



DFSA CYBER THREAT INTELLIGENCE PLATFORM (TIP)



USER CASE GUIDE
(HOW TO USE CYBER THREAT INTELLIGENCE)

TABLE OF CONTENTS

DISCLAIMER	3
1. INTRODUCTION	4
1.1 PURPOSE OF THIS USE CASE GUIDE	4
1.2 ABOUT THE CYBER THREAT INTELLIGENCE PLATFORM INITIATIVE	4
1.3 PLATFORM TERMS OF USE	5
1.4 DEFINITIONS	5
2. WHAT IS CYBER THREAT INTELLIGENCE?	7
2.1 USE OF CYBER THREAT INTELLIGENCE	7
2.1.1 TACTICAL	8
2.1.2 OPERATIONAL	8
2.1.3 STRATEGIC	8
3. THREAT INTELLIGENCE USE CASES	9
3.1 PREVENTIVE THREAT BLOCKING	10
3.2 ATTACK DETECTION AND SECURITY MONITORING	10
3.3 THREAT DATA SHARING	11
3.4 RETROSPECTIVE THREAT HUNTING	11
3.5 INCIDENT DATA ENRICHMENT	12
3.6 SECURITY AWARENESS EDUCATION	12
4. CONTACT US	13

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 THIS USE CASE GUIDE

This User Case 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 use cyber threat intelligence to (i) enhance the effectiveness of cyber capabilities; (ii) establish an effective threat detection; and (iii) add further capabilities to enhance the cyber maturity of the Participant.

This guide describes how cyber threat intelligence can be used generally in different contexts to detect, protect and defend from cyber-attacks and provides for specific situations where cyber threat intelligence can and has been used to detect, protect and defend from cyber-attacks.

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 Manual User Guide and the Integration 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 Case Guide.

The access to and use of this User Case 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.
Community	Means the particular forum in which a Participant elects to store or share data.
Campaign	Set of cyber activities carried out by threat actors using specific techniques
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.
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.

TERM	DEFINITION
MISP Community	The Community that allows for participation and sharing of data by users or entities that use the MISP.
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.
TTP	Tactics, Techniques and Procedures, these describe how Threat Actors orchestrate, manage and execute attacks.
User Case Guide	Means this guide 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.

2. WHAT IS CYBER THREAT INTELLIGENCE?

Cyber Threat Intelligence is actionable evidence-based knowledge, indicators, and facts about an existing or emerging cyber threat. This information can be used to help entities protect against the cyber threat, detect suspicious activities and make informed decisions. There are different types of Cyber Threat Intelligence– here are the most common:

- Threat indicators
- Indicators of actual or potential compromise
- Tactics, techniques and procedures (TTPs)
- Security alerts that describe threat activity
- Communications from cybersecurity specialist such as chat message or tweet;
- Threat intelligence advisories or reports.

Cyber Threat Intelligence is certainly not a new concept – it is another name for an old methodology, for example applying a structured analytical process to categorise attacks and factually knowing the adversary behind attacks can be inconceivable. In this way, as in old times, and even now, the study of cyber attackers or Threat Actor remains the way to building a compelling and contemplated defence framework, and prioritizing activities to identify and safeguard.

There are numerous approaches to utilize Cyber Threat Intelligence, Participants can utilize it in different portions. Some examples are as follows:

- A Participant suspects they have a malware present in their environment and they are seeking to understand specific malware indicators to determine if systems are infected and if so, the type of malware;
- Communicating to employees the relevance of current threats with instructions on how to avoid falling for new phishing scams;
- Implementing protective actions based on Cyber Threat Intelligence shared by a peer Participant on malicious events they have observed.

2.1 USE OF CYBER THREAT INTELLIGENCE

Use of Cyber Threat Intelligence can be divided broadly into three categories:

- Tactical Cyber Threat Intelligence;
- Operational Cyber Threat Intelligence; and
- Strategic Cyber Threat Intelligence

This guide has been made to enable Participants to comprehend and choose (operationally, strategically, as well as tactically) how to utilize Cyber Threat Intelligence they have access to through the Platform. At the Participant level, it is imperative to determine which type of Cyber Threat Intelligence is conveyed to the right decision maker in the right manner, at the right time. The three categories are described below.

2.1.1 TACTICAL

Tactical Cyber Threat Intelligence generally refers to current or immediate threats and its significance is most critical to those who are responding to and handling security threats and incidents.

Tactical Cyber Threat Intelligence typically takes the form of indicators, and is often used interchangeably with “Indicators of Compromise” (IOC), due to the data being used to confirm the presence (as evidence) of Threat Actors or malicious code.

Tactical Cyber Threat Intelligence is readily and easily consumed by IT and cybersecurity solutions. However, one weakness of Tactical Cyber Threat Intelligence is that it is useful for short periods and its usefulness decays rapidly over time, sometimes within hours or days.

2.1.2 OPERATIONAL

Operational Cyber Threat Intelligence provides Participants with increased context having most likely been at one-point Tactical Cyber Threat Intelligence that has experienced enrichment and transformation. Relationships between IOC and potential Threat Actors (often referred to as “attribution”) may be present in Operational Cyber Threat Intelligence through identification of the TTPs that are relevant or suspected.

Threat Actors may attempt to alter their tools (for example, malware, botnet hosts, backdoors, infrastructure, etc.), however it is progressively and sometimes prohibitively difficult for Threat Actors to change the methods they have adopted and apply to different targets.

2.1.3 STRATEGIC

Strategic Cyber Threat Intelligence is intended to provide a risk-oriented perspective, with greater context and situational awareness (potential or actual impact, risk and remediation plans, etc) and in general is intended to be seen in the context of global or worldwide events, threats and risks. Strategic Cyber Threat Intelligence lacks the granularity of Tactical Cyber Threat Intelligence, since it is intended to support long-term decision making for a Participant, aligning intelligence to business risks and objectives.

Strategic Cyber Threat Intelligence is circulated with Senior Leaders, Executive Management and Board members to promote effective decision-making, budgeting, forecasting and long-term planning to protect and defend Participants from cyber-attacks.

3. THREAT INTELLIGENCE USE CASES

This section contains a set of “Use Cases”. A Use Case is a situation, scenario or context and most Use Cases are simply a logical expression of one or more behaviours, with a view to acting “if” something is true.

For example, a Use Case to detect a phishing email might be defined as follows:

“if an email sent to an employee contains a link to a website
and
the email subject contains the words ‘Your Invoice’ then
do not deliver the email to the employee”

How Participant might use Cyber Threat Intelligence does depend on your Participant’s size and maturity level.

The table below lists the Use Cases described in this guide (left-hand column) and highlights using the green ‘tick’ (✓) where these Use Cases are likely to be most useful. Participants reading this guide are free and encouraged to use the Use Cases in whichever context they believe is useful – this table is provided as a starting point for Participants who are seeking guidance on where to start.

USE CASE	CATEGORY & CONSUMER TYPE			BUSINESS SIZE	
	Strategic (CEO Level)	Operational (Manager Level)	Tactical (Analyst Level)	Large Enterprise	SMB Entity
Preventive Threat Blocking	-	-	✓	✓	✓
Attack Detection and Security Monitoring	-	-	✓	✓	-
Threat Data Sharing	-	✓	✓	✓	✓
Retro Threat Hunting	-	-	✓	✓	-
Incident Data Enrichment	-	-	✓	✓	-
Security Awareness Education	✓	✓	✓	✓	✓

3.1 PREVENTIVE THREAT BLOCKING

The least complex application of Tactical Cyber Threat Intelligence is typically the preventive blocking or prevention of threats using IOC to determine what to allow or block. Preventive blocking acts as a mechanism to disrupt attackers and their tools. Threat Actors and malicious code must, at some point in time, leverage some type of network communications to accomplish the attackers' objectives. For example:

- Ransomware attempts to connect to a remote system on the internet to download encryption keys from attacker's server before encoding data;
- Trojan horses connect to command and control frameworks to receive commands or download extra code (for example for stealing password).

Attackers use proxy servers and anonymizers to hide their tracks. Internal attackers can also use anonymizers to access prohibited sites or leak confidential data.

To block such communication, administrators can perform one or more of the following:

- A Network Firewall could be used to block access, using the IP address;
- A DNS server can block requests to specific domain names;
- A Web proxy can block domain names, IP addresses as well as links to websites;
- A Network Router can block communication from an IP address.

For further information regarding how to implement preventive blocking, refer to the User Integration Guide.

3.2 ATTACK DETECTION AND SECURITY MONITORING

Blocking types of IOC is a simple strategy to protect Participants and systems, however, problems arise when IOC are old or inaccurate, and their blockage may block legitimate activity.

Attackers sometimes use legitimate servers for hosting command and control systems. If the IP address of a legitimate server is blocked on a Firewall, the threat will be blocked. However, Participants will not be able to access other legitimate websites hosted on the same server.

If the IOC is not accurate and thus cannot be used for blocking, an Administrator can still use the IOC to monitor for its presence in the network and investigate the root cause without interrupting business services or blocking legitimate/authorized users.

If the IOC is a domain name used by the sophisticated hacker group it is possible to monitor for network communications to this domain instead of blocking requests to the domain or website. Preventative actions can indicate awareness, which may cause an attacker to modify their tactics or change their behaviour, increasing the difficulty of further or ongoing detection.

If the IOC is the domain name of ransomware, then unless there is a good reason, access to the domain should be blocked to prevent further compromise. Monitoring for attempts to access the blocked domain is still important - malicious software could contain several domains for command and control servers within its embedded/initial configuration, so monitoring for a single domain may provide insight into other domains used by the ransomware.

Larger Participants typically use SIEM solutions. These are useful for aggregation, collection and processing of large numbers of Events.

3.3 THREAT DATA SHARING

Effectively sharing information on the Platform benefits all Participants. For a step-by-step guide on how to contribute to the Platform, refer to the Manual User Guide and the User Integration Guide.

Attackers actively exchange information about hacking techniques. Attackers also create communities, forums and attend conferences where they exchange the latest trends in information security.

Sharing of data amongst the Participants will help protect the business community: if one of the Participants detects an attack, identifies the IOC of the attacker and shares these with other Participants, others can do likewise, rapidly providing visibility of the attacker and the attackers' tools and techniques. With this information, all Participants can pre-empt an attack (if it has yet to occur) nullifying the effectiveness of an attack before it begins.

During the course of such sharing and ongoing activity, other IOC may be found and if shared help other Participants, perhaps even beyond the DIFC Community, including the first member who discovered the initial attack.

To facilitate such interactions and protection, a committed active group of professionals work together to support, maintain and enrich the Platform. If you have questions regarding the intelligence in the Platform you can reach out via email using: tip@dfsa.ae

3.4 RETROSPECTIVE THREAT HUNTING

One of the most popular forms of exchanging information about threats is threat reports. Reports can be in the form of an article, a blog, or it can be in the form of a separate document detailing a specific attacker or family of malware. These reports are created as a result of the analysis of past attacks, so historical data is needed to use them in detection.

For example, in such reports, you can see the hashes (unique signatures) of malicious files. To check whether a file with the same hash exists within the Participant, as in the report, you need to keep records and record the hashes of files, and review these regularly.

In addition to accounting for file hashes, it is useful to store information about the names of processes that are launched, the files they downloaded, and the network connections they establish.

The process of reviewing stored data (logs, events or network communication) and assessing systems with care and concern for Threat Actors, is referred to as "hunting", and requires specific skills and knowledge in order to be effective.

Industry good practice recommends storage of at least six months of such data, using solutions such as Endpoint Detection and Response (EDR), and periodically review the collected data (for example using a SIEM solutions mentioned previously).

That said, in many situations, especially in small operations which do not have nor require complex cybersecurity solutions or teams, it is sufficient (and effective) to use simple scanning tools to identify IOC. For more information on tools that can help you detect the presence of IOC in your systems, refer to the User Integration Guide.

3.5 INCIDENT DATA ENRICHMENT

When investigating an incident, it can be extremely useful to enrich the data received from the IT and/or cybersecurity systems with threat data from other sources. Such enrichment allows individuals to compile a more complete picture of what has occurred, the origin of such activity providing the individual the ability to better and more accurate conclusions.

A good example is the enriching of a malicious domain name with information from a 'WHOIS' record. Cybercriminals may use the same email address when registering a domain name. Therefore having learned the cybercriminal's preferred email address, it is possible to identify other malicious domains that the cybercriminal has registered, but not yet used, to block them in advance and pre-empt any future use of the malicious domain.

In addition to WHOIS data, it is also useful to enrich incident information with other types of data:

- Passive DNS data (containing information on which IP address the domain resolved in the past) from Services such as "[CIRCL Passive DNS](#)";
- Antivirus Coverage from a wide variety of Products (information about virus hashes and how different antivirus vendors detect) from services such as VirusTotal.com;
- Internet Abuse information (information about the reputation of internet connected systems) from services such as AbuseIPDB;
- Data shared on the Platform.

3.6 SECURITY AWARENESS EDUCATION

Many hackers use social engineering in their attacks. Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.

Security awareness education is a continual process of education. Employees should be made aware about information security, the basics of cyber hygiene and their role in protecting themselves. Awareness should typically extend to techniques for recognizing methods like social engineering.

Educating users is important and for this training to be effective, you need to use relevant and appropriate examples of attacks that draw on threat intelligence.

An effective use of Cyber Threat Intelligence in awareness is to design phishing simulations and trainings to mimic real phishing attacks in order to assess the user's reaction and readiness:

- Will he/she click on the suspicious link?
- Is an employee likely to delete a suspicious email?
- Will they report these suspicious emails to IT/ IT Security?

Training Senior and Executive Management on information security is also necessary. Current tactics and trends in social engineering attacks are increasingly relevant to Senior Leaders as more attacks are aimed specifically at Senior and Executive Leaders.

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.