Obje Parametreleri

[restSearch] Get a filtered and paginated list of objects:

Request Body Şeması:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
page	null	integer (int32)	>= 1	1
limit	null	integer (int32)	>= 0	10
quickFilter		string	Olayları herhangi bir etiket adı, olay açıklamaları, öznitelik değerleri veya öznitelik yorumlarıyla eşleştirmek için arama yapar.	"malware"
searchall		string	Olayları herhangi bir etiket adı, olay açıklamaları, öznitelik değerleri veya öznitelik yorumlarıyla eşleştirmek için arama yapar.	"ransomware"
timestamp		string (Timestamp)	^\d+$	"1617613315"
object_name		string	<= 131071 karakter	"malicious_file.exe"
object_template_uuid		string <uuid>	<= 36 karakter	"6f3c0d71-5b7a-46a9-a78b-29a146b5e3c7"
object_template_version		string	^\d+$	"1"
eventid		string	<= 10 karakter ^\d+$	"12345"
eventinfo		string	<= 65535 karakter	"Malware infection"
ignore		boolean	false	true
from		string veya null (DateRestSearchFilter)		
to		string veya null (DateRestSearchFilter)		
date		string veya null (DateRestSearchFilter)		
tags		Array of strings	veya null (TagsRestSearchFilter)	

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
last		integer veya string	veya null (LastRestSearchFilter)	
event_timestamp		string (Timestamp)	^\d+$	"1617613315"
publish_timestamp		string (Timestamp)	^\d+$	"1617613315"
org		OrganisationId veya OrganisationName		
uuid		string <uuid>	<= 36 karakter	"6f3c0d71-5b7a-46a9-a78b-29a146b5e3c7"
value		string	<= 131071 karakter	"1.2.3.4"
type		string	<= 100 karakter	"ip-src"
category		string	<= 255 karakter	"Network activity"
object_relation		string	veya null (ObjectRelationRestSearchFilter)	
attribute_timestamp		string (Timestamp)	^\d+$	"1617613315"
first_seen		string veya null (NullableMicroTimestamp)	^\d+$ veya null	"1617613315"
last_seen		string veya null (NullableMicroTimestamp)	^\d+$ veya null	"1617613315"
comment		string	<= 65535 karakter	"Malicious activity"
to_ids		boolean veya null (ToIDSRestSearchFlag)		
published		boolean	false	true
deleted		boolean	false	false
withAttachments		boolean	false	true
enforceWarninglist		boolean veya null (EnforceWarninglistRestSearchFilter)		
includeAllTags		boolean	false	true
includeEventUuid		boolean	false	true
include_event_uuid		boolean	false	true
includeEventTags		boolean	false	true
includeProposals		boolean	false	true
includeWarninglistHits		boolean veya null	false	true

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
includeContext		boolean veya null (IncludeContextRestSearchFlag)		
includeSightings		boolean veya null (IncludeContextRestSearchFlag)		
includeSightingdb		boolean veya null (IncludeSightingDbRestSearchFlag)		
includeCorrelations		boolean veya null (IncludeCorrelationsRestSearchFlag)		
includeDecayScore		boolean	false	true
includeFullModel		boolean	false	true
allow_proposal_blocking		boolean	false	true
metadata		boolean veya null (MetadataRestSearchFilter)		
attackGalaxy		string veya null (AttackGalaxyRestSearchFilter)		
excludeDecayed		boolean	false	true
decayingModel		string		
modelOverrides		object		
returnFormat		string	"json"	"json"

Add an object to an event:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	required	EventId (string) or UUID (string)	Etkinliğin UUID'si veya sayısal kimliği.	"12345"
objectTemplateId	required	ObjectTemplateId (string) or UUID (string)	Nesne şablonunun UUID'si veya sayısal kimliği.	"6f3c0d71-5b7a-46a9-a78b-29a146b5e3c7"

Request Body Şeması:

Attribute:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
category	-	string	Öznitelik kategorisi.	"Network activity"
value	-	string	Öznitelik değeri.	"192.168.1.1"
to_ids	-	boolean	IDS'ye rapor edilsin mi?	true
disable_correlation	-	boolean	Korelasyonu devre dışı bırak.	false
distribution	-	string	Yayımlanan etkinliği kimler görebilir?	"0"
comment	-	string	Özniteliğe yapılan yorum.	"Possible malware"
object_relation	-	string	Nesne ilişkisi.	"Related to incident"

Get object by ID:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
objectId	Gerekli	string	Nesnenin UUID veya sayısal kimliği.	"1234"

Delete object:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
objectId	Gerekli	string	Nesnenin UUID veya sayısal kimliği.	"1234"
hardDelete	Gerekli	string	Varlığın silinme yöntemi.	"0"

Revision #1
Created 12 April 2024 11:03:49 by İlayda Durlanık
Updated 12 April 2024 11:13:04 by İlayda Durlanık