



DFSA CYBER THREAT INTELLIGENCE PLATFORM (TIP)



MANUAL USER GUIDE

TABLE OF CONTENTS

DISCLAIMER	4
1. INTRODUCTION	5
1.1 PURPOSE OF THE USER GUIDE	5
1.2 ABOUT THE CYBER THREAT INTELLIGENCE PLATFORM INITIATIVE	5
1.3 PLATFORM TERMS OF USE	5
1.4 DEFINITIONS	6
2. HOW TO USE THE PLATFORM	8
2.1 PLATFORM OVERVIEW	8
2.2 DATA DISTRIBUTION AND SYNCHRONIZATION	8
2.2.1 HOW INFORMATION IS SHARED – DISTRIBUTION LEVELS	9
2.2.2 THE TRAFFIC LIGHT PROTOCOL (TLP)	10
2.3 CONSIDERATIONS FOR SHARING OF INFORMATION	11
3. HOW TO ACCESS THE PLATFORM	12
3.1 BEFORE YOU ACCESS THE PLATFORM	12
3.1.1 HOW TO REGISTER	12
3.1.2 I FORGOT MY USERNAME OR PASSWORD	12
3.2 ACCESSING THE PLATFORM	12
3.3 AFTER YOUR FIRST LOGIN	13

TABLE OF CONTENTS

4. HOW TO CONTRIBUTE	14
4.1 CREATING AN EVENT	14
4.2 ADDING ATTRIBUTES TO AN EVENT	16
4.2.1 ADDING ATTRIBUTES USING THE FREETEXT IMPORT TOOL	17
4.2.2 ADDING ATTRIBUTES MANUALLY	19
4.2.3 ADDING AN ATTACHMENT AS AN ATTRIBUTE	20
4.3 PUBLISHING EVENTS	20
4.4 PROPOSING CHANGES TO EXISTING EVENTS	21
4.5 DELEGATION	23
5. CONSUMING EVENTS	24
6. TECHNICAL DETAILS	25
6.1 IDS FLAG - INTRUSION DETECTION SYSTEM AUTOMATION	25
6.2 SIGHTINGS	25
6.3 TAGS	26
6.4 TAXONOMIES	26
6.5 GALAXY	27
7. CONTACT US	28

DISCLAIMER

IMPORTANT – PLEASE READ BEFORE PROCEEDING TO USE THIS GUIDE

1. This guide is available to Participants for general informational use only. The DFSA assumes no responsibility or liability for any errors or inaccuracies in this guide or omissions.
2. The DFSA expressly reserves the right to make changes to this guide. The DFSA makes no commitment to update or keep current the information in this guide. However, the DFSA will try to provide Participants with notices of any changes to this guide by email or by display on the Platform.
3. The DFSA is not responsible for the results of any actions taken by Participants based on information contained in this guide. The DFSA accepts no responsibility whatsoever for misrepresentation by any person whatsoever of the information contained in this guide. The DFSA expressly disclaims all liability and responsibility to any person, whether a reader of this guide or not, in respect of claims, losses, liability or damage or any other matter, either direct or consequential arising out of or in relation to the use and reliance, whether wholly or partially, upon any information contained in this guide.
4. The DFSA does not warrant that the Platform will work properly as described in this guide and makes no representations, warranties or guarantees of any kind regarding the availability or operation of the Platform or that the Platform will be error-free. Please refer to the DFSA Cyber Threat Intelligence Platform - Participant Terms and Conditions of Use (the “Terms”) for further clarification.
5. This guide is not any form of, and must not be relied upon on any basis whatsoever, as legal, tax, financial, professional or any other form of advice and is provided on a general, non-binding basis only. Participants should consult and seek advice from their own appropriate legal and other professional advisers as they deem appropriate.
6. In the event of any conflict or inconsistency between the Terms and this guide, the Terms shall prevail.
7. Links to websites may be included on the Platform, in the Terms or in this guide. The Participant is solely responsible for access to any linked website. The DFSA does not accept any responsibility or liability whatsoever for the content of any third party websites. The inclusion of a link to another website on the Platform, the Terms or in this guide is for general information purposes only and does not imply any relationship or association between the DFSA and the owner of the linked website or any endorsement, sponsorship or approval by the DFSA of the linked website or its contents. The DFSA does not control or monitor these linked websites and shall not be responsible for any materials, information or content posted on these linked websites, including any use of web measurement tools, customisation technologies, cookies, viruses or other harmful elements.
8. Please let us know if you find any information in this guide that is incorrect, misleading, or incomplete. Otherwise, we would appreciate any comments or suggestions you may have concerning this guide.

1. INTRODUCTION

1.1 PURPOSE OF THE USER GUIDE

This Manual User Guide (this guide) is a generic document designed to be read by Participants of the DFSA Cyber Threat Intelligence Platform (the “**Platform**”). It provides informal guidance on how to (i) use the Platform; (ii) make use of the cyber intelligence on the Platform; and (iii) contribute to the Platform.

This guide is not exhaustive and is not intended to be a complete or comprehensive guide for all matters or issues or relevant information concerning the Platform or any particular Participant or scenario.

The **User Integration Guide** and the **User Case Guide** are intended to work together with this guide. Accordingly, in order to maximise the benefit of each of these guides, it is suggested that Participants read them in the following order:

1. User Guide;
2. Use Case Guide; and
3. Integration Guide.

1.2 ABOUT THE CYBER THREAT INTELLIGENCE PLATFORM INITIATIVE

The DFSA launched the Platform to help businesses in the DIFC implement appropriate safeguards to mitigate against cyber risks and to provide enriched cyber threat intelligence to Participants. The Platform is hosted by the DFSA and will be managed and operated by an independent third party consultant who will provide intelligence analysis, curation and publication for the operation of the Platform and work towards the enhancement of cyber threat intelligence. The use of the Platform is voluntary and at no cost.

The Platform is a result of ongoing cooperation and collaboration with various government authorities, private companies and service providers. This initiative is aligned with the UAE National Cybersecurity Strategy and the Dubai Cyber Security Strategy, both of which aim to strengthen the position of Dubai and the United Arab Emirates as a world leader in innovation, safety and security.

The Platform is based on an open source project called MISP.
Further details can be located at: <https://www.misp-project.org/>

1.3 PLATFORM TERMS OF USE

Each Participant is required to have read, understood and accepted the “**DFSA Cyber Threat Intelligence Platform Participant Terms and Conditions of Use**” (the “**Terms**”) before accessing and using the Platform and the related User Guides, including this Manual User Guide.

The access to and use of this Manual User Guide is subject always to the Terms and the Disclaimer in this guide.

1.4 DEFINITIONS

This section defines common terms used in this document and their respective definitions.

TERM	DEFINITION
Attribute	Evident and specific information, which is expected to be mostly technical in nature, about an Event, which has been generated, collected or observed by people or systems.
Campaign	Set of cyber activities carried out by threat actors using specific techniques.
Community	Means the particular forum in which a Participant elects to store or share data.
Connected Community	Means the Community that allows for participation and sharing of data by Participants situated in the DIFC and specific Participants situated outside the DIFC, such as a Contributor or the Consultant.
Cyber Threat Intelligence or CTI	Actionable evidence-based knowledge, indicators, and facts about an existing or emerging threat.
DIFC	The Dubai International Financial Centre.
DIFC Community	Means the Community that allows for participation and sharing of data by Participants situated in the DIFC.
Event	A record in the Platform that has Attributes and other types of data and metadata attached to it. An Event describes a cyber threat and is usually accompanied with context and information on how to protect against it.
Indicators of Compromise or IOC	These serve as evidence of potential intrusions on a host system or network. IoCs enable information security (InfoSec) professionals and system administrators to detect intrusion attempts or other malicious activities. Security researchers use IoC's to analyse a malware techniques and behaviors. IoCs also provide actionable threat intelligence which can be shared within the community to further improve an Participant's incident response and remediation strategies.
Intrusion Detection System or IDS	A device or software that monitors a network or systems for malicious activity and alerts when such activity is discovered
Malware Information Sharing Platform or MISP	The Malware Information Sharing Platform, an open source information-sharing platform MISP that facilitates the sharing of information amongst entities and information sharing communities, commonly used for sharing Cyber Threat Intelligence and which is released under the Affero General Public Licence AGP Licence .
Manual User Guide	Means this guide intended to explain to Participants how to use the Platform.
MISP Communities	The Community that allows for participation and sharing of data by users or entities that use the MISP.

TERM	DEFINITION
Participant	Means any natural or legal person: (i) approved by the DFSA to access and use the Platform for the Purpose; and, (ii) who agrees to use the Platform in accordance with the Terms.
Platform	Means the MISP adopted and hosted by the DFSA to facilitate the detection and prevention of cyber threats in the DIFC.
Purpose	Means the purpose of the Platform, which is to store and share information on Events in accordance with the Terms.
Security Information and Event Management or SIEM	Software products that provide real-time analysis of security alerts generated by applications and network hardware.
Terms	Means the “ DFSA Cyber Threat Intelligence Platform Participant Terms and Conditions of Use ” required to be read, understood and agreed by each Participant before accessing and using the Platform and the User Guides, including this guide.
Threat Actor	Also called a malicious actor, is an entity that is partially or fully responsible for an incident that impacts or has the potential to impact a Participant’s security.
Traffic Light Protocol or TLP	The protocol adopted by the Platform for the classification of sensitive information and which offers Participants specific control parameters on the sharing of information on the Platform, and which is available at TLP Protocol .
TTP	Tactics, Techniques and Procedures, these describe how Threat Actors orchestrate, manage and execute attacks.
User Case Guide	Means the practical manual intended to explain to Participants how to utilise the Platform and the data it provides as a resource.
User Guides	Means each of the User Case Guide, User Integration Guide and the User Manual Guide.
User Integration Guide	Means the practical manual intended to explain to Participants how to integrate the Platform within their information systems.
Workspace	A designated area with a collection of Events.

2. HOW TO USE THE PLATFORM

2.1 PLATFORM OVERVIEW

The objective of the Platform is to support and foster the sharing of structured information amongst Participants. It will support Participants in their day-to-day operations by helping them share structured information efficiently and prioritise responses to cyber threats. The Platform will also facilitate information exchanges amongst Participants, Contributors and other territorial and worldwide sources that contribute focused threats intelligence.

The Platform provides functionality to support the exchange of information but also the consumption of information by NIDS, log analysis tools, SIEMs and other security controls.

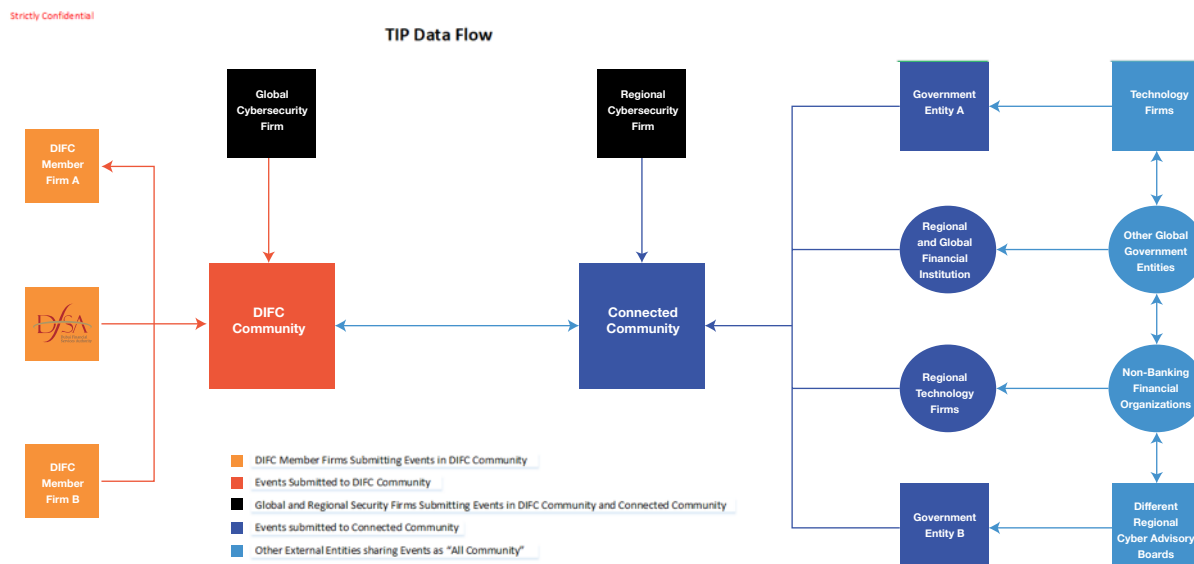
The Platform will host Cyber Threat Intelligence from government entities, leading international cyber experts and Participants. This intelligence includes IOC, TTP, Campaign and Threat Actor.

2.2 DATA DISTRIBUTION AND SYNCHRONIZATION

When sharing Cyber Threat Information on the Platform, each Participant should: (i) decide the level of distribution to be applied to the particular information by electing a specific Community for the storage and sharing of that information; and, (ii) signal, via the Traffic Light Protocol, how widely the Participant elects to circulate the information beyond the chosen Community.

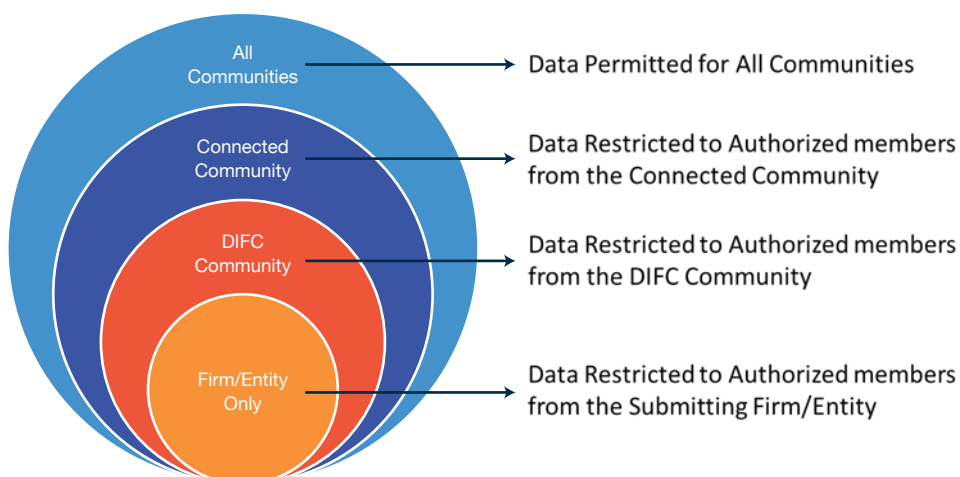
The Platform will be connected to other Cyber Threat Intelligence platforms to facilitate Cyber Threat Intelligence exchange. Any communication between platforms must be authorised to ensure appropriate distribution of information between systems. Below is a representation of the extended Community surrounding the Platform and description of the flow of data (Events and Attributes).

2.2.1 HOW INFORMATION IS SHARED – DISTRIBUTION LEVELS



The Platform has various distribution options. The list below summarises the “Distribution Levels” that are available for Events and Attributes within the Platform. These Distribution Levels control how data is distributed and shared amongst Participants.

The Distribution Levels are as follows:



“Firm/Entity” (Your organisation only)

This setting will only allow members of the Participant to see this Event. Events with this setting will not be synchronised to other Communities or platforms.

“DIFC Community” (This Community only)

Participants that are members of the DIFC Community will be able to see the Event.

Connected Communities

Participants that are members of the Connected Community will be able to see the Event.

MISP Communities

This Community shares the Event with all users or entities that use the MISP.

IMPORTANT: Prior to a Participant publishing the Event on the Platform, the Event will not be distributed/shared within any Community, rather, the Event will remain on the Participant's own account unless and until the Participant elects to publish the Event on the Platform.

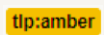
2.2.2 THE TRAFFIC LIGHT PROTOCOL (TLP)

The Traffic Light Protocol (TLP) is an internationally recognised set of guidelines that define how information is to be shared between Participants. TLP also defines how that information should be used by the recipients [Participants] and provides guidance on further distribution. A more detailed explanation of the protocol can be found [here](#).

Applying the TLP to Events is important for all Events and Participants are encouraged to apply a single TLP to each Event. TLP can be applied to Attributes, however, this not required nor encouraged.

The TLP complements the Distribution Levels by providing guidance for Participants with access to the information. Distribution Levels govern how the Platform exchanges information with connected systems; the TLP governs how Participants (and organisations) share information available to them, visible within the Platform as Events.

The TLP contains the following four (4) designations which are implemented as tags in the Platform:

TLP	CRITICALITY	HOW TO SHARE	PLATFORM TAG
TLP:RED	Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not restricted. The information could severely impact an organisation's reputation or operations if misused. Treat with great care.	Do not copy and paste, or forward to anyone; In most circumstances, TLP:RED should be exchanged verbally or in person.	
TLP:AMBER	Limited disclosure, restricted to participants' organizations The information presents a risk to an organisation's reputation or operations if known. Treat with sensitivity within your organisation.	CERTs sending indicators of compromise to an organization (1-to-group, limited). Recipients may only share TLP:AMBER information with members of their own organisation.	

TLP	CRITICALITY	HOW TO SHARE	PLATFORM TAG
TLP:GREEN	Limited disclosure, restricted to the community. Information given to a community or a group of organisations. The information is useful for you, your organisation and your partners and industry peers. The information is intended to be shared to benefit your extended community.	Can be shared within your organisation and or industry peers, or partners; Must not be shared publicly or in public forums.	
TLP:WHITE	The information does not present any known or foreseeable risk to an organisation and is intended to be shared widely and freely.	No restrictions on distribution. This information can be shared publicly or in public forums.	

[FIRST.org, TLP v1.0].[CIRCL TLP]

2.3 CONSIDERATIONS FOR SHARING OF INFORMATION

Sharing information outside your organisation means that you accept a certain level of responsibility concerning the information shared. Within your organisation, and within the DIFC, other responsibilities might also be applicable (e.g. applicable privacy, confidentiality and personal data protection laws). Please refer to the [Terms](#) which set out certain rights, responsibilities and obligations that apply to Participants when sharing information.

For further details on MISP's sharing guidelines on information sharing practices, please refer to the following link <https://github.com/MISP/MISP/wiki/Sharing-guidelines>.

3. HOW TO ACCESS THE PLATFORM

The Platform is accessible like any other website via a web browser (Internet Explorer, Mozilla Firefox or Google Chrome).

3.1 BEFORE YOU ACCESS THE PLATFORM

The **Terms** govern the access and use of the Platform and are legally binding on all Participants. Please read the Terms carefully as they contain important information regarding a Participant's legal rights and obligations. It is important that you read and understand the Terms carefully and in their entirety before agreeing to accept them as a Participant, and before accessing and using the Platform.

3.1.1 HOW TO REGISTER

Registration for the Platform is via the DFSA ePortal. Please use your Firm's login user name and password to access the ePortal and then follow the links for TIP registration.

3.1.2 I FORGOT MY USERNAME OR PASSWORD

In the event a Participant forgets their user name or password, please contact the DFSA Platform support team via e-mail on tip@dfsa.ae with the subject line: "Password Reset" to reset your Platform login credentials.

3.2 ACCESSING THE PLATFORM

Visit: <https://tip.dfsa.ae> The URL is accessible through a web browser connected to the internet.

Step 1: Please enter the username and password as suggested in the below Figure 1.2.1

Step 3: Click on login

Welcome to the DFSA Threat Intelligence Platform

DFSA
Dubai Financial
Services Authority

Login

Email Password

Please Enter "User ID" Please Enter "Password"

Login

Click Login

Powered by MSP - 2020-01-14 09:37:07

Figure 1.2.1

3.3 AFTER YOUR FIRST LOGIN

When a Participant logs in for the first time, the Platform will request the Participant to change their password. Please refer to Step 1, Step 2 & Step 3 in Figure 1.2.2 below.

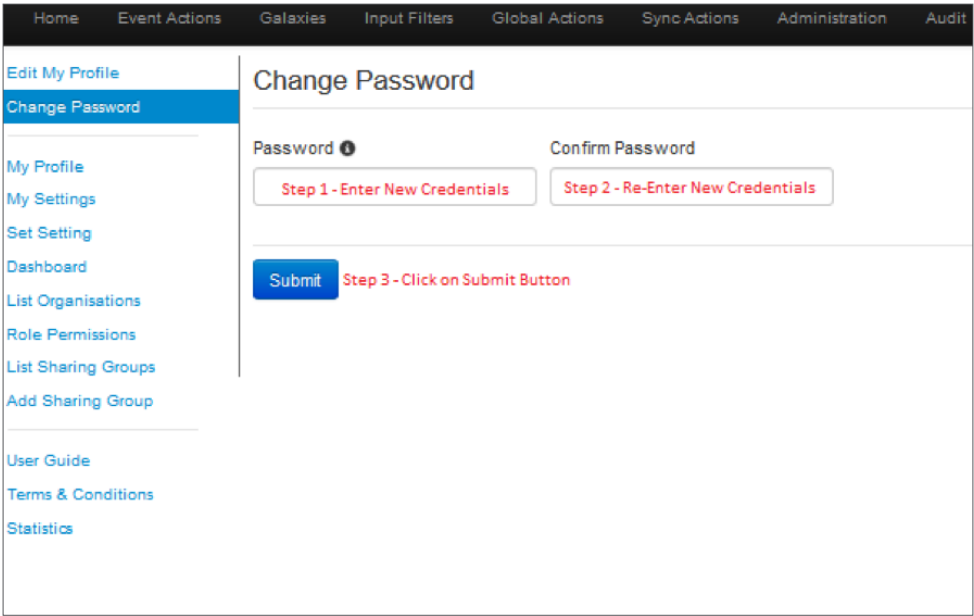


Figure 1.2.2

Upon logging on to the Platform, and once you have updated your password, a Participant may then create Events and add Event ‘Attributes’. The procedures for creating Events and adding Attributes is described in [Section 4](#) of this guide.

4. HOW TO CONTRIBUTE

There are multiple ways to contribute to the Platform. These are as follows:

- Creating and Publishing new Events; and
- Proposing Changes to existing Events;

An Event is a record that is created by a Participant and which can be shared or restricted based on the sharing model illustrated in [section 2.2.1](#)

Information is contributed to the Platform via the following steps:

1. Creating an Event;
2. Adding Attributes to the Event created;
3. Publishing the Event;

In addition to the above, Participants may also:

- a. Propose changes to existing Events; and
- b. Delegate Events.

The following sections describe the process of contributing via Events and Attributes, publishing, proposing changes and delegating Events.

4.1 CREATING AN EVENT

You only need to include a few details to register a new Event. Further details can be specified after the Event has been added. These details are referred to as 'Attributes'.

Once you have successfully logged into the Platform, you will be presented with the Platform Workspace. Click on the "Event Actions" menu (within the top menu bar) and select "List Events". You can also click on "Home" within the top menu bar.

1. Click "Add Event";
2. Fill in the template with necessary details like Date, distribution level, Threat level and analysis stage.
3. The analysis stage includes three levels:
 - a. Initial: Basic Information about an ongoing incident or Event.
 - b. Ongoing: Information about an ongoing incident or Event.
 - c. Completed: Complete information about an ongoing incident or Event.
4. "Threat Level" is one of the following and summarises the threat level of the Event:
 - a. Low: Encouraged, but not recommended to ignore.
 - b. Medium: Must be actioned as a priority.
 - c. High: Must be actioned with the highest priority.
 - d. Undefined: Not yet known or unable to be classified.
5. Click on the "Add" to create an Event.

Please refer to Step 1, Step 2, Step 3 & Step 4 in below figure to create an Event:

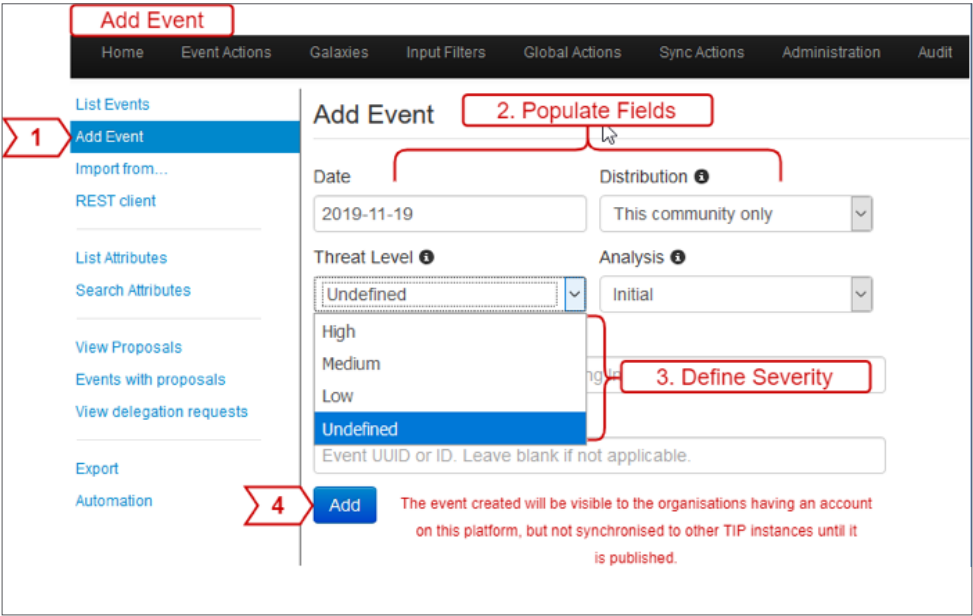


Figure 1.8.2

Once you have created the Event, it is important to add a single TLP tag. For more information about TLP, refer to the section above titled [The Traffic Light Protocol](#). To add an appropriate TLP tag, click on the add tag icon (it is a tiny globe with a 'plus' sign):

Click on “All Tags” and type “tlp:”. A list of options will appear underneath the text you typed. Select the appropriate TLP (e.g. “tlp:green”) as per the screenshot below:

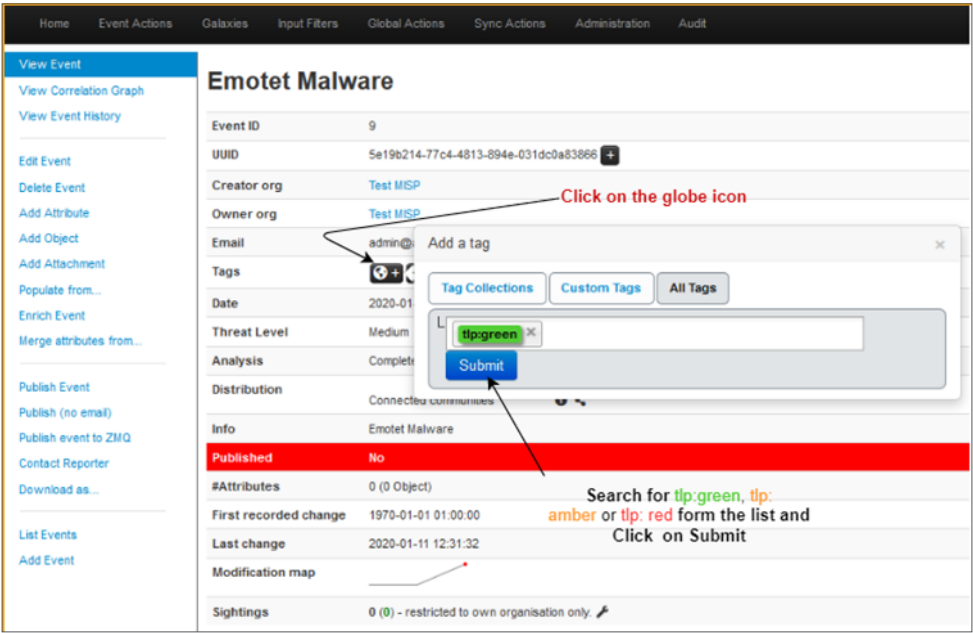


Figure 1.8.3

Once you have created the Event, and assigned the TLP, click on the “Home” tab in the top navigation bar. This will return you to the Event Workspace. The new Event created will appear as below in the Figure 1.8.4:

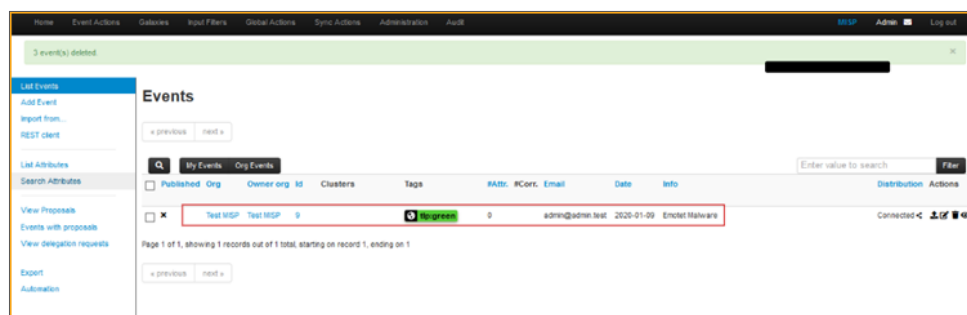


Figure 1.8.4

4.2 ADDING ATTRIBUTES TO AN EVENT

An Attribute is a property of an Event. Attributes can be network indicators (e.g. IP address), system indicators (e.g. a string in memory). The most important properties of an Attribute are:

- The **Type** (e.g. MD5, URL) which describes the data and information stored in the Attribute.
- The **Category** (e.g. Payload delivery) which adds limited context about the Attribute.
- The **IDS flag** this flag indicates whether an Attribute should be used for detection/protection in other systems. If the IDS flag is not present, the Attribute is still useful for contextualisation, investigation and correlation within the Platform.

In addition to the above, every Attribute also has the following properties:

- “Similar Attributes”** – highlights one or more Event IDs if the Attribute has been seen in other Events, otherwise will be blank.
- “Disable Correlation”** – Prevents correlation of this Attribute across future Events. There is no need to change this setting.
- “Distribution”** – Tells the Platform to set the Distribution Level of this Attribute to something different (different from the Event). There is no need to change this – leave as “Inherit event”.
- “Comment”** – Can be used to add a comment regarding this Attribute – e.g. origin, context.
- “Tags”** – Used to add specific tags to this Attribute. This can safely be left blank.

The following sections describe ways to add Attributes to an Event:

- [Adding Attributes using the Freetext Import tool](#)
- [Adding Attributes Manually](#)
- [Adding an Attachment as an Attribute](#)

4.2.1 ADDING ATTRIBUTES USING THE FREETEXT IMPORT TOOL

If you have a list of indicators from which you wish to generate Attributes quickly, the Free-text import tool can analyse and extract relevant indicators from a large amount of text. Some examples of text containing indicators are:

- a. A large amount of text from a document, advisory or report (mixture of indicators and other text).
- b. A list of indicators (e.g. IP addresses) from a system or control.
- c. An email describing indicators (perhaps with other text or context).

Once you have created an Event using the instructions from the previous Section 4.1, you can quickly add one or more attributes using the following procedure.

Step 1: Click on “Populate from...”

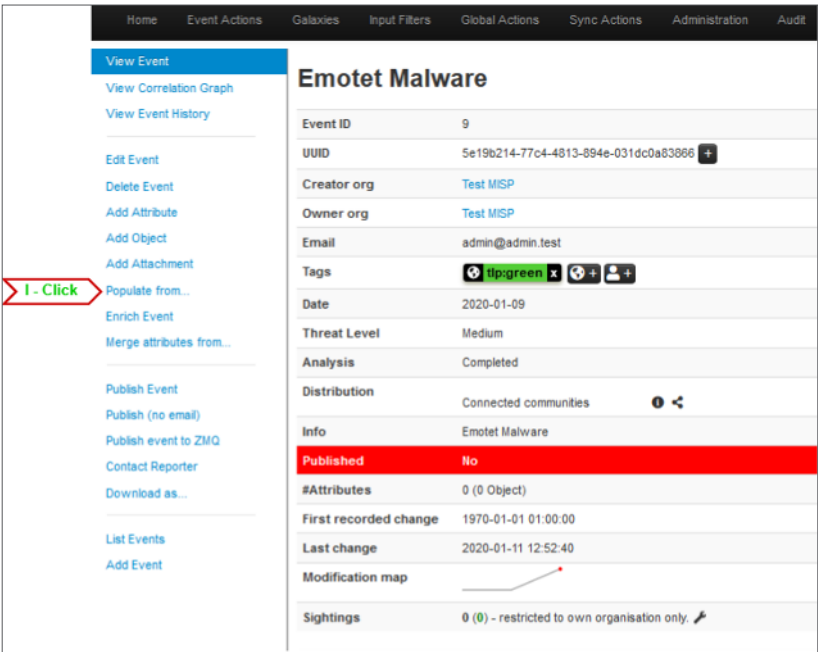


Figure 1.8.5

Step 2: Click “Freetext Import”

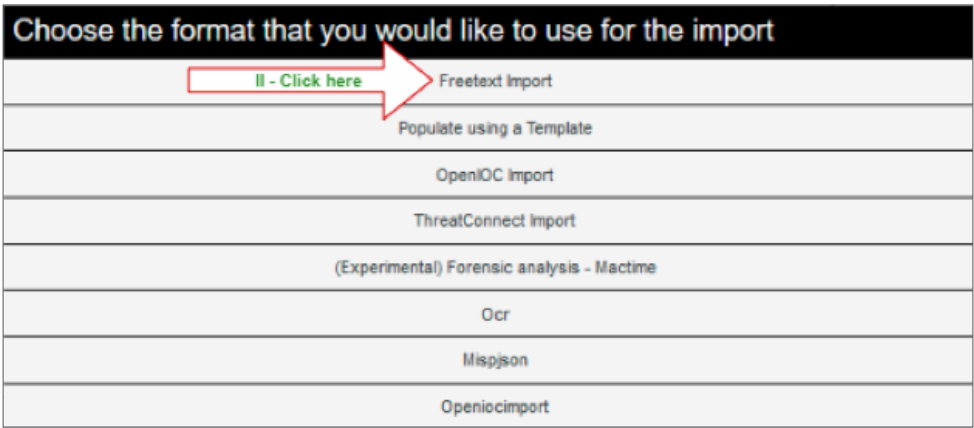


Figure 1.8.6

Step 3: Copy the text (e.g. from an email or PDF) and paste the text into box:

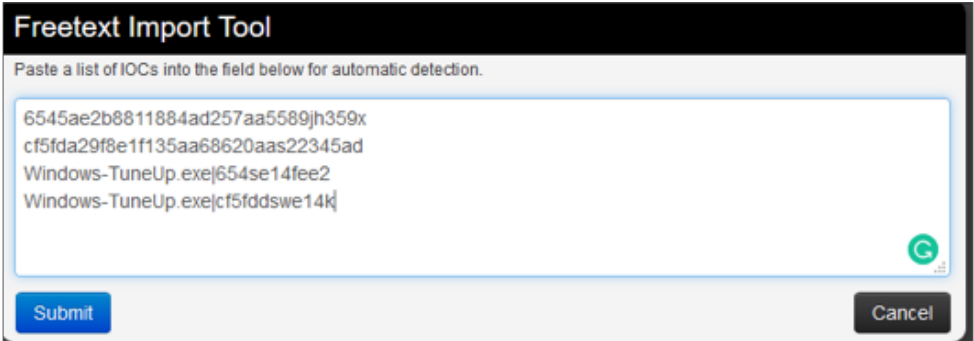


Figure 1.8.7

There may be more than one category/type combination that is valid for some Attributes. The Platform will analyse and recommend the most relevant type and/or category for all Attributes. You can alter the properties if you disagree with the results.

Freetext tool results are displayed below for further amendments if necessary.

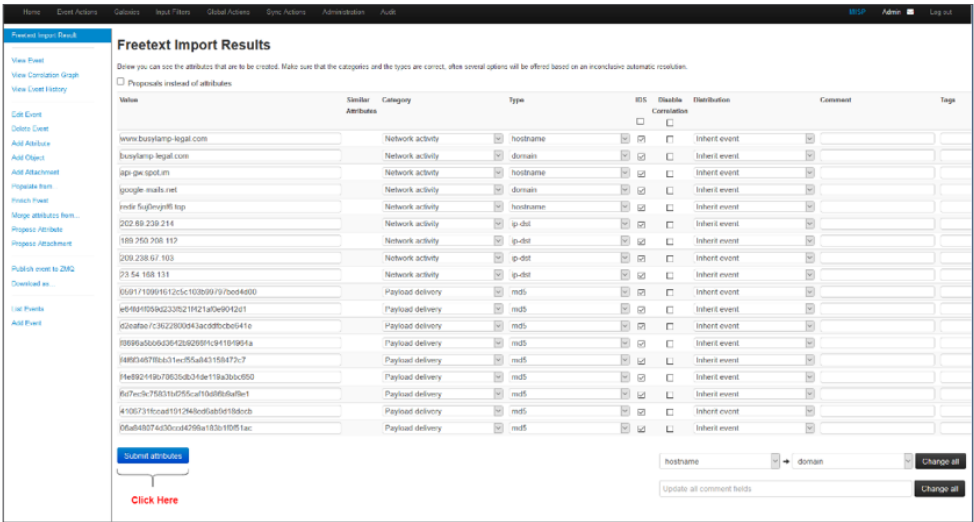


Figure 1.8.11

In the above screenshot, the Platform has detected and recommend the category and type associated to each Attribute. It has set the IDS by default (enabled) and has set all the properties of each Attribute.

The screen provides an opportunity to validate the Attribute details, it is recommended that you review the IDS flag and ensure it is only enabled for Attributes that you recommend others to take action on, for example blocking a malicious IP on a firewall.

If the results of Platform were not what you expected, or you wish to set an Attribute with a specific type or category, you can modify one or all Attributes. Using this form, you can also change each Attribute individually, or change all Attributes at the same time using the option on the bottom right of the form, “Change all”.

To select a different category or type, use the drop-down menu as shown in the screenshot below:

If this Attribute has been “seen” before (in another Event), the Platform will display one or more numbers (Event IDs) in the “Similar Attributes” column. Move your mouse pointer over the Event ID to see the details of each Event ID.

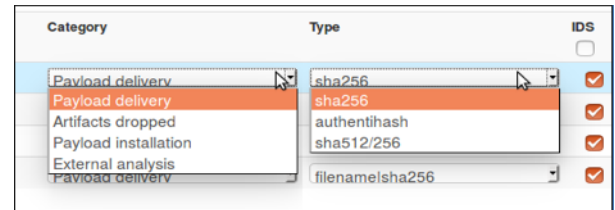
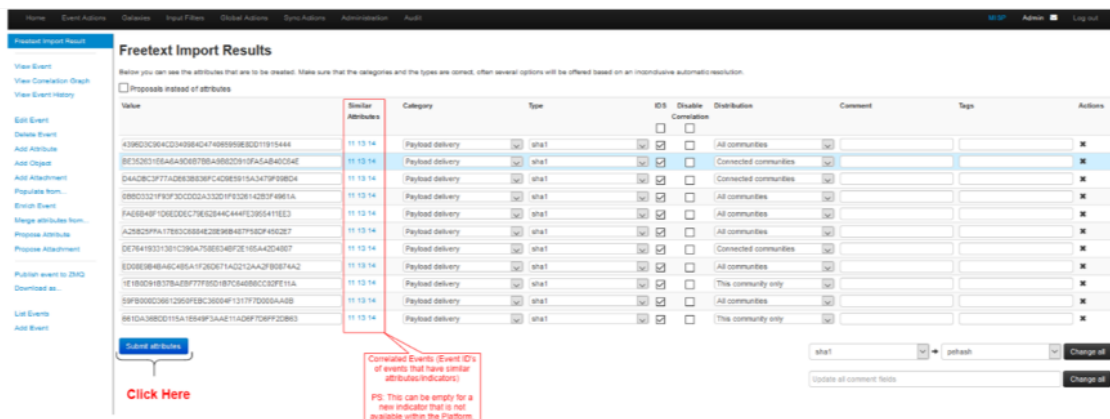


Figure 1.8.12

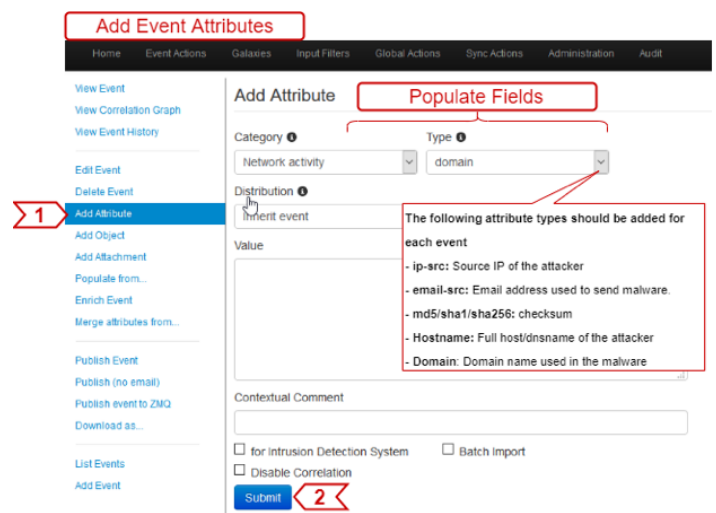
The screenshot below shows a set of Attributes that have been “seen” before by the Platform in existing Events:



Finally, click on the blue “**Submit Attributes**” button to complete the process and add the Attributes to the Event.

4.2.2 ADDING ATTRIBUTES MANUALLY

To add Attributes manually, click on the “Add Attribute” option, located above “Populate From...”. This screen will ask you to manually select all properties – the Platform will not recommend types or categories. The screenshot below shows the basic steps to add an Attribute manually, setting the Category and Type and clicking Submit to add the Attribute to the Event:



4.2.3 ADDING AN ATTACHMENT AS AN ATTRIBUTE

Attachments are often the source of Attributes. One or more attachments (e.g. PDF) can be added to a specific Event. An attachment can be a report that supports an Event, providing useful context to an Event.

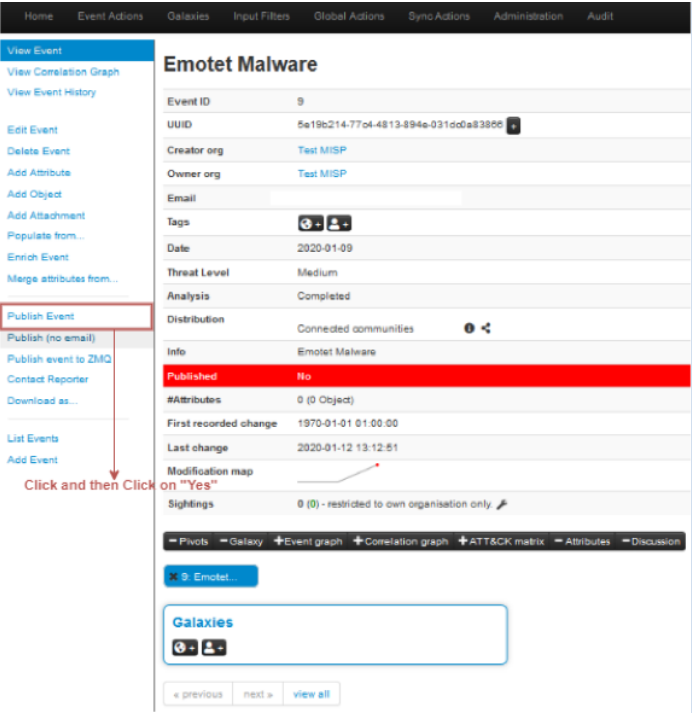
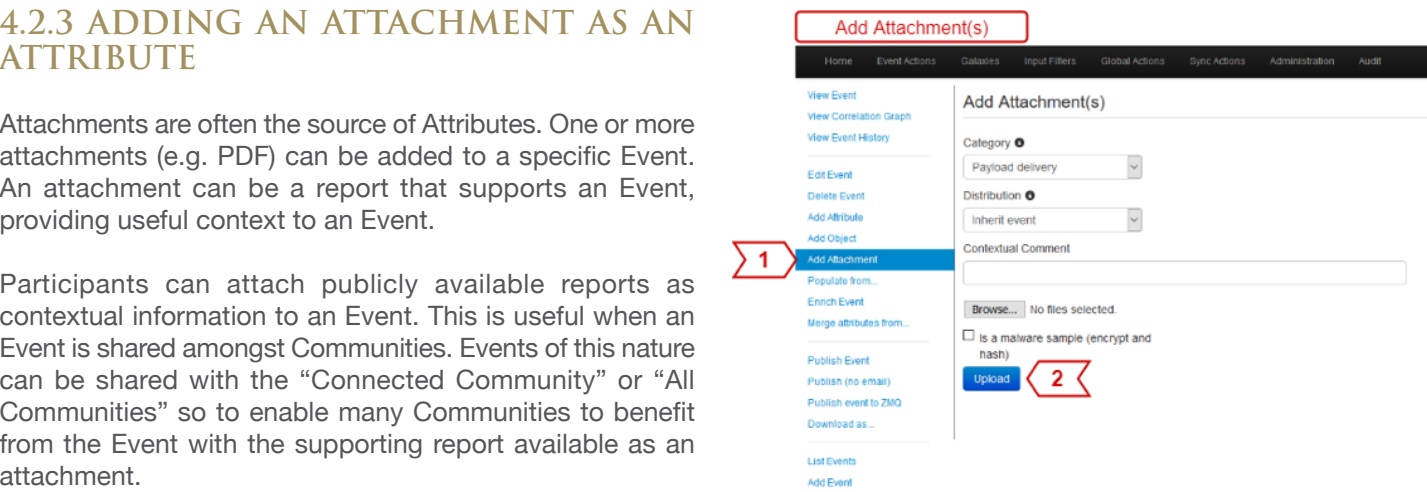
Participants can attach publicly available reports as contextual information to an Event. This is useful when an Event is shared amongst Communities. Events of this nature can be shared with the “Connected Community” or “All Communities” so to enable many Communities to benefit from the Event with the supporting report available as an attachment.

Follow steps 1 & 2 as per the screenshot below to add attachments to an Event:

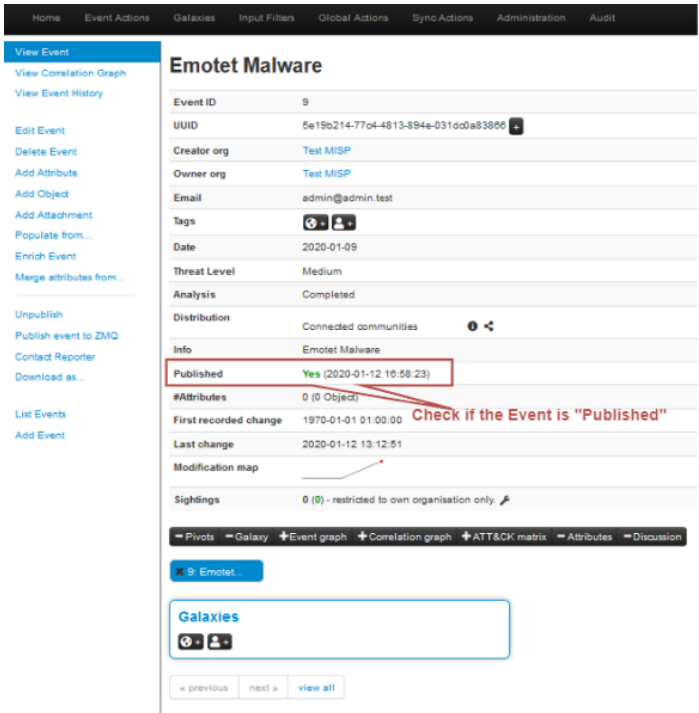
4.3 PUBLISHING EVENTS

Publishing of Events is an important and integral part of the Platform. Every Event should be published unless there is a specific reason to delay or avoid Publication. To Publish an Event click on the “Publish Event” link from the left-hand menu when viewing any single Event:

Publishing an Event makes it available to other participants on the Platform, according to the chosen level of distribution (i.e. Community). Refer to the Section titled “How Information is Shared – Distribution Levels” for more information on the Distribution Levels and how information is shared.



Once an Event is published, you may review the “Published” field to see when the Event was published:



4.4 PROPOSING CHANGES TO EXISTING EVENTS

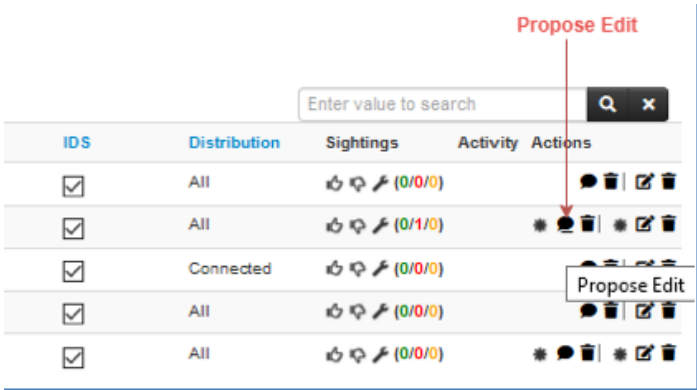
In order to ensure the integrity and accuracy of the Cyber Threat Intelligence on the Platform, the modification option for that Event is only available for a Participant who created the particular Event.

In addition, the Platform allows Participants who have access to an Event created by another Participant to also make proposals for changes to that Event.

Any proposal for change to an Event is reported back to the original creator of the Event. The original creator of the Event may accept or discard the proposal for change. Either way, the outcome of this decision will be disseminated to all interconnected platforms where the Event is present. Proposals for changes to an Event are typically used for the following reasons:

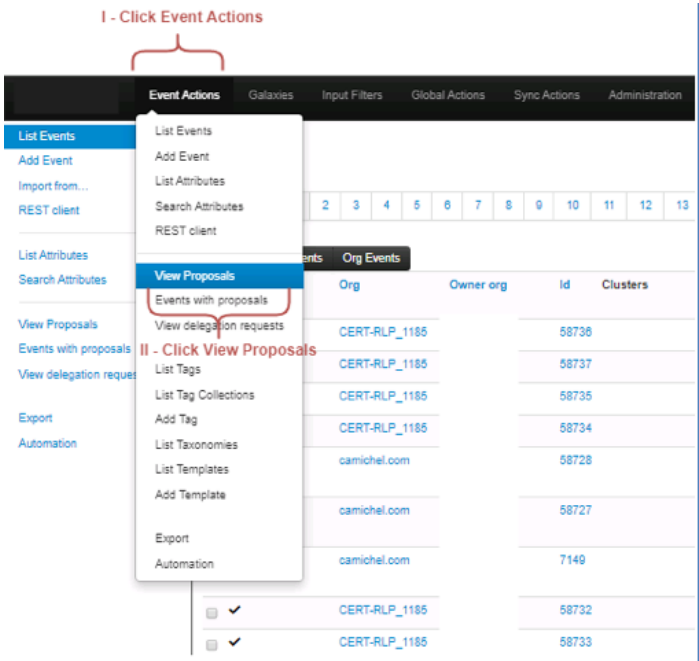
- a. Adding data (Attributes) to an existing Event; or
- b. notification to an Event creator of false positives; or
- c. asking for an error to be corrected.

To submit a proposal to change an Attribute, open the Event, navigate to the Attributes section and then (for each Attribute), select the “Propose Edit” icon as per the image below:



You will then be taken to the “Add Proposal” page, similar to the “Add Attribute” page. Populate the Attribute details you wish to propose (what you believe the Attributes should be) and then click the blue “Propose” button to send your proposal to the creator of the Event.

To see existing proposals, click on “Event Actions” from the top navigation bar then “View Proposals”



This will present a view of proposals for Events created by your organisation:

My Org's Events

All Events

Id	Event	Proposal by	Type	Event creator	Event Info
1	9	Test MiSP	Attribute edit	Test MiSP	Emotet Malware

Viewing an individual Event will show the normal Event screen. If there is a relevant proposal, a note will appear at the top of the Event indicating that the Event has “active proposals for you to accept or discard”:

HomeEvent ActionsGalaxiesInput FiltersGlobal ActionsSyno ActionsAdministrationAudit

This event has active proposals for you to accept or discard.

Event with a Proposal will have a note

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Enrich Event

Merge attributes from...

Unpublish

Publish event to ZMIQ

Contact Reporter

Download as...

List Events

Add Event

Emotet Malware

Event ID9

UUID5e19b214-7704-4813-894e-031d0d83800

Creator orgTest MiSP

Owner orgTest MiSP

ContributorsTest MiSP

Emailadmin@admin.test

TagsCIRCL O SHITMalwareIps green

Date2020-01-09

Threat LevelMedium

AnalysisCompleted

DistributionConnected communities

InfoEmotet Malware

PublishedYes (2020-01-12 18:35:14)

#Attributes5 (0 Object)

First recorded change2020-01-12 18:35:09

Last change2020-01-12 18:35:09

Modification map

Sightings1 (1) - restricted to own organisation only

PlotsGalaxyEvent graphCorrelation graphATT&CK matrixAttributesDiscussion

9: Emotet

To view the proposed changes, move to the Attributes section. A proposal will appear underneath an existing Attribute like the image below. The proposal is boxed in orange, beneath the original Attribute. To accept the proposal, click on the ‘tick’ icon to the right of the proposal:

Toggle tooltipsDisabledShow detailsContextShow TagsFiltering tool

Date 1OrgCategoryTypeValueTagsGalaxiesCommentCorrelateRelated EventsFeed bitsIDSDistributionSightingsActivityActions

☐	2020-01-12	Org	Network activity	url	abod.com/wwd21				☒		☒	All			
☐	2020-01-12		Network activity	domain	google.com				☒		☒	All			
☒	2020-01-12	Test MiSP	Network activity	domain	google.com			Please remove this as this is a legitimate website	☒		☒	No			
☐	2020-01-12		Payload delivery	email:to	abid@ora				☒		☒	Connected			
☐	2020-01-12		Payload delivery	email:ro	pl_service@delta.on				☒		☒	All			
☐	2020-01-12		Payload delivery	domain	gate.domain.on				☒		☒	All			

PreviousNextView all

Accept Proposal

The accepted change is then reflected in the (updated) Event and the proposal no longer appears. If you reject the proposal, the Participant who sent the proposal is notified that the proposal has been rejected.

22 OF 28

4.5 DELEGATION

The Platform allows participants to “Delegate” the publication of an Event, removing the connection between the information shared and the particular Participant sharing the information. If you want to publish an Event without being associated or identified as the publisher, you can delegate the publication to the Platform (i.e. Anonymous Submission) or any other Participant. This means you give up ownership and the other Participant or Platform will take oversight of the Event going forward. To do so, first select the Distribution Level of the Event as “Your organisation only” (the Delegate option will not be available if you select another Distribution Level):

[Publish Event](#)
[Publish \(no email\)](#)
[Delegate Publishing](#)
[Contact Reporter](#)
[Download as...](#)

Distribution	Your organisation only
Info	Delegate me
Published	No
Sightings	0 (0)
Activity	
Correlation	Enabled (disable)

When the “**Delegate Publishing**” option is clicked, a pop-up will show up:

If there are Delegations for your attention (Events that other Participants are Delegating to you) you will see a number (and View link) next to “Delegation requests”:

Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

Target Organisation

Select organisation

Desired Distribution

Recipient decides

Message to the recipient organisation

Yes

No

Dashboard

Notifications

Proposals: 0 (View)

Events with proposals: 0 (View)

Delegation requests: 1 (View)

Select the Participant or Platform who will take ownership (Target Organisation or Anonymous), and your desired Distribution Level of the Delegated Event.

Click on View to review the Events and ‘Accept’ or ‘Decline’ the Delegation request.

To review Delegations for you to action, click on the envelope icon next to your name:

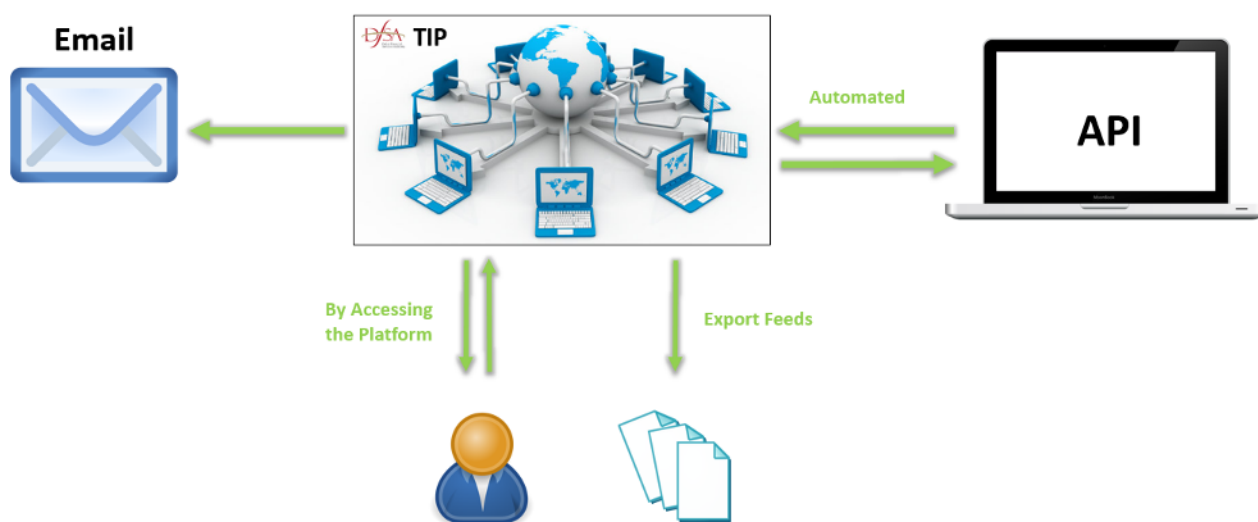
MISP

Max

Log out

5. CONSUMING EVENTS

A Participant with direct access to Platform may consume events in an automated fashion using API or manually by accessing the Platform and emails received from the Platform. The export feature is also available where the Platform provides a flexibility of Generating IDS, OpenIOC, plain text, CSV, Platform XML or JSON output to integrate with other systems.



Please refer to the User Integration Guide for details on how to effectively automate and utilise information from the Cyber Threat Intelligence. This includes a variety of security and non-security product integration to enhance the security detection posture of an organisation. You can also refer to the User Case Guide to add further capabilities to an effective threat detection strategy.

6. TECHNICAL DETAILS

6.1 IDS FLAG - INTRUSION DETECTION SYSTEM AUTOMATION

An IDS flag on an Attribute signals whether an Attribute can be automated (such as being exported as an IDS ruleset or used for detection). If the IDS flag is not present, the Attribute may only be useful for contextualisation and not automatic detection. This option allows the Attribute to be used as an IDS signature when exporting the data.

6.2 SIGHTINGS

Sighting is a mechanism that allows Participants to react to Attributes of an Event. It is a simple strategy for the Participant to communicate when they see a given Attribute, giving it greater credibility. Sightings may also be useful to signal false positives.

Use Sightings form the graphical user interface:

Sighting is applied to every Attribute, under the column “Sightings”, easily identifiable with its colored number. This column shows three icons and three values.

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
2017-04-03		Network activity	ip-src	123.56.76.7					No	Inherit	(0/0/0)		

These three values show respectively:

- a. The number of true positives detected with the Attribute, in green. Malicious activity as described in the Event.
- b. The number of times the Attribute has been marked as false positive, in red. Non-malicious activity or incorrect detection.
- c. The number of different expiration dates that have been reflected for this Attribute, in orange.

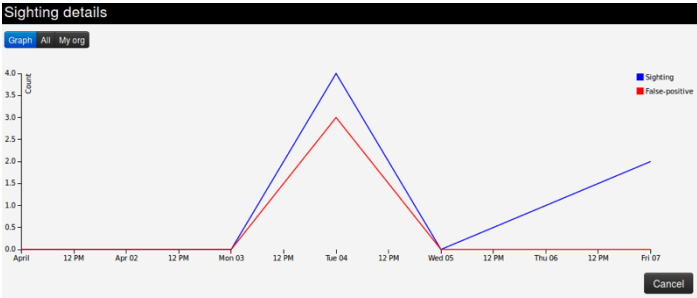
Concerning the three icons:

- 1. The first one (Thumb up) allows to add a sighting (true positive) on an Attribute.
- 2. The second one (Thumb down) allows to mark the Attribute as a false positive.
- 3. The third one (Tool) opens a popup for advanced Sightings, showing the Sighting details and allowing different actions.

For any individual Event, the total number of Sightings is visible as part of the metadata in front of the “Sightings” label, and a ‘sparkline’ graph that summarises the evolution (count over time) of Sightings.



Clicking on the tool will show Sighting details for the whole event.



6.3 TAGS

It is possible to filter Events based on tags. Tags can also be used to filter Events for automation. Tags are the simplest way to add information and/or context about an Event. A more complex method is using **Galaxies**. Refer to the Section titled “**Galaxy**” for further reading. Participants can add one or more tags to an individual Event. Below is an example of an Event with multiple Tags:

Sodinokibi Ransomware

Event ID

58738

UUID

5e1addfa-cfb4-4a51-bd53-0f0cac12035a

Creator org

HelpAG LLC, Middle East

Owner org

HelpAG LLC, Middle East

Email

Sumit.Bose@helpag.com

Tags

DLL Dropper

Download

Ransomware

Cybercrime

MALICIOUSACTIVITY

Malicious Domain

Partner Feed

Threat Source:OSINT

Intthreat-event-src="flash-intel"

circi.topic="undefined"

Date

2020-01-12

Threat Level

Undefined

Analysis

Initial

Distribution

Your organisation only

Info

Sodinokibi Ransomware

Published

No

#Attributes

0 (0 Object)

First recorded change

Last change

2020-01-12 08:51:08

Modification map

Sightings

0 (0) - restricted to own organisation only

6.4 TAXONOMIES

Taxonomies are groups of tags, expressed using a convention that identifies the tags as part of the group. Taxonomies are useful for classifying Events according to specific definitions.

The Traffic Light Protocol in the Platform is one type of Taxonomy. It is the only required Taxonomy for Events. All other tags and Taxonomies are optional.

There are several useful Taxonomies available in the Platform. Tagging Events using these plays an important role to ensure appropriate distribution, context, validation or action required of the shared information. Each Taxonomy has a “name” and a description.

A list of enabled Taxonomies is available under the “Event Actions” menu:

List Taxonomies

Update Taxonomies

Taxonomies

← previous

next →

Id	Namespace	Description	Version	Enabled	Actions
8	nato	NATO classification markings.	1	Yes	[-] [i]
7	euci	EU classified information (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.	1	Yes	[-] [i]
6	dri-ism	A subset of Information Security Marking Metadata ISM as required by Executive Order (EO) 13526. As described by DNI.gov as Data Encoding Specifications for Information Security Marking Metadata in Controlled Vocabulary Enumeration Values for ISM	3	No	[+] [i]
5	ecsiit	Incident Classification by the ecsiit.net project WP4 clearinghouse policy and updated by IntelMQ.	1	Yes	[-] [i]
4	veris	Vocabulary for Event Recording and Incident Sharing (VERIS)	2	No	[+] [i]
3	tlp	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.	1	Yes	[-] [i]
2	circl	CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection	1	Yes	[-] [i]
1	admiralty-scale	The Admiralty Scale (also called the NATO System) is used to rank the reliability of a source and the credibility of an information.	1	Yes	[-] [i]

Page 1 of 1, showing 8 records out of 8 total, starting on record 1, ending on 8

“Tag Collections” are groups of tags from different Taxonomies. Unless specifically directed, there is no reason to use Tag Collections (they are not required to use the Platform).

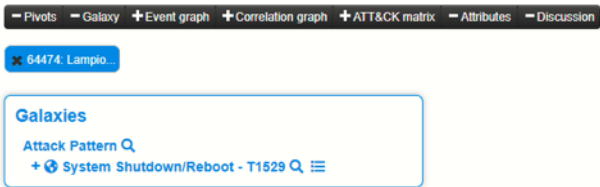
6.5 GALAXY

Galaxies are a method used to group, or cluster, Events and the associated Attributes. Galaxies provide a means to associate many different types of Attributes and are commonly used in the Platform to link activity, indicators, tactics and information to a specific Threat Actor or Threat.

Often referred to as a cluster, a Galaxy is the combination of the following:

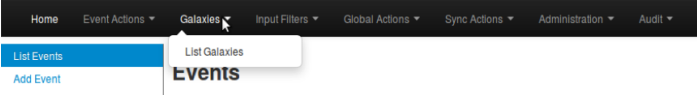
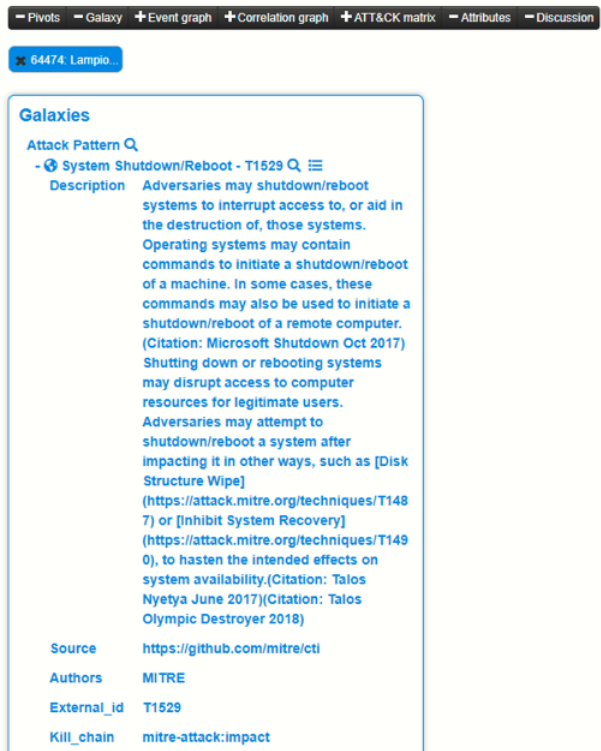
- a. One or more items (information specific to the Galaxy); and
- b. taxonomies (groups of related Tags) that are directly related to an individual Galaxy item; and
- c. the Events and Attributes which are “linked” to the Galaxy.

Unlike tags, an item can contain a significant amount of data, metadata or context, including links, without being linked to an Event. This information is **visible and presented to every Participant for every Event that is “linked” to a Galaxy**. Below is an example of an Event that is linked to the “Attack Patterns” Galaxy:



Clicking on the “+” sign will expand the information available, and provide a more detailed view of the Galaxy as follows:

To view available Galaxies, click on the “Galaxies” link on the top navigation menu.



7. CONTACT US

You can contact us directly via email on tip@dfsa.ae for any enquiries regarding the platform, the guides, suggestions or concerns and one of our team members will reach out to you as soon as possible.