Event Parametreleri

"Event" Kaynağını Aramak:

Request Body Şeması:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
page	Opsiyonel	integer or null <int32>	1'den büyük bir tamsayı.	1 veya null
limit	Opsiyonel	integer or null <int32>	0'dan büyük veya null.	10 veya null
value	Opsiyonel	string	131071 karaktere kadar olan bir dize.	"sample_value"
type	Opsiyonel	string	100 karaktere kadar olan bir dize.	"md5"
category	Opsiyonel	string	255 karaktere kadar olan bir dize.	"Internal reference"
org	Opsiyonel	OrganisationId (string) or OrganisationName (string)	Organizasyon kimliği veya adı.	"org_id" veya "org_name"
tags	Opsiyonel	Array of strings or null	Dize dizisi veya null.	["tag1", "tag2"] veya null
event_tags	Opsiyonel	Array of strings or null	Dize dizisi veya null.	["event_tag1", "event_tag2"] veya null
searchall	Opsiyonel	string	Etiket adları, etkinlik açıklamaları, öznitelik değerleri veya öznitelik yorumlarıyla eşleşen olayları arama.	"search_value"
from	Opsiyonel	string or null	Geçerli zaman filtreleri kullanılabilir.	"2024-01-01" veya null
to	Opsiyonel	string or null	Geçerli zaman filtreleri kullanılabilir.	"2024-12-31" veya null
last	Opsiyonel	integer or string or null	Son x zaman içinde yayımlanan etkinlikler.	7 veya "7d" veya null
eventid	Opsiyonel	string	10 karakterden az olan bir dize.	"12345"
withAttachments	Opsiyonel	boolean	Varsa eklerin base64 temsiliyle genişletir.	true veya false
sharinggroup	Opsiyonel	Array of strings or null	Paylaşım grubu ID(ler)i.	["sg_id1", "sg_id2"] veya null

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
metadata	Opsiyonel	boolean or null	Belirtilen sorgu kapsamının metadatasını sadece döndürür, içerilen veri atlanır.	true, false veya null
uuid	Opsiyonel	string <uuid>	36 karakterden az olan bir dize.	"uuid_value"
publish_timestamp	Opsiyonel	string	^\d+$	"timestamp_value"
timestamp	Opsiyonel	string	^\d+$	"timestamp_value"
published	Opsiyonel	boolean	false	true veya false
enforceWarninglist	Opsiyonel	boolean or null	Uyarı listesinin zorunlu olup olmayacağını belirtir. Eşleşen öznitelikler için engellenmiş alan ekler.	true, false veya null
sgReferenceOnly	Opsiyonel	boolean	Yalnızca paylaşım grubu kimliğini döndürür.	true veya false
requested_attributes	Opsiyonel	Array of strings	CSV dışa aktarmada seçilecek özelliklerin listesi.	["attr1", "attr2"]
includeContext	Opsiyonel	boolean or null	CSV dışa aktarmada etkinliklerin bağlam alanlarını ekler.	true, false veya null
headerless	Opsiyonel	boolean or null	CSV dışa aktarmada başlığı kaldırır.	true, false veya null
includeWarninglistHits	Opsiyonel	boolean or null	true, false veya null	true, false veya null
attackGalaxy	Opsiyonel	string or null	true, false veya null	true, false veya null
to_ids	Opsiyonel	boolean	true	true veya false
deleted	Opsiyonel	boolean	false	true veya false
excludeLocalTags	Opsiyonel	boolean or null	true, false veya null	true, false veya null
date	Opsiyonel	string or null	true, false veya null	true, false veya null
includeSightingdb	Opsiyonel	boolean or null	true, false veya null	true, false veya null
tag	Opsiyonel	string	255 karakterden az olan bir dize.	"tag_name"
object_relation	Opsiyonel	string or null	Öznitelik nesne ilişki değerine göre filtreleme.	"relation_value" veya null
threat_level_id	Opsiyonel	string	Tehdit seviyesini temsil eder.	"1" "2" "3" "4"
returnFormat	Opsiyonel	string	Yanıt yükü biçimi.	"json" veya "csv"

Add event:

Request Body Şeması:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
org_id	Opsiyonel	string	10 karakterden az olan bir dize.	"org_id"
distribution	Opsiyonel	string	Dağıtım seviyesi kimin etkinliği görebileceğini belirtir.	"0" "1" "2" "3" "4" "5"
info	Opsiyonel	string	65535 karaktere kadar olan bir dize.	"event_info"
orgc_id	Opsiyonel	string	10 karakterden az olan bir dize.	"orgc_id"
uuid	Opsiyonel	string <uuid>	36 karakterden az olan bir dize.	"uuid_value"
date	Opsiyonel	string	Tarih dizesi.	"2024-01-01"
published	Opsiyonel	boolean	false	true veya false
analysis	Opsiyonel	string	Analiz olgunluk seviyesini temsil eder.	"0" "1" "2"
attribute_count	Opsiyonel	string	^\d+$	"10"
timestamp	Opsiyonel	string or null	^\d+$ veya null	"timestamp_value" veya null
sharing_group_id	Opsiyonel	string or null	10 karakterden az olan bir dize veya null.	"sg_id" veya null
proposal_email_lock	Opsiyonel	boolean	true veya false	true veya false
locked	Opsiyonel	boolean	true veya false	true veya false
threat_level_id	Opsiyonel	string	Tehdit seviyesini temsil eder.	"1" "2" "3" "4"
publish_timestamp	Opsiyonel	string	^\d+$	"timestamp_value"
sighting_timestamp	Opsiyonel	string	^\d+$	"timestamp_value"
disable_correlation	Opsiyonel	boolean	Default: false	true veya false
extends_uuid	Opsiyonel	string or null	36 karakterden az olan bir dize veya null.	"extends_uuid_value" veya null
event_creator_email	Opsiyonel	string <email>	Etkinlik oluşturucu e-posta adresi.	"example@example.com"

Edit event:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Zorunlu	string	10 karakterden az olan bir dize.	"eventId"

Request Body Şeması:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
org_id	Opsiyonel	string (OrganisationId)	10 karakterden az olan bir dize, sadece rakamlar içerebilir.	"1234567890"
distribution	Opsiyonel	string (DistributionLevelId)	Dağıtım seviyesini belirten bir dize. 0 ile 5 arasında bir değer alabilir.	"2"
info	Opsiyonel	string	Olay hakkında bilgi içeren bir dize.	"Bu bir test olayıdır."
orgc_id	Opsiyonel	string (OrganisationId)	10 karakterden az olan bir dize, sadece rakamlar içerebilir.	"9876543210"
uuid	Opsiyonel	string <uuid>	En fazla 36 karakter içeren bir UUID dizesi.	"550e8400-e29b-41d4-a716-446655440000"
date	Opsiyonel	string	Tarih bilgisini içeren bir dize.	"2024-04-12"
published	Opsiyonel	boolean (PublishedFlag)	Olayın yayımlanıp yayımlanmadığını belirten bir boolean değer.	true
analysis	Opsiyonel	string (AnalysisLevelId)	Analiz olgunluk seviyesini belirten bir dize.	"1"
attribute_count	Opsiyonel	string (EventAttributeCount)	Olaya bağlı öznitelik sayısını belirten bir dize.	"5"
timestamp	Opsiyonel	string or null (NullableTimestamp)	Zaman damgasını içeren bir dize veya null değer.	"1649252400"
sharing_group_id	Opsiyonel	string or null (SharingGroupId)	10 karakterden az olan bir dize veya null değer, sadece rakamlar içerebilir.	"1234567890"
proposal_email_lock	Opsiyonel	boolean (EventProposalEmailLock)	Öneri e-postası kilidinin açık veya kapalı olup olmadığını belirten bir boolean değer.	false
locked	Opsiyonel	boolean (IsLocked)	Kilidin açık veya kapalı olup olmadığını belirten bir boolean değer.	true
threat_level_id	Opsiyonel	string (ThreatLevelId)	Tehdit seviyesini belirten bir dize.	"3"
publish_timestamp	Opsiyonel	string (Timestamp)	Yayımlama zaman damgasını içeren bir dize.	"1649252400"
sighting_timestamp	Opsiyonel	string (Timestamp)	Görünme zaman damgasını içeren bir dize.	"1649252400"
disable_correlation	Opsiyonel	boolean (DisableCorrelationFlag)	Korelasyonun etkin veya etkisiz olup olmadığını belirten bir boolean değer.	true

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
extends_uuid	Opsiyonel	string or null (ExtendsUUID)	En fazla 36 karakter içeren bir UUID dizesi veya null değer.	"550e8400-e29b-41d4-a716-446655440000"
event_creator_email	Opsiyonel	string <email>	Olayın oluşturulduğu e-posta adresi.	"example@example.com"

Delete event:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"

Search events:

Request Body Şeması:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
page	Opsiyonel	integer or null	Sorgunun başlayacağı sayfa numarası. 1'den büyük olmalı.	1 veya null
limit	Opsiyonel	integer or null	Sayfa başına dönecek maksimum öğe sayısı. 0 veya daha büyük olmalı.	10 veya null
sort	Opsiyonel	string or null	Sonuçları sıralamak için kullanılacak alan.	"date" veya null
direction	Opsiyonel	string or null	Sıralama yönü. "asc" (artan) veya "desc" (azalan). Varsayılan: "asc".	"asc" veya null
minimal	Opsiyonel	boolean or null	Varsayılan: false. Sadece attributeCount > 0 olan olayların minimal bir sürümünü döndürür.	true veya null
attribute	Opsiyonel	string or null	Verilen dizeyle eşleşen öznitelik değerlerine göre olayları filtreler.	"vulnerability" veya null
eventid	Opsiyonel	string	Olay kimliği.	"123456"
datefrom	Opsiyonel	string or null	Olay oluşturulma tarihi belirtilen tarihten büyük veya eşit olmalıdır.	"2024-01-01" veya null
dateuntil	Opsiyonel	string or null	Olay oluşturulma tarihi belirtilen tarihten küçük veya eşit olmalıdır.	"2024-03-31" veya null
org	Opsiyonel	string or null	Olayı oluşturan kuruluş adına göre olayları filtreler.	"ABC Corp" veya null

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventinfo	Opsiyonel	string or null	Olay bilgisi metni ile eşleşen olayları filtreler.	"suspicious activity" veya null
tag	Opsiyonel	string	Belirtilen etiket adlarından herhangi biriyle eşleşen olayları filtreler.	"malware"
tags	Opsiyonel	array of strings or null	Belirtilen etiket adlarından herhangi biriyle eşleşen olayları filtreler.	["malware", "phishing"] veya null
distribution	Opsiyonel	string	Olayın yayımlanmasının ve sonunda çekilmesinin kimler tarafından görülebileceğini belirtir.	"1"
sharinggroup	Opsiyonel	string or null	Paylaşım grubu kimliği.	"123456" veya null
analysis	Opsiyonel	string	Analiz olgunluk seviyesini temsil eder.	"2"
threatlevel	Opsiyonel	string	Tehdit seviyesini temsil eder.	"1"
email	Opsiyonel	string or null	Olay oluşturan kullanıcı e-postasıyla eşleşen olayları filtreler.	" user@example.com " veya null
hasproposal	Opsiyonel	string or null	Değişiklik önerileri içeren özniteliklere sahip olayları kontrol eder. Olası değerler: 0, 1.	"1" veya null
timestamp	Opsiyonel	string or null	Olay zaman damgası belirtilen tarihten büyük veya eşit olmalıdır.	"1648860516" veya null
publish_timestamp	Opsiyonel	string or null	Olayın yayımlanma zaman damgası belirtilen tarihten büyük veya eşit olmalıdır.	"1648860516" veya null
searchDatefrom	Opsiyonel	string or null	Tarihe göre filtreler, belirtilen tarihten daha yeni her şey alınır. YYYY-MM-DD biçiminde.	"2024-01-01" veya null
searchDateuntil	Opsiyonel	string or null	Tarihe göre filtreler, belirtilen tarihten daha eski her şey alınır. YYYY-MM-DD biçiminde.	"2024-03-31" veya null

Get event by ID:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"

Publish an event:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"

Unpublish an event:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"

Add event tag:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"
tagId	Gerekli	string	Sayısal bir kimliği temsil eden etiket kimliği.	"12345"
local	Opsiyonel	integer	Hedefe yerel olarak eklenip eklenmeyeceğini belirler.	0 veya 1 (Varsayılan değer: 0)

Remove event tag:

Path Parametreleri:

Parametre	Gerekli	Veri Türü	Açıklama	Örnek
eventId	Gerekli	string	Olayın benzersiz kimliği, ya bir dize ya da UUID olarak ifade edilebilir.	"123456" veya "550e8400-e29b-41d4-a716-446655440000"
tagId	Gerekli	string	Etiketin sayısal bir kimliğini temsil eder.	"12345"

Revision #5
Created 11 April 2024 19:24:51 by İlayda Durlanık
Updated 14 April 2024 16:13:48 by İlayda Durlanık