

Gözlemlenebilir Tipler

Gözlemlenebilir türler, uygulamada kullanılabilecek Gözlemlenebilirlerin mevcut veri türlerini tanımlar. TheHive, önceden tanımlanmış bir dizi türle gelir ve bu liste özel veri türleriyle zenginleştirilebilir.

Gözlemlenebilir türleri, Yönetici alanında yapılandırılır: Varlıklar Yönetimi'ni açın ve Gözlemlenebilir türler sekmesini seçin.

Yeni Bir Gözlemlenebilir Türü Oluştur

Yeni bir Gözlemlenebilir Türü oluşturmak için "+" simgesine tıklayın.

The screenshot shows the 'Adding an Observable Type' dialog in TheHive. The dialog has a 'Name' field (1) and an 'Attachment' toggle (2). The background shows a list of existing observable types: autonomous-system, domain, file, filename, fqdn, hash, hostname, ip, mail, mail-subject, other, regexp, registry, url_path. The 'file' type is highlighted. At the bottom of the dialog, there are 'Cancel' and 'Confirm observable type creation' buttons.

Bu yeni tür için bir isim belirtin. Bu yeni gözlemlenebilir türünün bir dosya ekine göre tanımlanıp tanımlanmadığını belirleyin. Eğer evet ise, analistler tarafından girilen veri bir dosyadır; değilse, bu bir metin alanıdır.

Sonra, Gözlemlenebilir tür oluşturmayı onaylamak için "Gözlemlenebilir tür oluştur" üzerine tıklayın.

Revision #3

Created 9 April 2024 10:31:07 by Güldeniz Akca

Updated 13 April 2024 14:53:28 by Güldeniz Akca