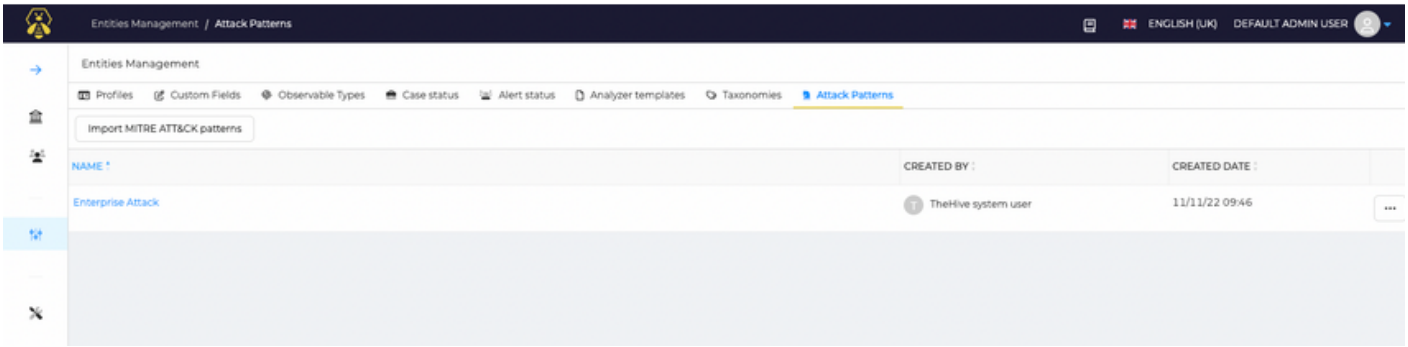
Att&ck Modelleri

Att&ck modelleri yapılandırması, Yönetici alanında mevcuttur: Varlıklar Yönetimi'ni açın, ardından Att&ck Modelleri sekmesine tıklayın.

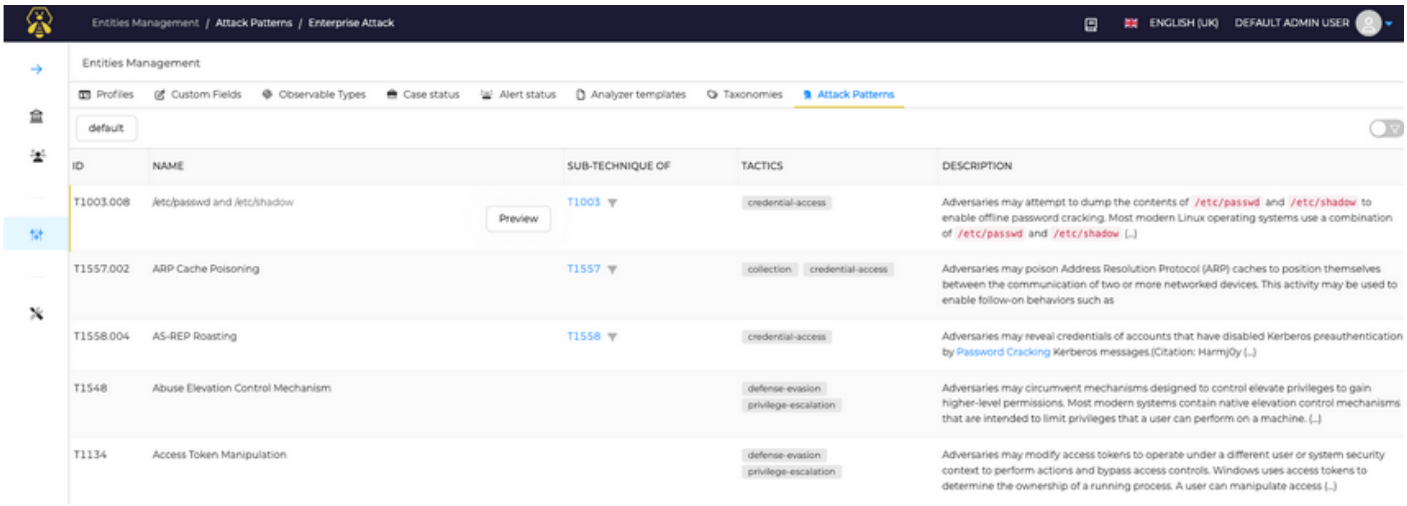
Giriş

Varsayılan olarak, TheHive, MITRE'den Enterprise ATT&CK modelleri ile birlikte gelir. Bu, kurulum süreci sırasında yüklenir ve ilgili tüm tekniklerle birlikte Katalog adı Enterprise Attack oluşturulur.

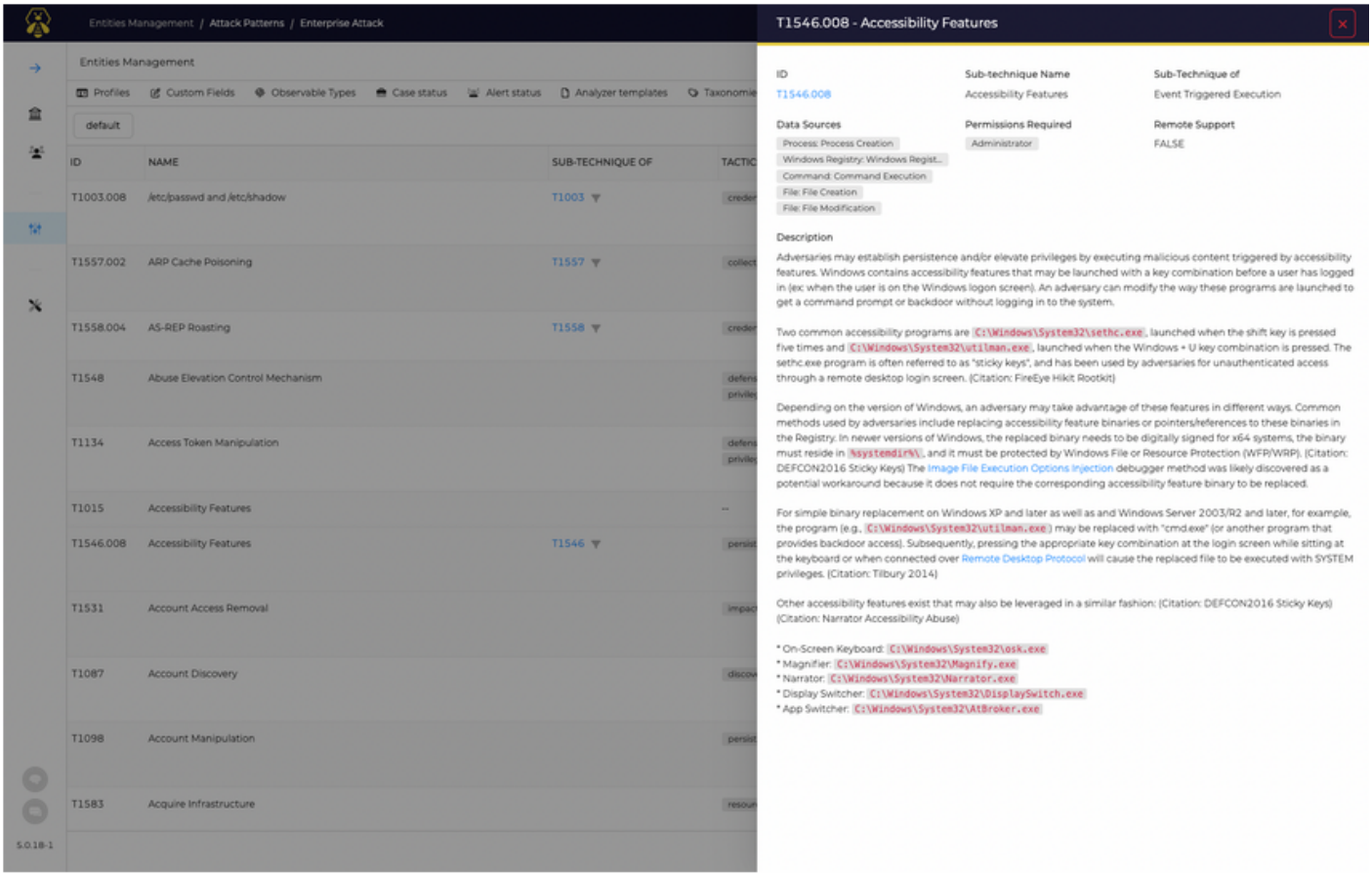


Modelleri Görüntüle

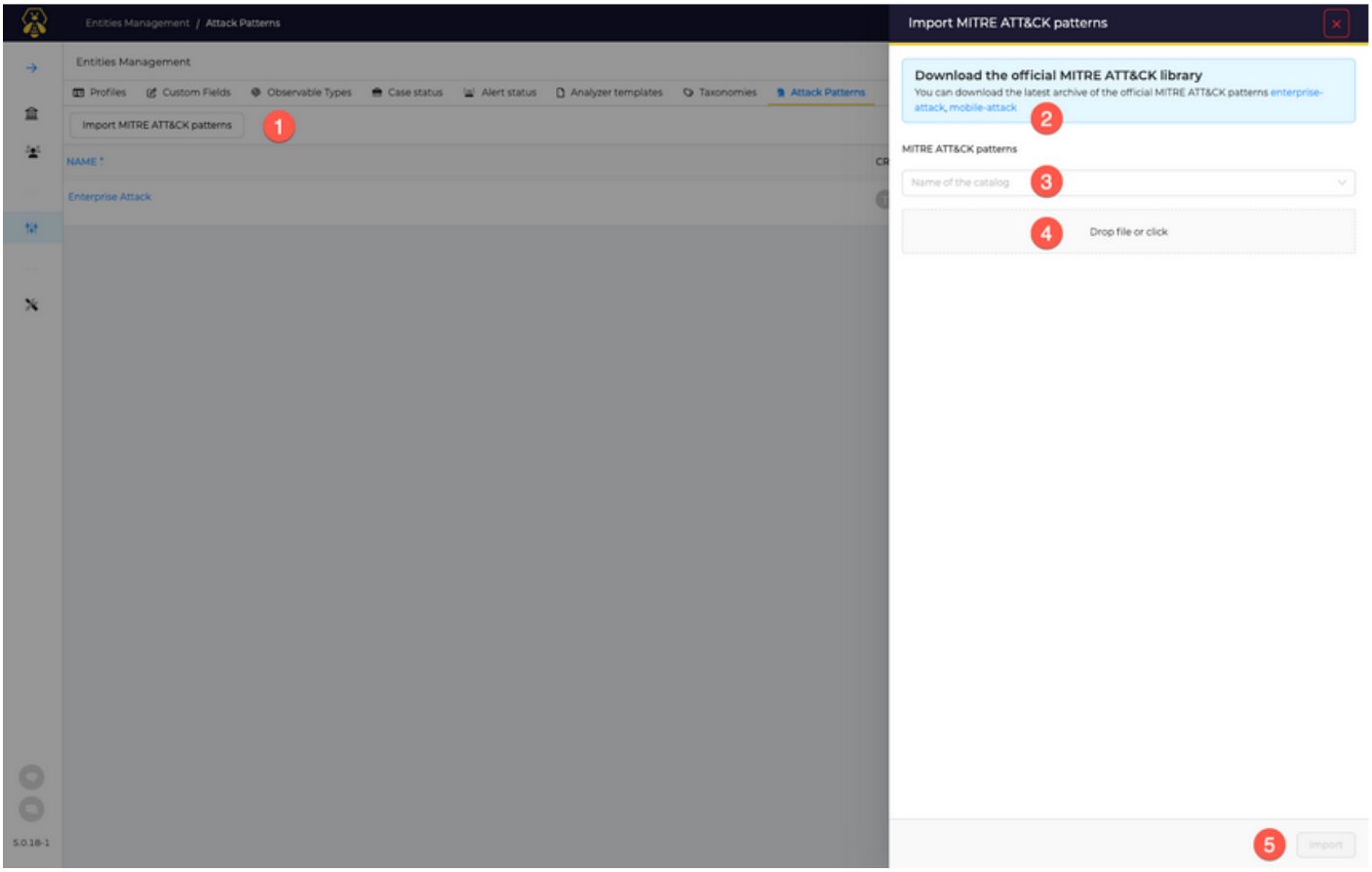
Bir kataloğa dahil edilen modellerin ayrıntılarını görmek için bir kataloğa tıklayın.



Her bir modelin tüm ayrıntıları teknik kimliğine tıklanarak incelenebilir



Kataloglar otomatik olarak güncellenmez, kurulum sırasında gelen Enterprise kataloğu da güncellenmez. Dolayısıyla, çerçevenin en son sürümlerinden yararlanmak istiyorsanız, bunları güncellemeniz gerekir.



Yeni bir katalog eklemek için:

1. "MITRE ATT&CK desenlerini içe aktar" üzerine tıklayın.
2. Kurmak istediğiniz desenleri seçin.
3. Yeni bir katalog oluşturuyorsanız bir katalog adı ekleyin veya güncellemek istediğiniz mevcut bir adı seçin.
4. İndirilen dosyayı sürükleyip bırakın.
5. İçe Aktar düğmesine tıklayın.

Bu işlemler biraz zaman alabilir.

Revision #2
Created 9 April 2024 11:07:20 by Güldeniz Akca
Updated 9 April 2024 18:14:05 by Güldeniz Akca