Dubai Financial Services Authority

DFSA CYBER THREAT INTELLIGENCE PLATFORM (TIP)



User Integration Guide

TABLE OF CONTENTS

DISCLAIMER 4

1. INTRODUCTION 5

1.1 Purpose of the Integration Guide 5

1.2 About the Cyber Threat Intelligence Platform Initiative 6

1.3 Platform Terms of Use 6

1.4 Definitions 7

2. INTEGRATION BENEFITS 9

3. INTEGRATING WITH THE PLATFORM 10

3.1 Consuming and Contributing 10

3.2 Obtaining your API Key (AuthKey) 11

3.3 Using the Platform API 12

3.4 Integrating with Network Security Solutions 13

3.5 Integrating with other Threat Intelligence Solutions 14

3.6 Integrating with other Threat Intelligence Solutions 15

3.6.1 Integration with Palo Alto 'MineMeld' 15

3.7 Integrating with SIEM Solutions 16

3.7.1 Integrating with Splunk SIEM 16

3.7.2 Integrating with McAfee ESM 17

3.7.3 Integrating with IBM QRadar 17

TABLE OF CONTENTS

3.8 Integrating with Endpoint Security Solutions 18

3.8.1 Integrating with Carbon Black Response 18

3.8.2 Integrating with McAfee Active Response 18

3.9 Integrating with Web Application Firewall 19

3.9.1 Integrating with ModSecurity WAF 19

3.10 Other Integration Options 19

3.10.1 What if I do not have any cybersecurity systems or capabilities? 19

3.10.2 My office is just me and few others – what can I do? 20

3.10.3 Manually Check your Systems 20

3.10.4 Use PyMISP 21

3.10.5 I do not see my system or solution in this document. What can I do? 21

3.10.6 Talk to your Solution Vendor 21

3.10.7 I have my own MISP instance. How do I synchronize with the Platform? 21

4. CONTACT US 22

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 INTEGRATION GUIDE

This User Integration 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: (i) the potential benefits of integration with TIP; (ii) consuming intelligence; and, (iii) contributing intelligence.

This guide describes different strategies (referenced) for common integration scenarios for use of the Platform. Each integration scenario describes the approach of a proprietary or open source toolset providing an additional layer of detection capability.

In this guide, readers will find:

- A description of the potential benefits of Platform integration.
- Several ways that the Platform may be integrated via different security solutions and tools.
- Guidance for consuming and contributing data to the Platform.
- Options for Participants that do not currently have any security solutions or tools.

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 Case Guide** and the **Manual User 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 found here: **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 User Integration Guide.

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

1.4 DEFINITIONS

This section defines certain common terms used in this guide.

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.
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 that can be shared within the Community to further improve a 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 the practical manual intended to explain to Participants how to use the Platform.
MISP Community	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 or person 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 this guide which is intended to explain to Participants how to integrate the Platform within their information systems.

2. INTEGRATION BENEFITS

The Platform is intended to be utilised as a resource for Participants of all sizes and sophistication to assist them to better understand cyber attackers, respond faster to cyber incidents, and proactively anticipate and mitigate against cyber incidents. Exchanging Cyber Threat Intelligence can help Participants achieve a level of protection that may otherwise be out of reach. One of the significant advantages of sharing cyber intelligence is that Participants with little or no cyber security capability will have access to the same high-fidelity Cyber Threat Intelligence as larger, international or global groups and entities.

Obtaining current and relevant cyber intelligence empowers system and security administrators, including incident response groups, to determine which events, alerts or other occurrences are critical threats worthy of time and further investigation, including possible response actions.

The Platform and the surrounding ecosystem is intended to provide advantages to every Participant and will work best when all Participants are consuming and contributing data to the Platform. Participants are encouraged to share data such as Cyber Threat Intelligence, indicators, threat actor information or any kind of cyber threat which can be described. Participants benefit from the collaborative knowledge about existing malware or threats. The aim of the Platform is to improve the counter-measures and protection against cyber-attacks for all Participants, and therefore by extension, the DIFC as a whole.

The table below describes how the data in the Platform may benefit Participants, small or large:

	IT Teams & CSOC	Executive / Compliance
Benefits	• Maximise scarce resources (people, time, systems) to focus on Critical Threats • Optimize existing prevention and detection capabilities and strengthen defences • Decrease time to prioritize incidents based on threat, risk and impact to the organization • Accelerate security incident investigations, management, and prioritization	• Understand and support qualification of cyber risks, using relevant threat intelligence data • Provide Peers/Board with visibility of current general and/or targeted threats and risks
Use Cases	• Integrate CTI feeds with other security products • Block threat actors and disrupt their attacks • Enrich management reporting and employee awareness • Look wider and dig deeper for intrusion evidence using the correlation of data within the platform. • Tune newly deployed security controls based on latest discoveries • Track and Manage indicators of compromise to identify relationships: IPs, URLS, domains, files	• Assess overall threat level for the Participant. • Identify gaps in security controls, processes • Development of intelligence-driven cybersecurity capability roadmap • Enrich sharing of threat intelligence and collaboration with industry peers

3. INTEGRATING WITH THE PLATFORM

The data contained within the Platform may be used in a variety of contexts and integrated with a variety of technologies.

Threats come in many shapes and sizes, attacking different persons and organisations in different industries and geographical areas. Additionally, users like security analysts and compliance professionals use threat intelligence data in different ways to discharge their functions and responsibilities.

The Platform can integrate with technologies like SIEM and security infrastructure (i.e., firewalls, web threat gateways, proxies, etc.). This enables interoperability between the platform and a range of security technologies, creating a security operations and analytics platform architecture (SOAPA).

Participants can export indicators and threat intelligence data in a wide variety of formats, like Snort, Suricata, Bro/Zeek IDS rules, STIX, OpenIOC, text or csv exports. These outputs can be automatically or manually imported to other detection or processing systems resulting in faster detection of intrusions, better protection of business systems and prioritisation of resources to combat current or active threats and risks.

3.1 CONSUMING AND CONTRIBUTING

The Platform can support integration in many forms. In this guide, specific integrations have guidance on whether the (solution, system, method or alternative) provides the ability to:

1. **Consume** threat intelligence from the Platform; and/or

2. **Contribute** threat intelligence to the Platform.

In this guide **Contribute** refers to updates or observations **pushed to the Platform** from another system, interface or integration described or referred to in the relevant section. This does not cover updates performed manually through the web interface by a person, as these are covered in the **Manual User Guide**.

The integration guidance is presented in the form of a table like the following:

Integration Method	[Method Description]
Consume	[Yes/No]
Contribute	[Yes/No]

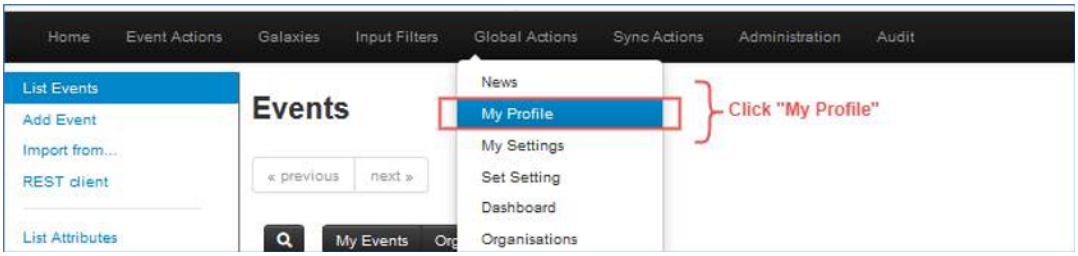
This is general guidance based on the capabilities of the Platform and indicates whether the integration in this section is capable of one or both (i.e. “pull” and/or “push”). Note that the mechanics of consuming (pulling) and contributing (pushing) data may require specific configurations within, or actions perform on, your solutions or systems, including configuration of new systems that are set aside for integration with the Platform.

As stated earlier, the Platform and surrounding ecosystem work best when Participants are consuming threat intelligence from the platform and contributing data to the Platform. As each Participant observes consumes intelligence, observes occurrences of indicators and provides feedback to the Platform, all Participants benefit. Other Participants may in-turn consume threat intelligence data, observe occurrences of indicators and feedback to the Platform these observations, further protecting all Participants of the platform.

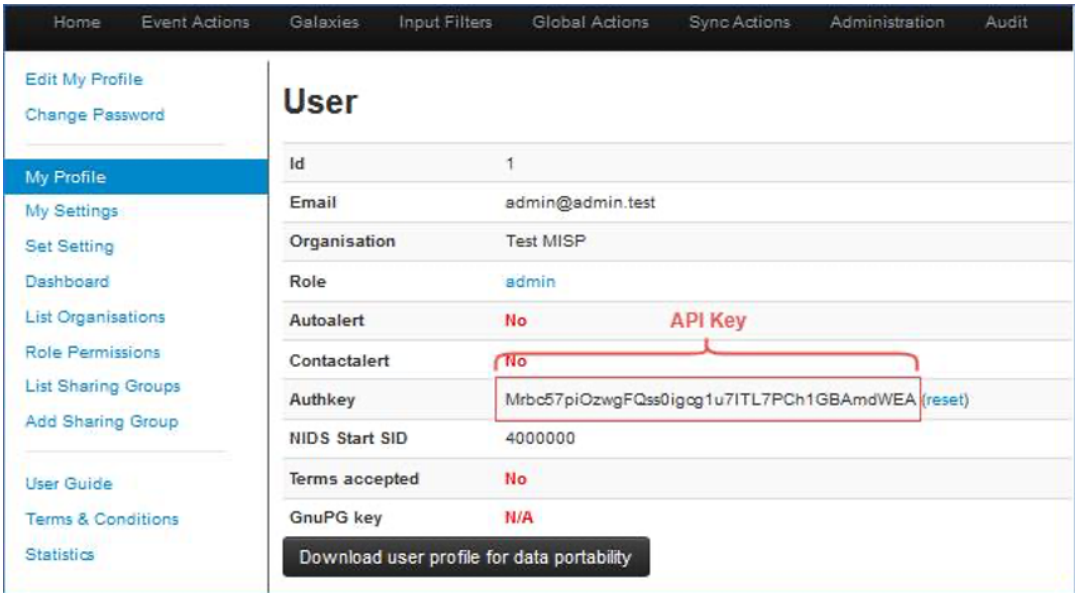
3.2 OBTAINING YOUR API KEY (AUTHKEY)

The Platform provides a specific method to authenticate you when integrating with the Platform using the API. This method is called the "Authkey", also called an "API key". The API key must be passed when using the MISP API. It is passed in the HTTP headers, using the "Authorisation:" parameter. For more information on how to use the API, refer to this document.

Your Authkey can be found in your profile within the Platform. To obtain your Authkey, login to the Platform, select "Global Actions" from the top navigation bar, and then select "My Profile":



Within your Profile, your Authkey is visible as follows:



Your Authkey can be reset (to create a new key) from this screen as per the image above by clicking on the "reset" link.

The Platform has built-in documentation about the API and how to use the API to integrate with the Platform. Click on "Event Actions", then "Automation" to see the built-in documentation. The Authkey key shown here is the same as that in your profile.

3.3 USING THE PLATFORM API

Once you have obtained your Login and Password, you should obtain and safely store your 'Authkey' as this is necessary to interact with the Platform when not using the Web User interface. To obtain your Authkey, refer to section 3.2, "Obtaining your API Key (Authkey)".

Example API Call:

$ curl --header "Authorization:<<PLACE YOUR AUTHKEY HERE>>" --header "Accept: application/json" --header "Content-Type: application/json" https://tip.dfsa.ae/attributes/restSearch/returnFormat:csv/tags:tlp:red/type:ip-src

The 'curl' command sends a normal web request to the Platform, using the API. This command does the following:

- Returns a list of "Attributes" (/attributes); and
- Formats the returned list as Comma-separated Values (one Attribute per line) (/returnFormat:csv); and
- Filters the Attributes and returns only those Attributes that have the tag "tlp:red" (/tag:tlp:red); and
- Filters the Attributes and returns only those Attributes that are of type "ip-src" (/type:ip-src).

The results of the above command will look like the following (NOTE: the actual values and number returned by the Platform will depend on the Attributes available in the Platform)":

uuid,event_id,category,type,value,comment,to_ids,date,object_relation,attribute_tag,object_uuid,object_name,object_meta_category

"5d9326a7-c364-43fa-9713-478f950d210f",63181,"Payload delivery","ip-src","88.4.x.x","Source IP",1,1569924775,"","","","","",""

The first line (beginning with 'uuid') contains the column headings and provides a description of each column, separated by a comma. All other lines including the second are the Attributes returned from the Platform, matching the above filter(s). Commands like this can be used to obtain and process Attributes automatically and send them to other systems.

For more information about using the API, refer here.

3.4 INTEGRATING WITH NETWORK SECURITY SOLUTIONS

Integration Method	Dynamic List/Feed Downloaded by Firewall
Consume	Yes
Contribute	No

The Platform integrates with multiple network solutions to support effective detection capabilities. This helps the security teams to stitch specific threat intelligence data with various platforms like IDS (Intrusion detection systems), IPS (Intrusion prevention systems), Network forensic managers, Firewalls, Email gateways, web proxy and DNS solutions. The information can be pumped into data flow behavior tools to better detect threats that have already infiltrated the network, and significantly accelerate incident response to curtail further damage.

A successful integration will allow Participants to automatically pull data from the Platform and push relevant indicators to Firewall devices/appliances for the purposes of detection and/or prevention (blocking) of network-based communication between systems.

A sample of relevant Network Security Solutions that can consume specific types of indicators is included in the table below:

Vendor/Product	IP Address?	Domain?	URL?	Further Information
Palo Alto NGFW	Yes	Yes	Yes	External Dynamic Lists
Cisco ASA FirePOWER	Yes	Yes	Yes	Custom Intelligence Feed
Fortinet FortiGate NGFW	Yes	Yes	Yes	Fortinet Custom Feed

To extract and download data from the Platform you can use PyMISP described later in this document to extract/ download indicators from the Platform. You will need to configure a system to (e.g. Web Server) to make them available for download by your devices.

IMPORTANT NOTES – AUTOMATED BLOCKING OF INDICATORS:

This setup allows an Administrator to automatically block network traffic without any human interaction. This setup requires specific configuration parameters on each firewall, including the creation of a dynamic object and specific policy/rule that performs an action e.g. block/drop. Please ensure you adhere to the specific change management policy for your organisation when updating policies on any production firewalls.

3.5 Integrating with other threat intelligence solutions

Integration Method	Configuration of Solutions (built-in)
Consume	Yes
Contribute	No

SOAR (Security Orchestration, Automation and Response) systems simplify the management and automation of incident response tasks. They can leverage many types of data, including threat intelligence. SOAR systems provide a capability to create “playbooks”, a structured procedure or series of actions which, reduce human/manual effort and effortlessly manage the integration and data transfer between different systems.

The following systems provide “out-of-the-box” or built-in integration with MISP through the administration interface (sometimes referred to as “Integrations” within the solutions below):

Vendor/Product	IP Address?	Domain?	URL?	Further Information
Palo Alto Demisto	Yes	Yes	Yes	Demisto Integration
Fortinet CyberSponse	Yes	Yes	Yes	CyberSponse
Splunk Phantom	Yes	Yes	Yes	Phantom Integration

3.6 Integrating with other threat intelligence solutions

Integration Method	Configuration of Solutions (built-in)
Consume	Yes
Contribute	No

Threat intelligence platforms, like the DFSA CTI, provide a structured, automated and streamlined mechanism to exchange data between participants and distributed systems. Exchange of data on the Platform between Participants and Communities provides Participants with:

- enhanced and enriched intelligence data
- missing pieces of intelligence data
- visibility of threats from different contexts
- data that may not be publicly available

The following systems provide "out-of-the-box" or built-in integration with MISP through the administration interface (sometimes referred to as "Integrations" within the solutions below):

Vendor/Product	IP Address?	Domain?	URL?	Further Information
ThreatConnect	Yes	Yes	Yes	ThreatConnect Integration
ThreatQ	Yes	Yes	Yes	ThreatQ
EclecticIQ	Yes	Yes	Yes	EclecticIQ Integration

3.6.1 Integration with Palo Alto 'MineMeld'

Integration Method	MineMeld Configuration
Consume	Yes
Contribute	Yes

MineMeld, by Palo Alto Networks, is a threat intelligence processing framework. MineMeld is used to collect, aggregate and filter indicators from a variety of sources and make them available for consumption by Palo Alto Networks security platforms.

The Platform integrates with the Palo Alto Firewall by using a MineMeld Miner and MineMeld Output node to process intelligence and push intelligence data to a firewall device/appliance.

Before proceeding, follow the process here to setup MineMeld. There is a dedicated miner created for the Palo Alto Firewall that serves the purpose of delivering data so the appropriate policies can be enforced based on the appropriate risk scores. To setup integration between MineMeld and a PAN-OS Next-Generation Firewall, refer to community guide here. Further readings on MineMeld can be found here.

3.7 INTEGRATING WITH SIEM SOLUTIONS

As previously noted many open source and proprietary tools integrate with the Platform in order to extend their toolset or enhance the data available to Participants.

A "SIEM" solution is the combination of two systems:1) Security Event Management (SEM); and, 2) Security Information Management (SIM). Threat intelligence is considered "Security Information" in this context. SIEM systems are capable of monitoring for threats, providing real time security alerts and increasing compliance. A SIEM system centralises interpretation and storage of logs, collects data to be analysed for reporting and enriches events with additional context or information – in this case, threat intelligence data extracted from the Platform.

A successful integration will allow Participants to automatically pull data from the Platform and push relevant indicators to the SIEM system, automating the correlation of indicators against available event or log data, to provide rapid detection of threats and/or threat actors.

3.7.1 INTEGRATING WITH SPLUNK SIEM

Integration Method	Splunk App for MISP
Consume	Yes
Contribute	No

Splunk is an analytics tool for data collection, monitoring and correlating. As a cybersecurity platform, Splunk provides individuals and teams with the ability to analyse log and event data to prioritise response actions and investigate incidents.

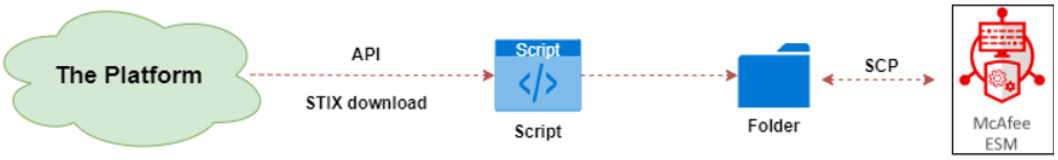
This integration method also permits the pushing of data to MISP as new Events or updates to the Platform following creation of alerts in Splunk.

Details of the Splunk integration with the platform can be found here.

3.7.2 INTEGRATING WITH MCAFEE ESM

Integration Method	Script and Configuration
Consume	Yes
Contribute	No

A purpose-built script (details available here) downloads the Events from the Platform in STIX (Structured Threat Information eXpression) format. McAfee Enterprise Security Manager (ESM) is configured to pull these STIX files from a folder location via secure copy files and run automated triage processes.The graphic below shows the mechanisms required to transfer data from the Platform to the McAfee the ESM system.



3.7.3 INTEGRATING WITH IBM QRADAR

Integration Method	Script and Configuration
Consume	Yes
Contribute	No

A purpose-built tool (details available here) downloads attribute data from the Platform. The script then prepares the data for QRadar and publishes the data to QRadar.

3.8 INTEGRATING WITH ENDPOINT SECURITY SOLUTIONS

Endpoint solutions provides flexibility to block activity, disrupt the attacker and alert relevant teams about malicious actors within the environment. The most common end-point systems are antivirus solutions, EDR (Endpoint Detection and Response) solutions and Endpoint protection solutions.

3.8.1 INTEGRATING WITH CARBON BLACK RESPONSE

Integration Methods	Carbon Black MISP App
Consume	Yes
Contribute	No

Carbon Black Response (CB Response) is an incident response and threat hunting solution designed for security operations center (SOC) teams. The combination of endpoint data and data from the Platform helps Participants obtain rapid visibility to in-progress incidents. The most recent version of CB Response provides an "out-of-the-box" App that integrates MISP into Carbon Black. For further information about Carbon Black see here.

A successful integration will allow Participants to automatically pull data from the Platform and push relevant indicators to the CB Response system for the purposes of detection and/or prevention (blocking and disruption) of end-point threats and/or threat actors.

3.8.2 INTEGRATING WITH MCAFEE ACTIVE RESPONSE

Integration Method	Script
Consume	Yes
Contribute	No

McAfee Active Response is an endpoint toolset used by the enterprises as an EDR (Endpoint Detection and Response) solution. The Platform provides integration with McAfee Active Response to support automated hunting and investigation capabilities in the Active Response solution.

A successful integration will allow Participants to automatically pull data from the Platform and push relevant indicators to the McAfee Active Response system for the purposes of detection and/or prevention (blocking and disruption) end-point threats and/or threat actors.

Instructions for how to integrate can be found here.

Further reading about McAfee Active response can be found here.

3.9 INTEGRATING WITH WEB APPLICATION FIREWALL

3.9.1 INTEGRATING WITH MODSECURITY WAF

Integration Method	Script
Consume	Yes
Contribute	No

ModSecurity is a toolkit for real-time web application monitoring, logging, and access control. ModSecurity is an open source initiative, providing robust integration to transform passive defence into active defence using threat intelligence data from the Platform.

A successful integration will allow Participants to automatically pull data from the Platform and push relevant indicators to ModSecurity for the purposes of detection and/or prevention (blocking) of web-based attacks against web application systems.

Once the data is exported security administrators can various ModSecurity policies like block rules, directory brute-force attacks and convert the site to active honeypot site.

For more information about ModSecurity see here.

3.10 OTHER INTEGRATION OPTIONS

3.10.1 WHAT IF I DO NOT HAVE ANY CYBERSECURITY SYSTEMS OR CAPABILITIES?

DFSA initiated the Platform and related CTI for all DIFC entities, including entities equipped with full scale cybersecurity capabilities to entities with no personnel performing a “cybersecurity” role.

This section provides options for all individuals and Participants, including lone IT administrators or technology professionals.

3.10.2 My office is just me and few others – what can I do?

Integration Method	Download of indicators (email address)
Consume	Yes
Contribute	No

Outlook and Office365 (Outlook on the Web) provide **Junk Email** Filter protection for all users. The filtering system has various levels, and by default (when installed) is often set to "**No Automatic Filtering**". This setting means only bad senders you specify are blocked – all other email will appear in your inbox.

The threat intelligence data provided by the Platform contains IP addresses, file hashes and email addresses. For protection against specific threats, it may be necessary to block specific email addresses in your systems. To block email addresses in Outlook/Office365, refer to the guidance from Microsoft for Outlook and/or Outlook on the Web:

3.10.3 Manually check your systems

Integration Method	Download data from the Platform, then sweep a single system for evidence of the data
Consume	Yes
Contribute	No

If you do not have a system that can be used for Platform integration, you can still search and review your systems using data from the Platform.

To do this you will need to download or extract data from the Platform. Once extracted (e.g. through the Platform web interface, or using PyMISP), if you wish to search for evidence using data downloaded, you can use the an open-source tool called **LOKI** available here.

LOKI provides a Windows executable and script (written in python) that can search systems for lists of indicators. Note that you may need to download, and update LOKI once installed.

For further details on extracting data from the Platform, refer to the articles here and here (refer to the section titled "MISP Receiver").

3.10.4 USE PYMISP

Integration Method	Script
Consume	Yes
Contribute	Yes

Participants can use PyMISP to extract data form the Platform instantly and this data can be consumed by the firewall administrators. For details on how to use PyMISP, please refer to the official documentation here.

The threat data extraction is an easy process. Participants with enough privileges (sync user or administrator users) can export: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS or custom tools). The extracted data can go to the firewalls default block or alert list.

For further information on PyMISP, see the documentation here.

3.10.5 I DO NOT SEE MY SYSTEM OR SOLUTION IN THIS DOCUMENT. WHAT CAN I DO?

If the solution you use is not described in this guide or does not have a native or "out-of-the-box" integration with the Platform, there are several options and open-source tools that are available, described in the following sections. If you are not sure where to start, or have a question about integrating with your systems, contact the DFSA Cybersecurity team: **tip@dfsa.ae**

3.10.6 TALK TO YOUR SOLUTION VENDOR

Speak directly with your vendor representative or vendor support team. Alternatively, download your vendor documentation or review community-created information to understand if integration with "**MISP**"

3.10.7 I HAVE MY OWN MISP INSTANCE. HOW DO I SYNCHRONIZE WITH THE PLATFORM?

If you have your own Platform or MISP instance, please reach out to the DFSA team via email at: **tip@dfsa.ae**

4. 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.