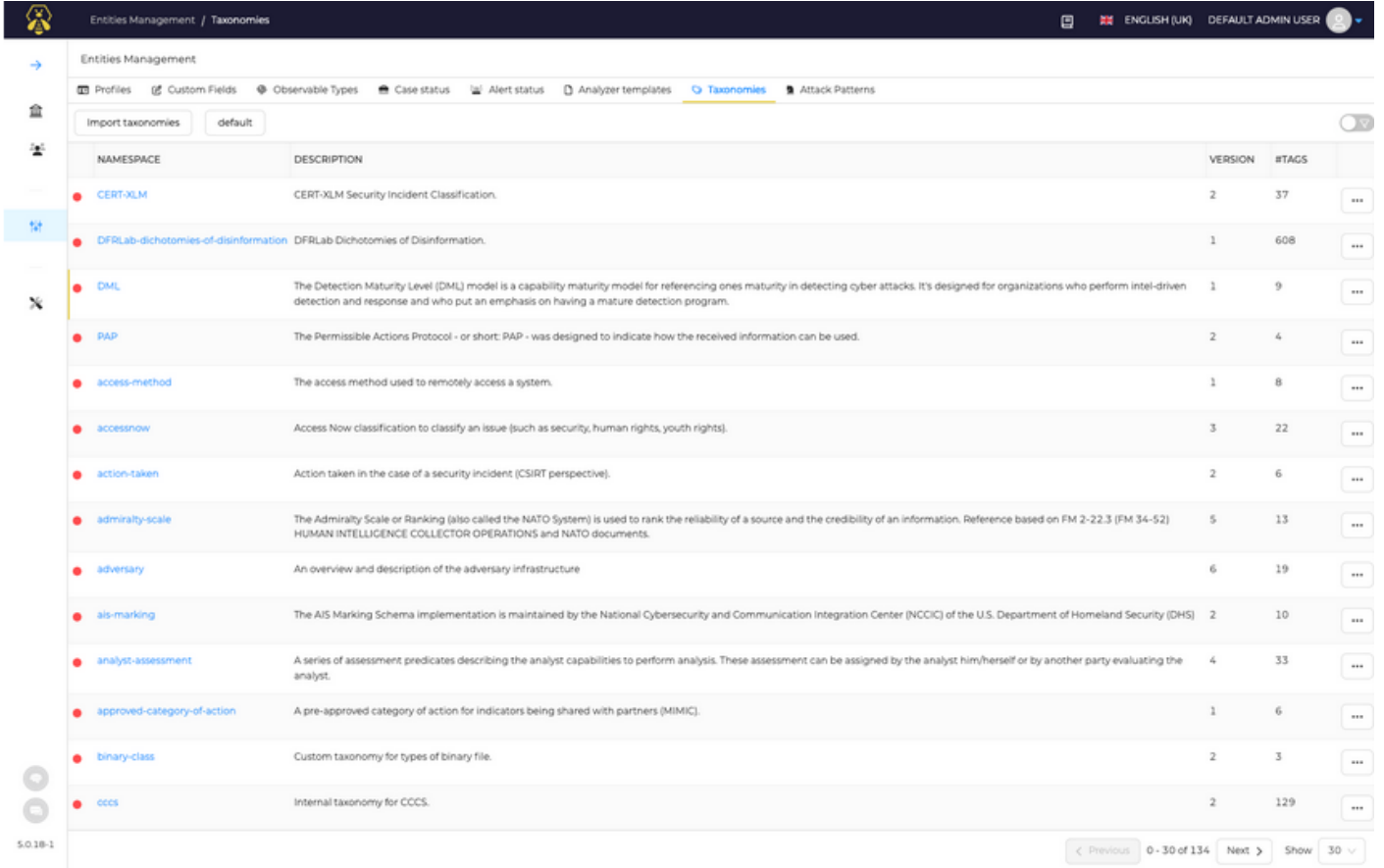


Sınıflandırmalar

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 'Entities Management / Taxonomies', a language selector set to 'ENGLISH (UK)', and a user profile for 'DEFAULT ADMIN USER'. Below the navigation bar, there are tabs for 'Profiles', 'Custom Fields', 'Observable Types', 'Case status', 'Alert status', 'Analyzer templates', 'Taxonomies' (which is active), and 'Attack Patterns'. Under the 'Taxonomies' tab, there are buttons for 'Import taxonomies' and 'default'. The main content area is a table with columns: 'NAMESPACE', 'DESCRIPTION', 'VERSION', and '#TAGS'. The table lists various taxonomies, each with a red dot icon in the 'NAMESPACE' column and a three-dot menu icon in the '#TAGS' column. The taxonomies listed are: CERT-XLM, DFRLab-dichotomies-of-disinformation, DML, PAP, access-method, accessnow, action-taken, admiralty-scale, adversary, ais-marking, analyst-assessment, approved-category-of-action, binary-class, and cccs. At the bottom of the table, there is a pagination bar showing '0 - 30 of 134' and a 'Show 30' dropdown menu.

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	

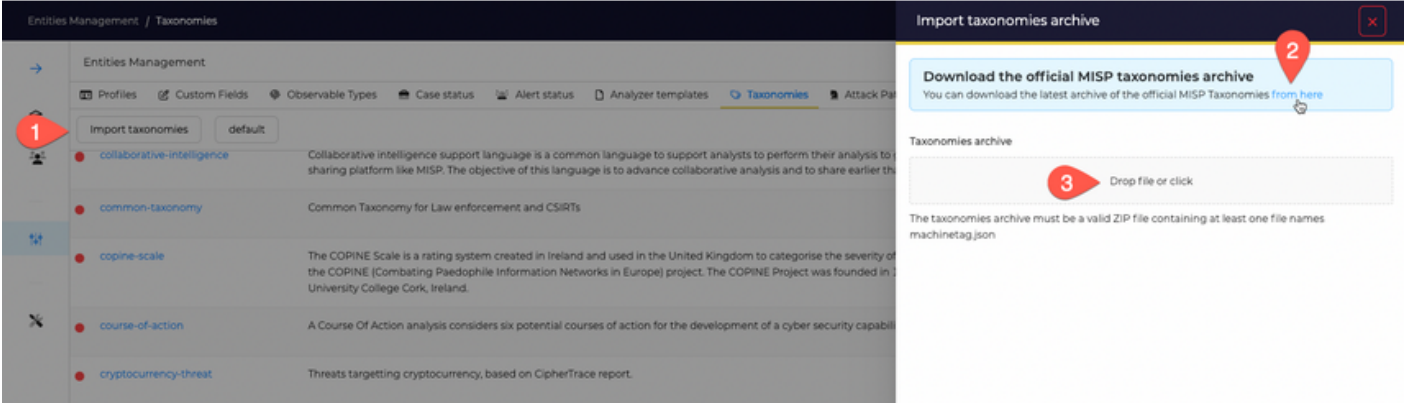
Bir Sınıflandırmayı Etkinleştirme veya Silme

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	14	...
csirt-americas	Taxonomia CSIRT Américas.	1	17	...
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	6	...
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>)

Revision #1

Created 9 April 2024 10:55:21 by Güldeniz Akca

Updated 9 April 2024 11:03:00 by Güldeniz Akca