

# Varlık Yönetimi

Bu bölümde profiller, özel alanlar, gözlemlenebilir tipler, vaka durumu, uyarı durumu, analiz şablonları, sınıflandırmalar, att&ck modellerinin nasıl oluşturduğu anlatılacaktır.

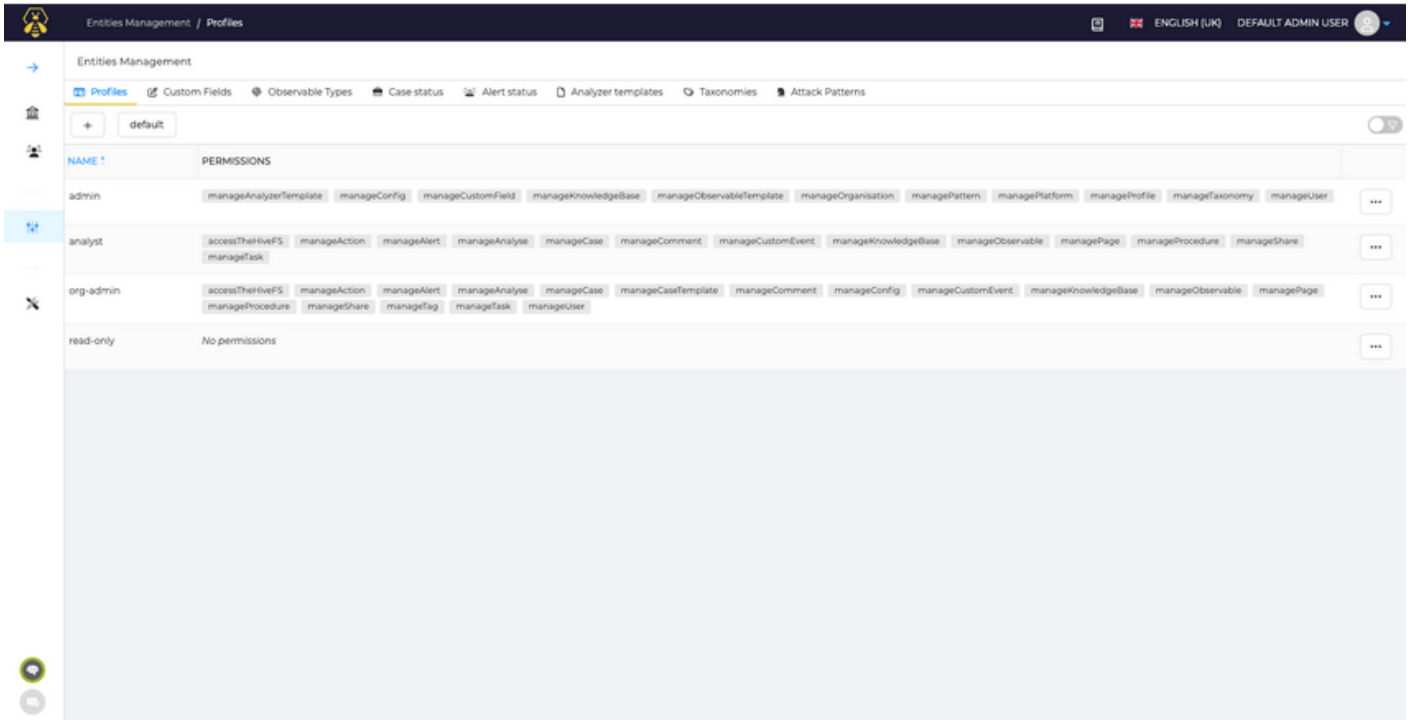
- [Profiller](#)
- [Özel Alanlar](#)
- [Gözlemlenebilir Tipler](#)
- [Vaka Durumu](#)
- [Uyarı Durumu](#)
- [Analiz Şablonları](#)
- [Sınıflandırmalar](#)
- [Att&ck Modelleri](#)

# Profiller

Profiller, Varlıklar Yönetimi sayfasının ilk sekmesinde bulunmaktadır.

## Giriş

TheHive, Yöneticiler ve Kuruluşlar için önceden tanımlanmış bir dizi profil ile gelir; bu set, ihtiyaçlarınıza bağlı olarak oluşturabileceğiniz özel profillerle zenginleştirilebilir.



The screenshot shows the 'Entities Management / Profiles' page in TheHive. It features a sidebar with navigation icons and a main content area with a table of profiles. The table has columns for 'NAME' and 'PERMISSIONS'. The 'admin' profile has permissions like 'manageAnalyzerTemplate', 'manageConfig', etc. The 'analyst' profile has 'accessTheHiveFS', 'manageAction', etc. The 'org-admin' profile has 'accessTheHiveFS', 'manageAction', etc. The 'read-only' profile has 'No permissions'. There are also buttons for '+', 'default', and a toggle switch in the top right.

NAME	PERMISSIONS
admin	manageAnalyzerTemplate, manageConfig, manageCustomField, manageKnowledgeBase, manageObservableTemplate, manageOrganisation, managePattern, managePlatform, manageProfile, manageTaxonomy, manageUser
analyst	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageComment, manageCustomEvent, manageKnowledgeBase, manageObservable, managePage, manageProcedure, manageShare, manageTask
org-admin	accessTheHiveFS, manageAction, manageAlert, manageAnalyse, manageCase, manageCaseTemplate, manageComment, manageConfig, manageCustomEvent, manageKnowledgeBase, manageObservable, managePage, manageProcedure, manageShare, manageTag, manageTask, manageUser
read-only	No permissions

Profilleri güncellemek için geçerli bir lisans gereklidir.

## İzinler

Her profil, bir dizi izin tarafından tanımlanır. İki profil türü vardır:

- Yönetim: Admin kuruluşundaki kullanıcılar tarafından platformun yönetimi için kullanılır.
- Kuruluş: İş kuruluşlarında kullanılan.

İzinler, uygulamadaki bir varlık olan Entity ile `manageEntity` adı verilir. Örneğin: `manageCase`. Bir `manageEntity` izni, bir varlığı yazma, güncelleme, silme haklarını içerir.

## Profilleri Yönet

Admin profili hariç, tüm profiller özelleştirilebilir ve silinebilir.

## Profil Ekle

- Profil sekmesinde, Entities Management sayfasında "+" düğmesine tıklayarak yeni bir profil ekleyin.
- Ardından oluşturulacak profil türünü seçin ve ilişkilendirilmiş izinleri belirleyin.

Profil Ekleme penceresi açılır.

- Yeni profil için bir Ad girin.
- Profil türünü Seçin.
- O profil türü için İzinleri seçin.
- Profil oluşturma işlemini onaylamak için "Profil Oluşturma" düğmesine tıklayın.

Adding a Profile

Name \*

NewAdmin

Profile type

☒ Administration

☐ Organisation

Permissions

Select all

☐ Manage knowledge base

☐ Manage analyzer template

☐ Manage taxonomy

☒ Manage profile

☐ Manage pattern

☐ Manage custom fields

☐ Manage config

☒ Manage organisations

☒ Manage users

☐ Manage platform

☐ Manage observable template

# Özel Alanlar

Özel Alanlar, bir Vaka veya Uyarıyı daha fazla bağlam sağlamak, istatistikler veya panolar oluşturmak için kullanılan özel bilgilerle zenginleştirilmiş bilgilerdir.

TheHive'in Yönetici görünümünde tanımlanır ve platformdaki tüm Kuruluşlara sunulur.

Bu Özel Alanlar görünümü, Yönetici alanında mevcuttur: Varlıklar Yönetimi görünümünü açın, ardından Özel Alanlar sekmesini açın.

## Özel Alan Oluştur

Yeni bir Özel Alan oluşturmak için "+" simgesine tıklayın.

The screenshot shows the 'Adding a Custom Field' form in TheHive. The form is divided into two main sections: 'Entities Management' on the left and 'Adding a Custom Field' on the right. The 'Adding a Custom Field' section contains several input fields and a toggle switch, each numbered 1 through 7. The fields are: 1. Display name (Business Unit), 2. Technical name (business-unit), 3. Description (Business Units of the company), 4. Group (default), 5. Type (string), 6. Options (Sales, Marketing, HR, Security, IT), and 7. Mandatory (toggle switch).

Yeni bir Özel Alan oluşturmak için aşağıdaki bilgileri doldurun:

- Vakalar ve Uyarılarda görüntülenecek bir isim
- Teknik bir isim. Varsayılan olarak, bu isim otomatik olarak ad ile ayarlanır, ancak gerektiğinde ayarlanabilir. Bu isim, API ile Özel Alanı kullanırken kullanılır.
- Analistlerin Vakalar ve Uyarılarla bu ÖA'yı kullanmasına yardımcı olmak için bir açıklama ekleyin.
- Bu ÖA için bir grup adı tanımlayın.
- ÖA'nın türünü tanımlayın; Birden fazla tür mevcuttur - Dize, Boolean, Tamsayı, Ondalık, Tarih
- Önceden tanımlanmış değerler varsa, bunları doldurun veya bu bir serbest alan ise boş bırakın

- Bu Özel Alanın zorunlu olması ve bir Vakayı kapatmadan önce deęerlendirilmesi gerekiyorsa bu seeneęi etkinleřtirin.

Sonra, Özel Alan oluřturma iřlemini onaylamak iin "Özel Alan Oluřtur" zerine tıklayın.

# 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 left sidebar is titled 'Entities Management' and has a sub-tab 'Observable Types'. The main area displays a list of existing observable types: 'autonomous-system', 'domain', 'file', 'filename', 'fqdn', 'hash', 'hostname', 'ip', 'mail', 'mail-subject', 'other', 'regex', 'registry', and 'url\_path'. The right panel is the 'Adding an Observable Type' form. It has a 'Name' field (1) with the value 'emi file' and an 'Attachment' toggle (2) which is currently turned on. At the bottom right, 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 oluşturmaya onaylamak için "Gözlemlenebilir tür oluştur" üzerine tıklayın.

# Vaka Durumu

Vaka Durumu, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi sayfasını açın ve Vaka durumu sekmesini seçin.

## Giriş

TheHive, bir dizi önceden tanımlanmış durum ile gelir. Her durum bir Aşamaya aittir.

Entities Management		
Profiles	Custom Fields	Observable Types
Case status	Alert status	Analyzer templates
Taxonomies	Attack Patterns	

STATUS *	STAGE *
New	New
In progress	InProgress
Duplicated	Closed
False positive	Closed
Indeterminate	Closed
Other	Closed
True positive	Closed

Aşamalar sabitlenmiştir; güncellenemez veya silinemezler ve platforma yeni bir aşama eklenemez. Durumlar oluşturulabilir, güncellenebilir ve silinebilir.

## Durum Oluşturma

Yeni bir durum eklemek için "+" simgesine tıklayın.

Entities Management / Case status

Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

+

STATUS \*

New

In progress

Pending analysis

Duplicated

False positive

Indeterminate

Add a custom status

Stage \* InProgress 1

Value \* In review 2

Colour #f97a00 3

Preview In review

Bir durum şu özelliklere sahiptir:

- Bir aşama: Yeni durumun aşamasını seçin.

- Bir değ er: Yeni durum i in bir ad se in.
- Bir renk: Kullanıcıların uygulamada durumu hızlıca tanımlaması i in bir renk se in.

### **Durumu D zenle/Sil**

Renk, bir durumu g ncellerken yalnızca g ncellenebilir.

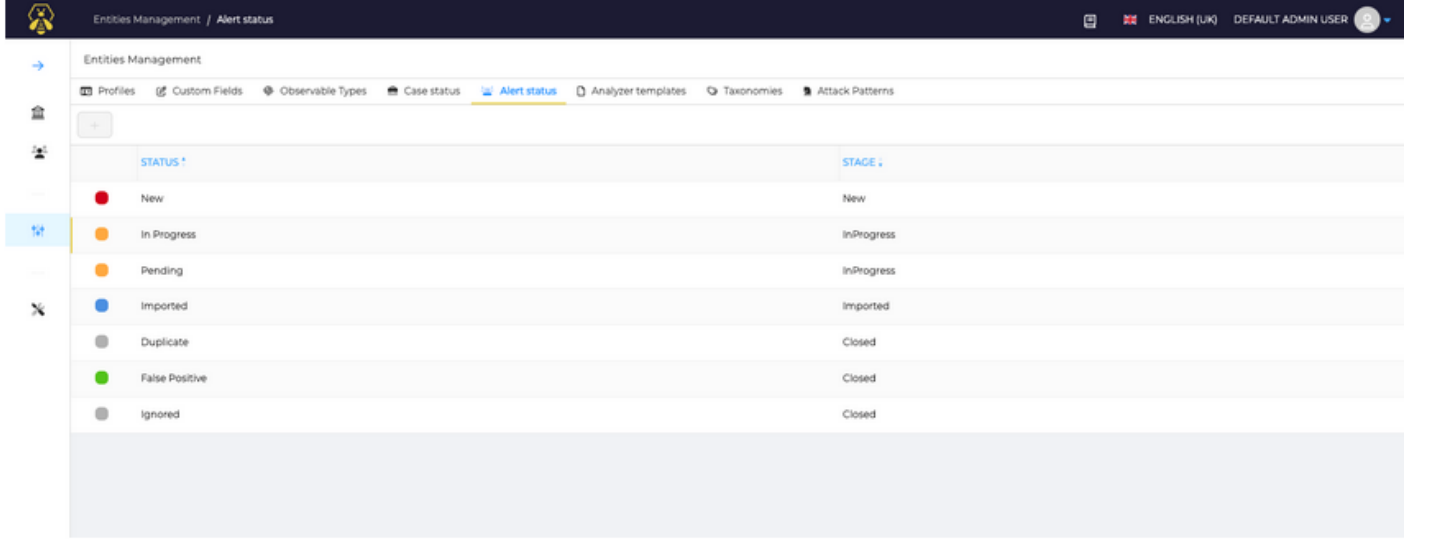


# Uyarı Durumu

Uyarı Durumu, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi sayfasını açın ve uyarı durumu sekmesini seçin.

## Giriş

TheHive, bir dizi önceden tanımlanmış durum ile gelir. Her durum bir aşamaya aittir.



The screenshot shows the 'Alert status' page in TheHive. The page has a dark blue header with the title 'Entities Management / Alert status' and user information 'ENGLISH (UK) DEFAULT ADMIN USER'. Below the header is a navigation bar with tabs: Profiles, Custom Fields, Observable Types, Case status, Alert status (selected), Analyzer templates, Taxonomies, and Attack Patterns. A sidebar on the left contains icons for various entities. The main content area is a table with two columns: 'STATUS' and 'STAGE'. The table lists eight statuses: New, In Progress, Pending, Imported, Duplicate, False Positive, and Ignored. Each status has a corresponding color-coded icon and a stage value.

STATUS	STAGE
New	New
In Progress	InProgress
Pending	InProgress
Imported	Imported
Duplicate	Closed
False Positive	Closed
Ignored	Closed

Aşamalar sabitlenmiştir; güncellenemez veya silinemezler ve platforma yeni bir aşama eklenemez. Durumlar oluşturulabilir, güncellenebilir ve silinebilir.

## Durum Oluşturma

Yeni bir durum eklemek için "+" simgesine tıklayın.

Entities Management / Alert status

Add a custom status

Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

+

STATUS \*

New

In Progress

Pending

Imported

Duplicate

False Positive

Ignored

Stage \*

InProgress

Value \*

In review

Colour

#f55a04

Preview

In review

Bir durum, şu özelliklere sahiptir:

- Bir aşama: Yeni durumun aşamasını seçin.
- Bir değer: Yeni durum için bir ad seçin.
- Bir renk: Kullanıcıların uygulamada durumu hızlıca tanımlaması için bir renk seçin.

## Durumu Düzenle/Sil

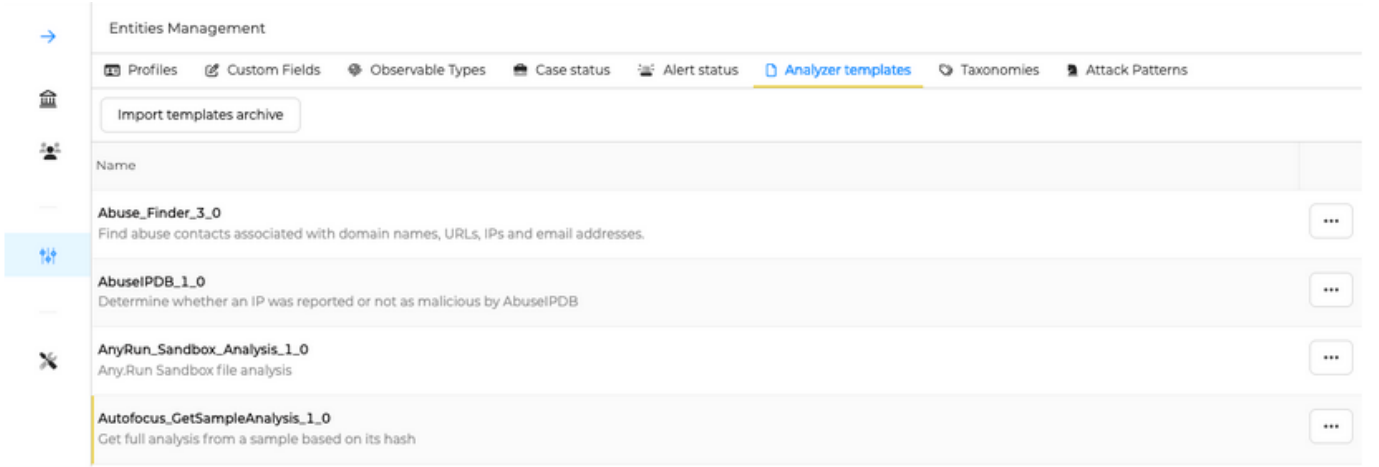
Renk, bir durumu güncellerken yalnızca güncellenebilir.

# Analiz Şablonları

TheHive, analiz raporlarını görüntülemek için HTML şablonlarına ihtiyaç duyar.

## Genel Analiz Şablonlarını Kurun veya Güncelleyin

- Yönetici olarak, "Varlık Yönetimi" menüsüne ve "Analiz Şablonlarına" gidin.



- ZIP arşivini indirin, ekleyin ve İçer Aktar düğmesine tıklayın.

Entities Management / Analyzer templates

→ Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

Import templates archive

Name
<b>Abuse_Finder_3_0</b> Find abuse contacts associated with domain names, URLs, IPs and email addresses.
<b>AbuseIPDB_1_0</b> Determine whether an IP was reported or not as malicious by AbuseIPDB
<b>AnyRun_Sandbox_Analysis_1_0</b> Any.Run Sandbox file analysis
<b>Autofocus_GetSampleAnalysis_1_0</b> Get full analysis from a sample based on its hash
<b>Autofocus_SearchIOC_1_0</b> Search samples in Autofocus based on a single IOC
<b>CIRCLHashlookup_1_1</b> CIRCL hashlookup uses a public API to lookup hash values against databases of known good files
<b>Crt_sh_Transparency_Logs_1_0</b> Query domains against the certificate transparency lists available at crt.sh.
<b>DShield_lookup_1_0</b> Query the SANS ISC DShield API to check for an IP address reputation.
<b>dshield_test_1_0</b> Query the SANS ISC DShield API to check for an IP address reputation.
<b>EmiParser_2_1</b> Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.
<b>FileInfo_8_0</b> Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate us

Import templates archive

Download the official templates archive

You can download the latest official analyzer templates archive from here

Templates archive

Drop file or click

report-templates.zip

Import

## Şablonları Düzenle

Yeni bir Analiz Cortex'te etkinleştirildiğinde ve TheHive için kullanılabilir hale geldiğinde, bu listede bir şablon satırı eklenir.

- Düzenlenecek şablonu bulun

**VirusTotal\_GetReport\_3\_1**  
Get the latest VirusTotal report for a file, hash, domain or an IP address.

**VirusTotal\_Rescan\_3\_1**  
Use VirusTotal to run new analysis on hash.

Default Template

...

Düzenleyin ve kaydedin

Entities Management / Analyzer templates

→ Entities Management

Profiles Custom Fields Observable Types Case status Alert status Analyzer templates

Import templates archive

Name
<b>Abuse_Finder_3_0</b> Find abuse contacts associated with domain names, URLs, IPs and email addresses.
<b>AbuseIPDB_1_0</b> Determine whether an IP was reported or not as malicious by AbuseIPDB
<b>AnyRun_Sandbox_Analysis_1_0</b> Any.Run Sandbox file analysis
<b>Autofocus_GetSampleAnalysis_1_0</b> Get full analysis from a sample based on its hash
<b>Autofocus_SearchIOC_1_0</b> Search samples in Autofocus based on a single IOC
<b>CIRCLHashlookup_1_1</b> CIRCL hashlookup uses a public API to lookup hash values against databases of known good files
<b>Crt_sh_Transparency_Logs_1_0</b> Query domains against the certificate transparency lists available at crt.sh.
<b>DShield_lookup_1_0</b> Query the SANS ISC DShield API to check for an IP address reputation.
<b>dshield_test_1_0</b> Query the SANS ISC DShield API to check for an IP address reputation.
<b>EmlParser_2_1</b> Parse and visualise EML email message. Submit a .eml formatted file and extract some useful information.
<b>FileInfo_8_0</b> Parse files in several formats such as OLE and OpenXML to detect VBA macros, extract their source code, generate us

Import templates archive

Download the official templates archive

You can download the latest official analyzer templates archive [from here](#)

Templates archive

Drop file or click

report-templates.zip

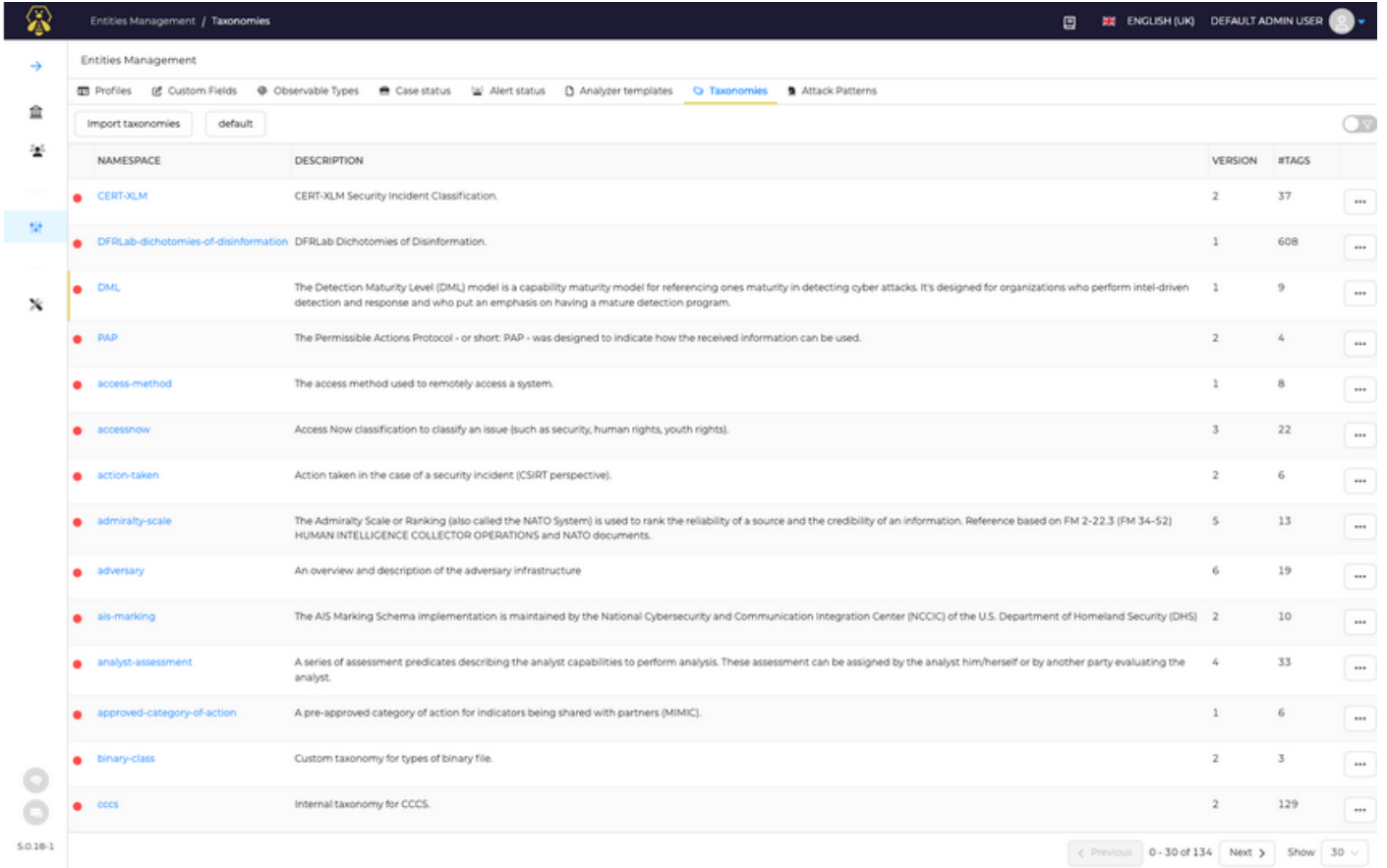
Import

Bağlı analizleri çalıştırmak, yeni şablonun uygulandığı sonuçları görüntülemelidir.

# Sınıflandırmalar

Sınıflandırmalar, TheHive'da yapılandırılmış etiketleri tanımlamak için kullanılır. Sınıflandırmalar, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi'ni açın ve Sınıflandırmalar sekmesini seçin.

Varsayılan olarak, MISP sınıflandırmaları içe aktarılır.



The screenshot shows the 'Taxonomies' section of TheHive's 'Entities Management' interface. The top navigation bar includes 'Profiles', 'Custom Fields', 'Observable Types', 'Case status', 'Alert status', 'Analyzer templates', 'Taxonomies' (selected), and 'Attack Patterns'. Below the navigation bar, there are tabs for 'Import taxonomies' and 'default'. The main content area is a table listing various taxonomies. Each row includes a red dot icon, a namespace, a description, a version number, and the number of tags. A 'Show' button is visible at the bottom right of the table.

	NAMESPACE	DESCRIPTION	VERSION	#TAGS	
	CERT-XLM	CERT-XLM Security Incident Classification.	2	37	...
	DFRLab-dichotomies-of-disinformation	DFRLab Dichotomies of Disinformation.	1	608	...
	DML	The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven detection and response and who put an emphasis on having a mature detection program.	1	9	...
	PAP	The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.	2	4	...
	access-method	The access method used to remotely access a system.	1	8	...
	accessnow	Access Now classification to classify an issue (such as security, human rights, youth rights).	3	22	...
	action-taken	Action taken in the case of a security incident (CSIRT perspective).	2	6	...
	admiralty-scale	The Admiralty Scale or Ranking (also called the NATO System) is used to rank the reliability of a source and the credibility of an information. Reference based on FM 2-22.3 (FM 34-52) HUMAN INTELLIGENCE COLLECTOR OPERATIONS and NATO documents.	5	13	...
	adversary	An overview and description of the adversary infrastructure	6	19	...
	ais-marking	The AIS Marking Schema implementation is maintained by the National Cybersecurity and Communication Integration Center (NCCIC) of the U.S. Department of Homeland Security (DHS)	2	10	...
	analyst-assessment	A series of assessment predicates describing the analyst capabilities to perform analysis. These assessment can be assigned by the analyst him/herself or by another party evaluating the analyst.	4	33	...
	approved-category-of-action	A pre-approved category of action for indicators being shared with partners (MIMIC).	1	6	...
	binary-class	Custom taxonomy for types of binary file.	2	3	...
	cccs	Internal taxonomy for CCCS.	2	129	...

Bir sınıflandırmadaki mevcut etiketlerin listesini gözden geçirmek için istenen adı tıklayın; bu, etiketlerin listesiyle bir çekmeceyi açacaktır.

## Kullanıcı Bir Sınıflandırmayı Görüntüle

Bir belirli sınıflandırmadaki mevcut etiketlerin listesini gözden geçirmek için istenen adı tıklayın; bu, etiketlerin listesiyle bir çekmeceyi açacaktır.

Entities Management / europol-event taxonomy		Namespace	Version	Description
		europol-event	1	This taxonomy was designed to describe the type of events
		Tags		
TAG	PREDICATE	VALUE	COLOUR	
europol-event:aggregation-inform...	aggregation-information-phishing-schemes	-	#000000	
europol-event:brute-force-attempt...	brute-force-attempt	-	#000000	
europol-event:c&c-server-hosting	c&c-server-hosting	-	#000000	
europol-event:connection-malware...	connection-malware-port	-	#000000	
europol-event:connection-malware...	connection-malware-system	-	#000000	
europol-event:content-forbidden-by...	content-forbidden-by-law	-	#000000	
europol-event:control-system-byp...	control-system-bypass	-	#000000	
europol-event:copyrighted-conten...	copyrighted-content	-	#000000	
europol-event:data-exfiltration	data-exfiltration	-	#000000	
europol-event:deletion-informati...	deletion-information	-	#000000	
europol-event:dictionary-attack...	dictionary-attack-attempt	-	#000000	
europol-event:disruption-data-tr...	disruption-data-transmission	-	#000000	
europol-event:dissemination-malw...	dissemination-malware-email	-	#000000	
europol-event:dissemination-phis...	dissemination-phishing-emails	-	#000000	
europol-event:dns-zone-transfer	dns-zone-transfer	-	#000000	
europol-event:email-flooding	email-flooding	-	#000000	
europol-event:exploit	exploit	-	#000000	
europol-event:exploit-attempt	exploit-attempt	-	#000000	
europol-event:exploit-framework...	exploit-framework-exhausting-resources	-	#000000	
europol-event:exploit-framework...	exploit-framework-exhausting-resources	-	#000000	

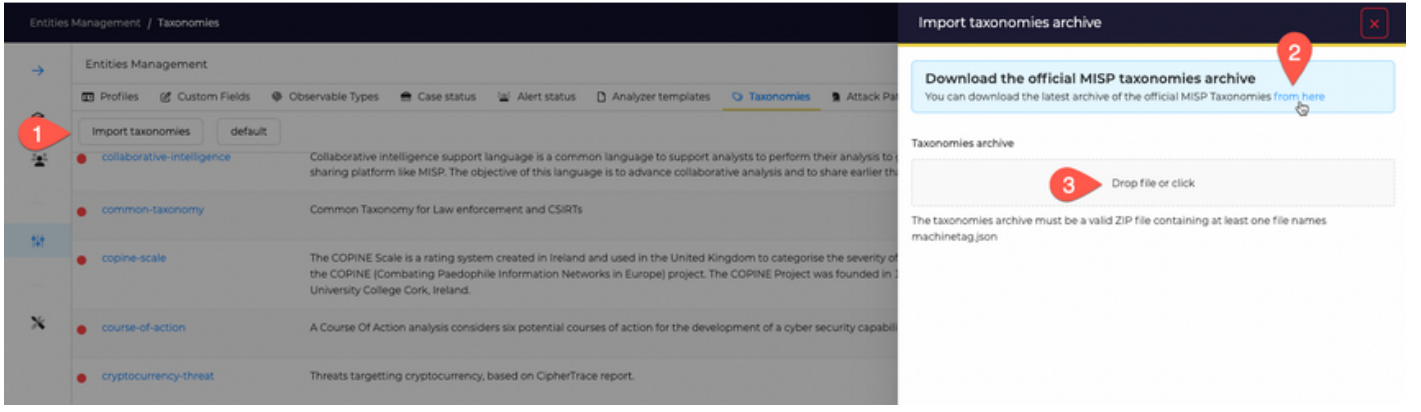
## Bir Sınıflandırmayı Etkinleştirme veya Silme

Varsayılan olarak hiçbir sınıflandırma etkin değildir; bu nedenle Vakalarda veya Uyarılarda kullanılamazlar. Vakalarda ve Uyarılarda bir etiket setini kullanmak için ilgili sınıflandırma etkinleştirilmelidir.

course-of-action	A Course Of Action analysis considers six potential courses of action for the development of a cyber security capability.	2	7	...
cryptocurrency-threat	Threats targeting cryptocurrency, based on CipherTrace report.	1	7	Activate Delete
csirt-americas	Taxonomia CSIRT Américas.	1	14	...
csirt_case_classification	It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IMs with proper case handling procedures and will form the basis of SLA's between the CSIRT and other Company departments.	1	17	...
cssa	The CSSA agreed sharing taxonomy.	8	15	...
cti	Cyber Threat Intelligence cycle to control workflow state of your process.	1	6	...

## Sınıflandırmaları Güncelle

TheHive, kurulum anındaki MISP sınıflandırmaları sürümüyle birlikte gelir. TheHive güncellenirken en son kullanılabilir sürümü güncellemez veya eklemaz. Dolayısıyla, MISP ekibinin yayınladığı en son sürümü almak istiyorsanız bunu manuel olarak güncellemeniz gerekir.



1. Taksonomileri "İçe Aktar" düğmesine tıklayın.
2. Son arşivi buradan indirebilirsiniz: <https://github.com/MISP/misp-taxonomies/archive/main.zip>
3. İndirilen dosyayı sürükleyip bırakın ve "İçe Aktar" düğmesine tıklayın

## Özel Sınıflandırmalar

MISP tarafından belirtilen JSON şemasını takip ederek kendi taksonomilerinizi ekleyebilirsiniz. (<https://github.com/MISP/misp-taxonomies>)

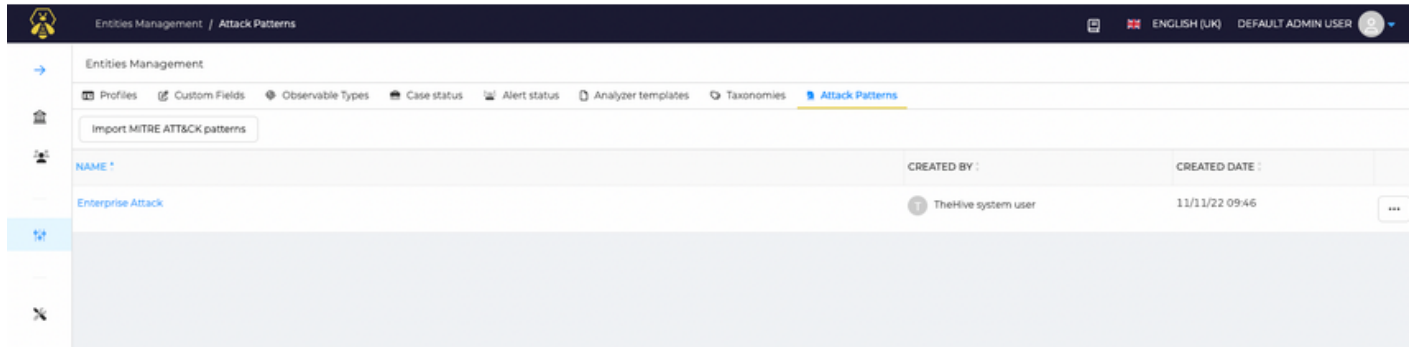


# Att&ck Modelleri

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

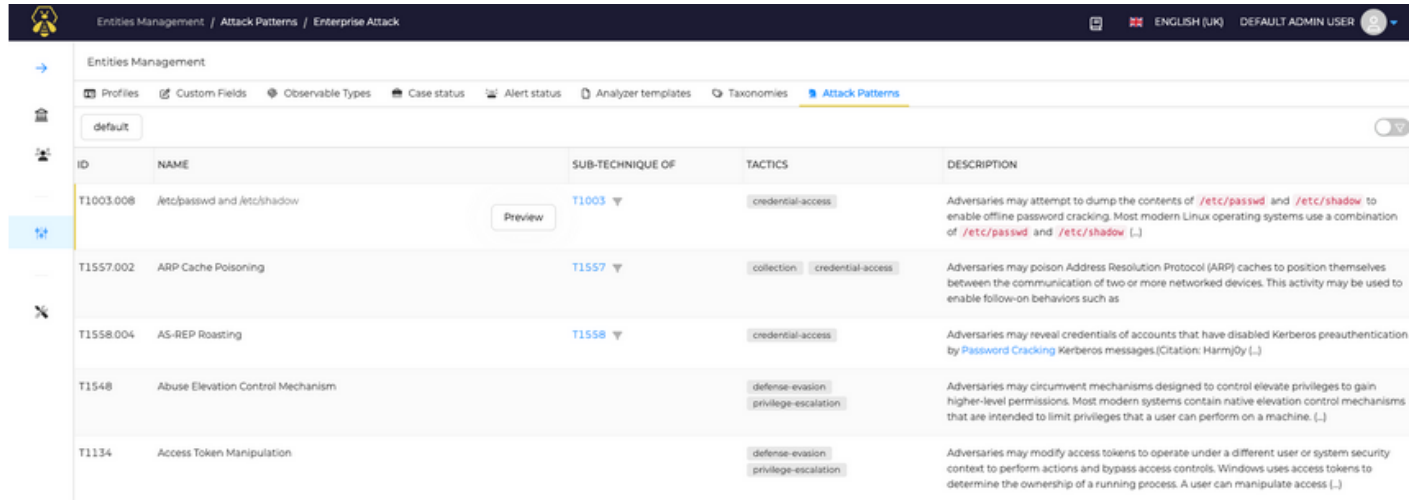
## Giriş

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

Entities Management / Attack Patterns / Enterprise Attack

Entities Management

ProfilesCustom FieldsObservable TypesCase statusAlert statusAnalyzer templatesTaxonomie

default

ID	NAME	SUB-TECHNIQUE OF	TACTIC
T1003.008	lsc/passwd and lsc/shadow	T1003	credential
T1557.002	ARP Cache Poisoning	T1557	collect
T1558.004	AS-REP Roasting	T1558	credential
T1548	Abuse Elevation Control Mechanism		defense, privilege
T1134	Access Token Manipulation		defense, privilege
T1015	Accessibility Features		
T1546.008	Accessibility Features	T1546	persist
T1531	Account Access Removal		impact
T1087	Account Discovery		discover
T1098	Account Manipulation		persist
T1583	Acquire Infrastructure		resource

T1546.008 - Accessibility Features

ID

T1546.008

Sub-technique Name

Accessibility Features

Sub-Technique of

Event Triggered Execution

Data Sources

Process: Process Creation  
Windows Registry: Windows Regist...  
Command: Command Execution  
File: File Creation  
File: File Modification

Permissions Required

Administrator

Remote Support

FALSE

Description

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (e.g. when the user is on the Windows login screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are `C:\Windows\System32\sethc.exe`, launched when the shift key is pressed five times and `C:\Windows\System32\utilman.exe`, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

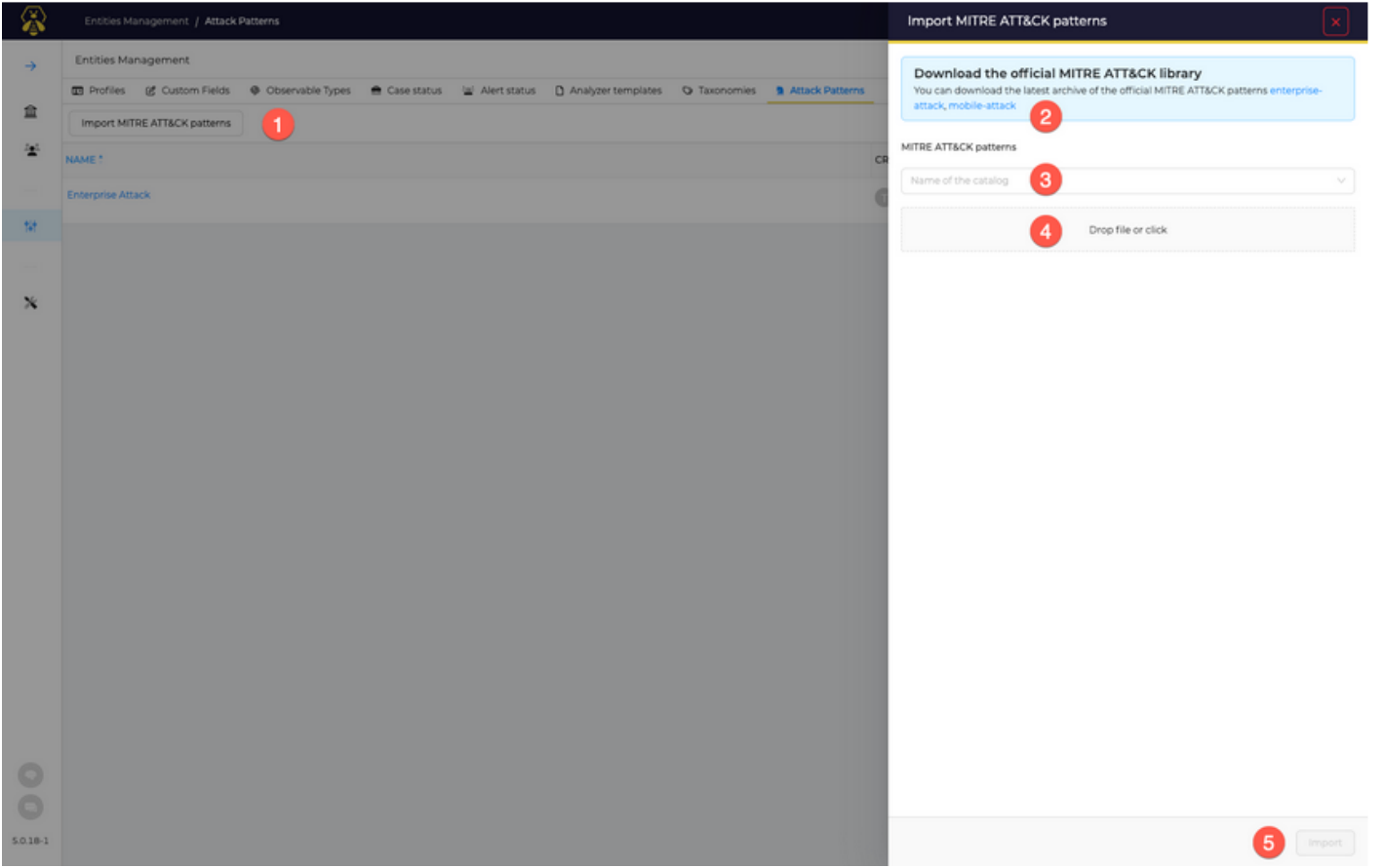
Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in `%systemdir%`, and it must be protected by Windows File or Resource Protection (WFR/WRP). (Citation: DEFCON2016 Sticky Keys) The `Image File Execution Options Injection` debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as Windows Server 2003/R2 and later, for example, the program (e.g., `C:\Windows\System32\utilman.exe`) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over `Remote Desktop Protocol` will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tibbory 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys) (Citation: Narrator Accessibility Abuse)

- \* On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- \* Magnifier: `C:\Windows\System32\Magnify.exe`
- \* Narrator: `C:\Windows\System32\Narrator.exe`
- \* Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- \* App Switcher: `C:\Windows\System32\AtBroker.exe`

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