

Event

MISP'e *Event* eklemek, güvenlik profesyonellerinin tehditleri daha iyi anlamalarını, savunma stratejilerini geliştirmelerini ve genel olarak siber güvenliği artırmalarını sağlar.

- "Event Actions" menüsü içinde "Add Event" butonu kullanılarak yeni bir Event oluşturulabilir.

[Home](#) [Event Actions](#) [Dashboard](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#)

The event created will be visible to the organisations having an account on this platform, but not synchronised to other

[List Events](#)
[Add Event](#)
[Import from...](#)
[REST client](#)
[List Attributes](#)
[Search Attributes](#)
[View Proposals](#)
[Events with proposals](#)
[View delegation requests](#)
[View periodic summary](#)
[Export](#)
[Automation](#)

Add Event

Date

2024-04-07

Distribution *i*

This community only

Threat Level *i*

High

Analysis *i*

Initial

Event Info

Quick Event Description or Tracking Info

Extends Event

Event UUID or ID. Leave blank if not applicable.

Submit

- Distribution (Dağıtım):** Oluşturulan bilgilerin kısıtlı bir grupta ya da herkese açık dağıtılabileceği seçeneklerini belirler.
- Threat Level (Tehdit Seviyesi):** Oluşturulan *Event*'in düşük,orta ve yüksek olmak üzere 3 ayrı önem derecesini belirtir.
- Event Info (Olay Bilgisi):** Oluşturulan *Event* hakkında genel bilgileri içerir. Bu, olayın adı, tanımı, zaman damgası, kaynakları vb. içerebilir.
- GFI Sandbox(opsiyonel):** MISP *Event*'i, kötü amaçlı yazılım analizi için GFI Sandbox gibi bir çözümle ilişkilendirilebilir. Bu, tehditlerin analiz edilmesine ve kötü amaçlı faaliyetlerin tespit edilmesine yardımcı olabilir.

5. **Does it extend (Uzatma var mı)(opsiyonel):** Bu, MISP *Event'inin* genişletilip genişletilmediğini belirtir. Yani, *Event'e* daha fazla ayrıntı veya bağlantılar eklenip eklenmediğini ifade eder.

- "Submit" butonu ilgili alanları doldurduktan sonra bir sonraki aşamaya geçmek için kullanılır.
- *Event* oluşturulduktan sonra, "View Event" içinde *Event'e* ait özellikler belirlenebilir.

The event has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

Add Event to Collection

List Events

Add Event

DEMO -multi-domain

Event ID160

UUID6ebc51bd-eb34-4a4c-b710-c042c884502a

Creator orgORGNAME

Owner orgORGNAME

Creator useradmin@admin.test

Protected Event (experimental)Event is in unprotected mode. Switch to protected mode

Tags

Date2024-04-07

Threat LevelHigh

AnalysisInitial

DistributionThis community only

Warnings

Content: Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out.

Contextualisation: Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.

PublishedNo

#Attributes0 (0 Objects)

Last change2024-04-07 19:13:24

Modification map

Sightings0 (0) - restricted to own organisation only

PivotsGalaxyEvent graphEvent timelineCorrelation graphATT&CK matrixEvent reportsAttributesDiscussion

160: DEMO -multi-d...

Galaxies

previousnextview all

Scope toggleDeletedDecay scoreContextRelated TagsFiltering tool

DateContextPatternTimeValueTimeGalaxiesCommentCorrelateRelated EventsEvent hits

Revision #7

Created 7 April 2024 11:47:16 by İlayda Durlanık

Updated 7 April 2024 19:17:01 by İlayda Durlanık