Dubai Financial Services Authority



INSIGHTS

Launching a Cyber Threat Intelligence Sharing Community in the Dubai International Financial Centre

01 | Opening Statement

03 | Introduction

04 | Threat Intelligence

05 | The DFSA's Cyber Risk Supervision

06 | Progress with TIP

08 | The Importance of Sharing

09 | The Challenges Ahead & Closing

10 | Annex 1 to 6



Opening Statement

Welcome to the first edition of the Dubai Financial Services Authority's Cyber Threat Intelligence Platform report. As part of our commitment to support the directives of His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, and in line with the National Cybersecurity Strategy and the Dubai Cyber Security Strategy, we established the DFSA Threat Intelligence Platform (TIP) - the first financial regulator-led Cyber Threat Intelligence Platform in the region.

The financial services industry is one of the most targeted industries by cyber criminals who continue to leverage technology to conduct illicit activities. The global annual cost of cybercrime is predicted to hit $8 trillion this year and estimated to grow to $10.5 trillion by 2025. The DFSA categorises cyber risk as among the top risks facing our organisation and the financial services community, and hence, places much importance on a robust Information Technology (IT) infrastructure, internal controls, and governance to ensure effective management of cyber risks and preparedness for cyber incidents.

DFSA TIP was launched to provide a platform upon which to build a threat intelligence sharing community. Registrations have grown from 132 DIFC-based firms in its first year to 250+ firms to date, with a notable increase in the diversity of intelligence contributed covering a number of top cyber threats such as ransomware, phishing, Zero-day vulnerabilities and malicious sites. In addition, the appeal of joining our platform has expanded beyond the DIFC, and we've had the privilege of welcoming local banks to our community.



We continue to build our collaboration with global players in this sector, and we aspire to leverage this success by forging new alliances with well-established international sharing communities.

We are very grateful to the Dubai Electronic Security Center (DESC), the National Computer Emergency Response Team for the UAE (aeCERT) Telecommunications and Digital Government Regulatory Authority (TDRA), the Computer Incident Response Center Luxembourg (CIRCL), HelpAG and the Open Source Threat Intelligence and Sharing Platform Project (MISP) for their assistance and support in launching TIP. We remain resolute in our determination to protect the DIFC community from cyber risk and are committed to building cyber awareness based on best practices and international standards.

As we celebrate the 3rd anniversary of the launch of TIP, we would like to share our experience from the past three years supporting firms in sharing cyber threat intelligence, the key lessons learnt from bringing this concept to fruition, as well as some insights into what may come next. As the platform continues to grow, we look forward to seeing contributions from our community not just on conventional cybersecurity topics such as threat intelligence, malware analysis, and indicators of compromise, but we are also keen to explore expanding the scope to cover cyber financial fraud. Cyber Intelligence Sharing Communities depend heavily on the valuable contributions of their members, I take this opportunity to encourage you to join the Platform, if you have not already done so, and contribute to further enhancing the robustness and resilience of our community.

Waleed Saeed Al Awadhi
Chief Operating Officer
DFSA

Introduction

On 21 January 2020, drawing on cooperation with the Dubai Electronic Security Centre (DESC), the National Computer Emergency Response Team (aeCERT) and the Computer Incident Response Center Luxembourg (CIRCL), the DFSA launched TIP - the first financial regulator-led cyber threat intelligence platform in the region. When developing this idea, the DFSA decided the platform would be managed and operated by an independent consultant; they would directly support users and work towards the enhancement of threat intelligence. Since its launch, TIP has been operated and managed in coordination with Help AG. In addition to Help AG, international experts such as Palo Alto Networks and Recorded Future are involved in the platform.

The TIP 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, hosted and funded by the DFSA, is an initiative to improve the cyber risk posture of organisations in the Dubai International Financial Centre (DIFC). The use of the platform by firms in the Centre is voluntary and at no cost. The platform is physically located on DFSA premises in the DIFC and is based on an open-source product called MISP (Malware Information Sharing Platform). Further details can be found here.

The objective of the platform was, and remains, to create a network to support and foster the sharing of structured cyber threat information within the DIFC community. The platform is designed for community members to support their day-to-day operations by sharing structured information efficiently and to assist members in prioritising responses to cyber threats, including implementing appropriate safeguards to mitigate cyber risks. The platform provides functionality to support the exchange and consumption of information by Network Intrusion Detection Systems (NIDS), as well as to support log analysis tools, Security Information and Event Management (SIEM) and other security controls.

You can find more detail on the implementation of TIP in Annex 1.

Threat Intelligence

Cyber Threat Intelligence (CTI) is information relating to cyber events (whether past, current or indications of future threats) that any individual or entity can access, observe, and consume for their own benefit. The key added benefit of CTI is that it can be collated, organised and disseminated, which can involve large amounts of data or information, in a simple, easy, and efficient manner allowing security operation teams to work on pre-emptive measures or to understand any ongoing events that may be affecting their current operations.

CTI can help teams to prepare, plan, and execute their operations quickly. Rather than providing generic information about cyber events, CTI offers insights into threat actors, tactics, techniques, and provides information on how to counter them with prevention measures, risk analysis, and high-level security processes. When threat intelligence is understood and leveraged, security professionals can:

- Make informed incident response decisions;
- Understand threat actors' decision-making processes;
- Understand the tactics, techniques, and procedures (TTPs) of cyber actors; and
- Demonstrate the effectiveness of security operations to Chief Information Security Officers (CISOs), other stakeholders, and decision-makers with intelligence reports.

The DFSA has adopted, and encourages organisations to develop, a Security Programme that relies on a CTI framework to increase the robustness of security practices from strategic, operational and tactical perspectives.

You can find further information on CTI frameworks in Annex 2, on Threat intelligence sharing levels in Annex 3 and on types of Threat intelligence in Annex 4.

The DFSA's Cyber Risk Supervision

The DFSA formed a Cyber Risk Supervision unit in 2018. The unit's objectives are to improve cyber risk awareness in the DIFC, promote sharing of cyber threat intelligence amongst firms, whether authorised by DFSA or not, and support the continued development of cyber resilience within the DIFC community. The unit monitors progress towards the achievement of these objectives by assessing cyber risk across the population of DFSA-regulated firms, cooperating with other regulatory and public sector bodies and by publishing rules and guidance to prescribe cybersecurity systems and controls.

Assessing Risk

The DFSA evaluates and monitors cyber risk in the DIFC and collects information about cyber incidents to assist in better understanding the regional cyber risk landscape and to inform risk assessment planning. A risk assessment is a fundamental tool in evaluating cyber risk and includes institution-specific desk-based and onsite risk assessments, self-assessments, and thematic reviews. The results of our assessment work are used to evaluate cyber maturity levels and to tailor our actions towards mitigating cyber risks in the DIFC. We also collect information from regulated firms through various reports and use this information to inform our supervisory activities. The DFSA conducted cyber risk thematic reviews in 2020 and 2022. The results of those reviews can be found here.

Engage and Educate

Cyber security is a shared responsibility. We understand that our involvement is essential to build cyber security awareness among regulated firms and the broader DIFC community. Our engagement approach includes outreach sessions and roundtable discussions dedicated to cyber security topics. It also includes engaging relevant institutions in cyber simulations that help them to test their response to cyber incidents and assess their cyber resilience.

Guide

We publish Rules to require regulated firms to build and maintain cyber resilience and issue Guidance to help firms in developing their approaches. We participate in internal and external training to maintain our awareness of emerging cyber risks and supervision methodologies as well to develop a sustainable pool of cyber supervision resources.

Cooperate

We engage and cooperate with other regulators through regional and global cyber supervision forums and working groups. We also encourage firms to cooperate and share information with each other. Prior to launching the TIP, we concluded that there was need for a centralised mechanism to facilitate cooperation and information sharing. As a government entity, the DFSA decided that the Information Sharing and Analysis Centres (ISAC) community model was the best fit, given the DFSA's role and responsibility within the DIFC and Dubai. After consulting with the community and industry, it was decided that the DFSA should lead this initiative. The DFSA developed a mechanism to enable firms to share information with each other, namely the DFSA TIP.

The DFSA has taken on the responsibility and costs of the platform to benefit all participating entities. This is an unusual move for a financial regulatory body, but it is one that we believe was necessary to encourage entities of various sizes and capabilities to join and participate.

Progress with TIP

The DFSA has urged all DIFC firms to utilise the DFSA TIP. It has educated firms on the importance of threat intelligence sharing and contribution through various events and sessions. The DFSA has always encouraged voluntary involvement of firms and connected communities. In the launch year, 2020, 152 firms enrolled for DFSA TIP. As of January 2023, 233 firms and connected communities have joined the platform.

Initially, Help AG, participating vendors, MISP, OSINT and CERT were the highest contributors to DFSA TIP. Several regulated entities have experienced tangible benefits from the platform and a number have proactively started contributing threat intelligence to the community. TIP has now received contributions from numerous participant firms. Those contributing include many firms that vary in size and cyber capabilities.

During the first three years of TIP, the DFSA, with support from Help AG, conducted several workshops for participant firms and connected communities. These workshops were designed to drive awareness of the evolving cyber threat landscape, the latest techniques used by attackers, common threats and attacks, common methods to address attacks, and threat hunting and incident response methods. Most importantly, these workshops reinforced the benefits of using DFSA TIP for threat intelligence, sharing a threat intelligence through this platform, how member firms and connected communities can be well informed and proactively prepare to handle incident response.

The illustration below provides summaries of the topics addressed in the workshops conducted between 2020 and 2022.



Purpose

- Introduction to CTI
- Intelligence Sharing by DFSA TIP

Coverage

- Cyber Threat Intelligence
- DFSA TIP
- Evolving Threat Landscape
- Use Cases

Purpose

- Cyber Risk Fundamentals
- MFA
- Ransomware

Coverage

- Cyber Risk Fundamentals
- Risk Mitigations
- Necessity of MFA Implementing MFA
- Ransomware & Various Techniques

Purpose

- Common and Top Attacks
- Phishing
- Spamming

Coverage

- TOP Attacks
- Common Methods of Phishing & Spamming
- Importance of Email Security
- Threat Hunting and IR for Phishing Attacks

You can find more information on the development of TIP so far in Annex 5 and key Statistics in Annex 6 on the threat intelligence shared by the community.

The Importance Of Sharing

Attackers actively exchange information about hacking techniques and monetisation methods on darknet forums, in private visits and on social networks. They also create communities, forums and attend conferences where they exchange the latest trends in information security. Our adversaries operate in this way with great effect. So, what stops us benefitting from this model?

Sharing data within the DIFC community protects the entire community: if one member of the community detects an attack, identifies the indicators of the attacker and shares these with other members of the community, others can do likewise, rapidly providing visibility of the attacker and the attacker's targets to the whole community. During such sharing and ongoing activities, other indicators or information may be found and, when shared, help other participants, even those beyond the TIP community, and not just the participant who discovered the initial attack.

With this information, all members of the TIP community can pre-empt an attack, if it has yet to occur, by nullifying the effectiveness of an attack before it begins. Effectively sharing information benefits all users of the Platform and multiplies the value of the information.

It may be helpful to think of the TIP community as a herd. The herd is stronger and better protected because all members are aware of threats against the herd and actively share information about threats or attacks – when one is threatened, information is shared quickly, protecting the whole herd. The herd is a significantly harder target than an individual.



The Challenges Ahead

Experiences so far have taught us a lot and we have acquired valuable insights. The success of the platform depends on community members' contributions, ongoing adoption, and value recognition.

As cybersecurity operations mature within the region and the DIFC, we expect further adoption of the platform by DFSA-regulated firms, as well as others in the DIFC. One of the natural challenges we expect to face is improving and encouraging contribution in an organic manner without mandating participation.

We will continue to hold various workshops. Through these workshops, we aim to reinforce the value proposition of the platform, work to build trust amongst participants within the community and further widen the net of contributors. With the help and participation of highly reputable threat feed providers and specialist support partners, we plan to hold more frequent workshops with topics chosen to drive home the importance of embedding threat intelligence into firms' cybersecurity arsenals.

We anticipate that continuing to provide the platform as a public service encourages openness and trust, prompting wider participation and ongoing contribution.

Closing

The DFSA strives to expand partnerships, communities and innovate further to support local and government-led initiatives across the cybersecurity spectrum. In publishing this report, which is expected to be the first of a regular series, we reiterate our call – both to existing participants and those who are not already part of the TIP network – to join this community and work together for the common good in increasing cyber resilience in the DIFC, Dubai and the UAE.

DFSA
Dubai Financial Services Authority

ANNEX 1:

Implementing the platform

The DFSA performed benchmarking exercises and studied how similar platforms and initiatives were implemented in other countries and jurisdictions. The DFSA also engaged with similar platforms around the world and met existing sharing communities who shared insights on how to approach the initiative, as well as sharing valuable lessons learned. Two key conclusions from this exercise were that:

The platform was unlikely to succeed if it was dependent upon the intelligence contributions of only a small number of members; and

The community should be allowed to grow organically, without forced participation.

With these considerations in mind, we took steps to ensure the platform had a continuous supply of enriched and actionable threat intelligence and we launched outreach sessions to encourage smaller entities within the DIFC to join the platform. Sharing threat intelligence with smaller entities vastly improves their access to data that otherwise may have been prohibitively expensive for them to obtain.

To ensure TIP contained a continuous supply of enriched and actionable threat intelligence, we invited Palo Alto Networks and other cyber security specialists to support and participate in TIP. After establishing the required partnerships with these vendors, and other relevant government bodies, we were able to design the right model to suit our needs.

The next step was to choose the technology. To do this, we studied success factors in other communities, community feedback, integration capabilities with various security technologies, and capabilities of both off-the-shelf commercial and open-source platforms. We decided on a community-built and driven open-source software solution called MISP. One of the key features we found was that it was community driven and allowed for continuous development. From our perspective. commercial models carried higher risk and operating cost, which would need to be borne by participating firms. Our desire to provide the Platform as a public service and minimise or avoid charging firms, where possible, influenced our decision-making.

The platform is workflow based, where any individual from the connected community may view the intelligence and integrate the data with supported security tools or platforms to automate, prioritise, or accelerate response actions. The Platform offers:

An efficient database allowing storage of technical and non-technical information related to malware samples, indicators, incidents, attackers, and any type of cyber threat intelligence.

Automatic correlation to identify relationships between indicators from malware, attack campaigns or other types of analysis.

Built-in sharing functionality to ease data sharing using different models of distribution.

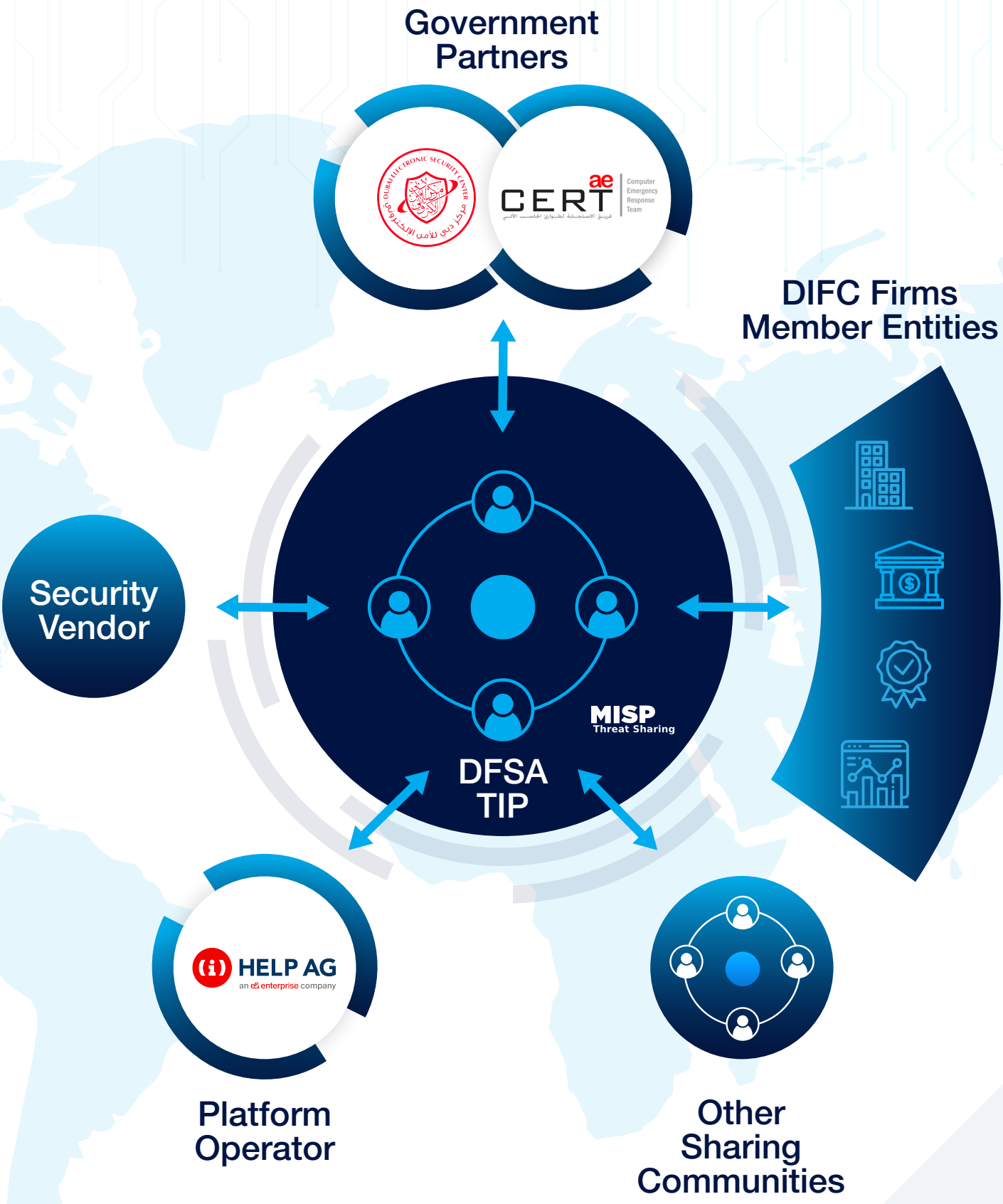
An intuitive user interface for users to work with functionality to create and view relationships between objects and data sets.

Storing data in a structured format (allowing automated use of the database for various purposes) with extensive support of cyber security indicators and financial fraud indicators.

Flexible free text import tool to ease the integration of unstructured reports into the Platform.

Once the platform was operational, we began, in conjunction with our supporting vendors, hosting ongoing education forums such as workshops and roundtable discussions for Platform members and the wider community. We also produced and distributed documentation for use cases and technical guides. Moreover, through these workshops, we worked to foster a culture of sharing and working together, unifying efforts towards sustaining the community-driven Platform (TIP).

The DFSA Cyber Threat Intelligence Community

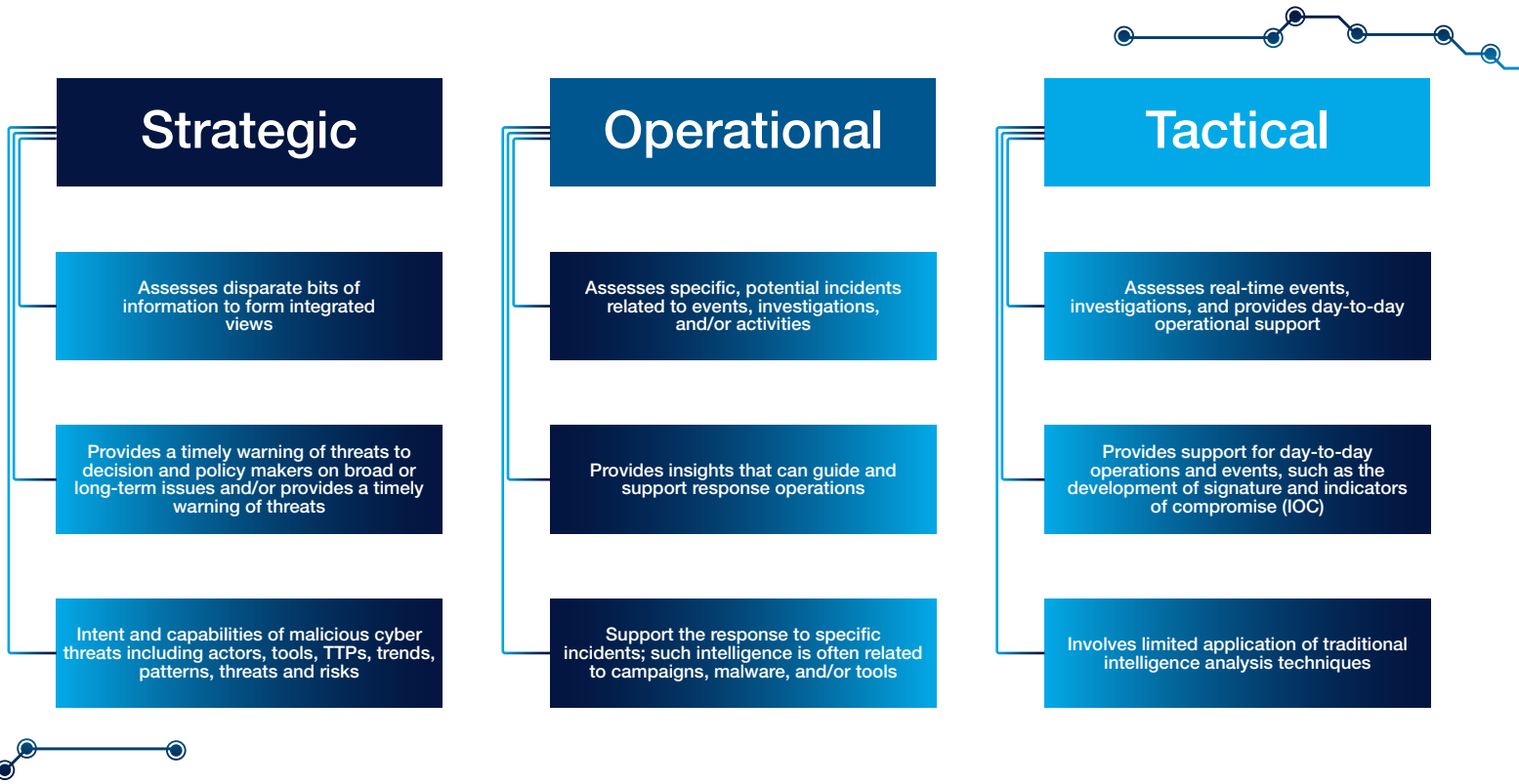


ANNEX 2:

Cyber threat intelligence (CTI) frameworks

A reliable CTI framework consists of basic components called Threat Intelligence Feeds. These feeds are obtained from various sources. The main purpose of Threat Intelligence Feeds is to provide (so allowing collation, aggregation and centralisation) contextual attacker data, which may include attacker intent and plans in a standardised consumable format. Threat Intelligence Feeds can contain additional meta data which can be applied to specify equipment, industries, countries, business or assets that could be affected. This enables consumers of these feeds to disseminate, inform, and educate individuals, businesses, and industries across the world quickly and efficiently. Further, with additional meta data, tailored warnings can be provided that may only be relevant to the recipient, ensuring they are acting on information that will directly affect their line of work or industry.

Threat Intelligence Feeds contain continuously updated actionable threat data from various Open-source intelligence (OSINT) sources and commercial vendors. These feeds consist of context, risk data, artifacts, and indicators in each of the below listed focus areas; that can be used to enhance the cyber threat response awareness and capabilities of the organisation. There are three types of threat intelligence – Strategic, Operational and Tactical.



Each type of intelligence corresponds to a specific type of audience; the information feed sent is tailored to each type of audience. This means that users of a platform do not need to log into the platform and check for the latest events. Information will be automatically fed to users via electronic feed.

ANNEX 3:

Threat Intelligence Sharing Levels

Threat intelligence communities consist of organisations that collectively share threat information. Community members can benefit from shared knowledge to fight cyber-attacks through real time threat information exchange. There are four types of security sharing which are highlighted in the table below.



ANNEX 4:

Types of threat intelligence

THE TYPES OF INTELLIGENCE TIP PROVIDES INCLUDE:

Indicators of Compromise (IoCs) - 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 IoCs to analyse a malware's techniques and behaviours better. IoCs also provide actionable threat intelligence that can be shared within the community to improve further an organisation's incident response and remediation strategies.

Tactics, Techniques and Procedures (TTPs) - these describe how threat agents orchestrate, manage, and execute attacks. Tactics are also sometimes called tools in the acronym. Specifically, TTPs are the patterns of activities or methods associated with a specific threat actor or group of threat actors.

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 an organisation's security.

Campaign - a series of related activities, initiated by a Threat Actor, intended to achieve a goal, involving a specified type of TTPs and IoCs.

ANNEX 5:

TIP development so far

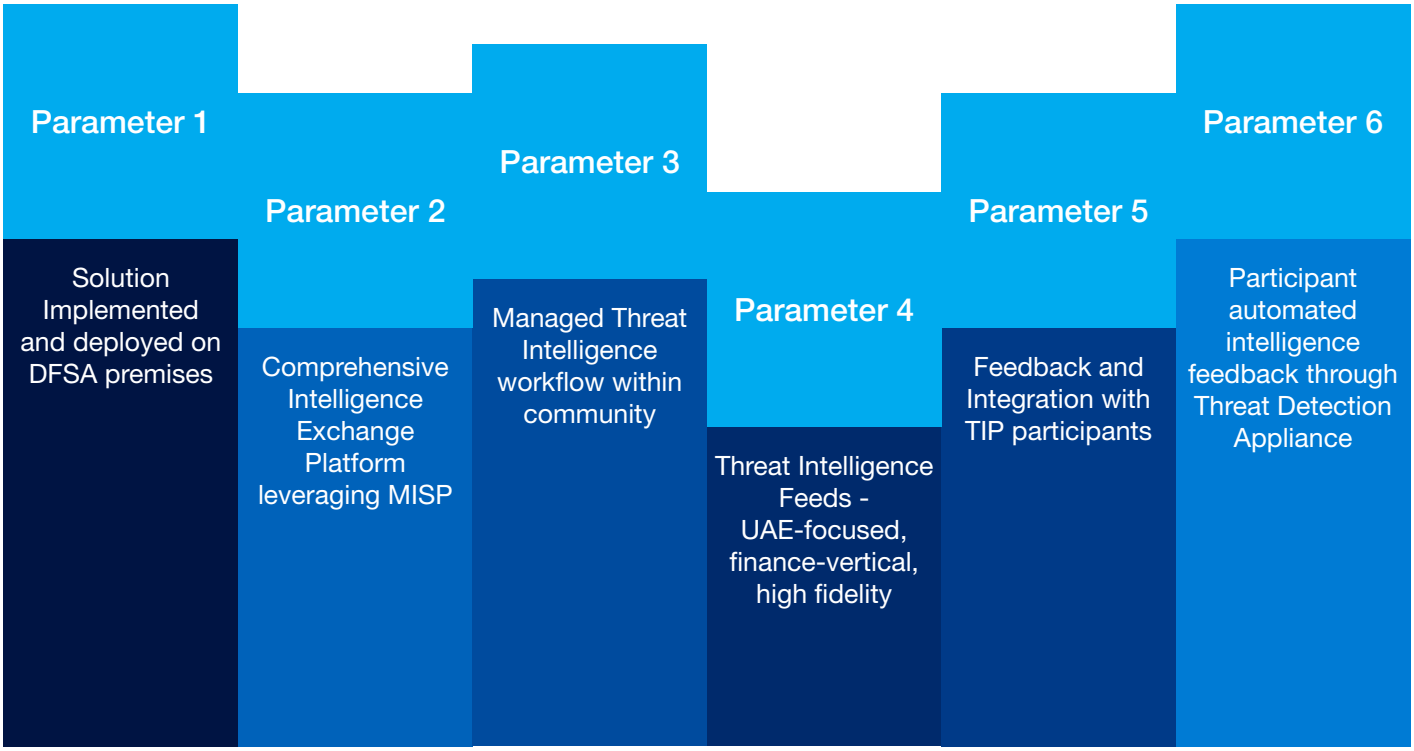
Inception and Implementation - Key Milestones

In January 2020, the DFSA TIP was launched and made available to DFSA-regulated firms, DIFC registered firms, and connected communities.

THE CORE PILLARS OF THE SERVICE ARE:

- Threat Intelligence Exchange Platform
- Intelligence Analysis, Selection and Publication
- Member Firm Support, Integration and Engagement
- UAE Based Security Experts

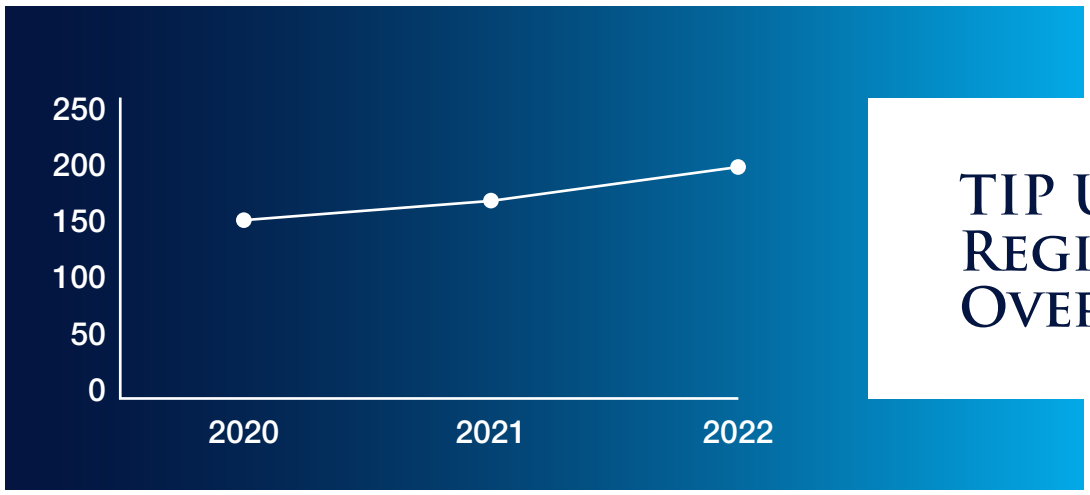
Service Architecture, Operations, Threat Intelligence Data Sharing and Threat Intelligence Exchange were designed. The TIP service parameters were described as:



ANNEX 6:
Statistics

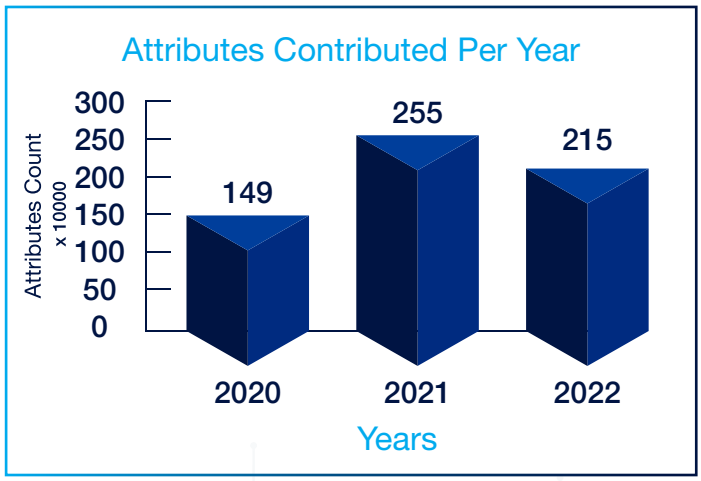
The graphs below show trends of various aspects of DFSA TIP.

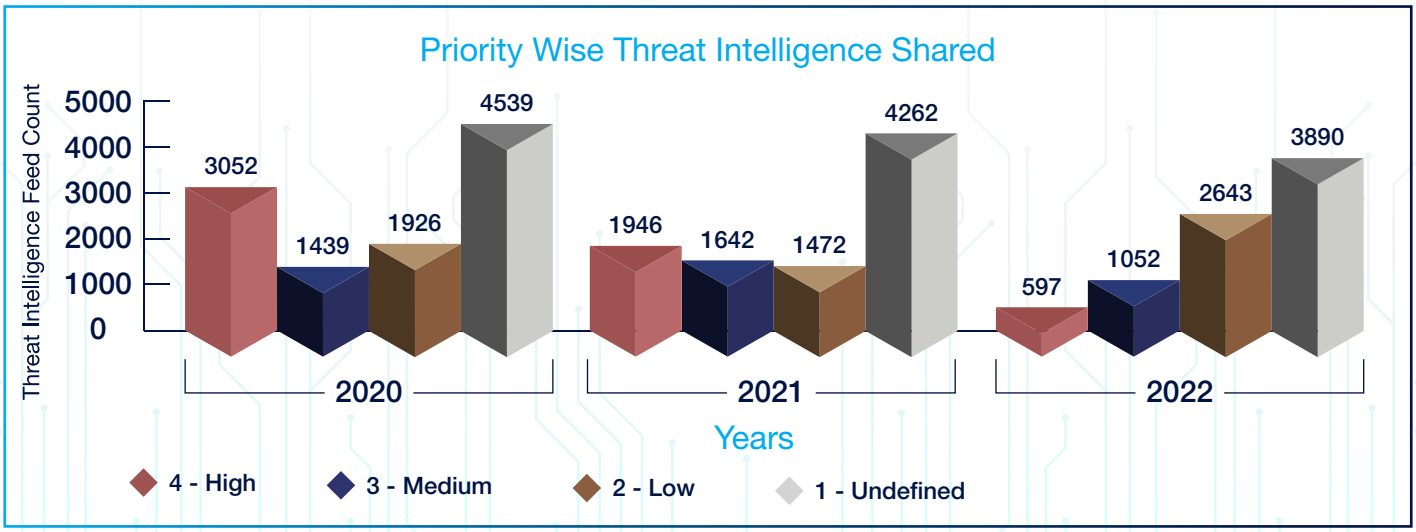
Note: Information and statistics cover the period of January 2020 to the end of 2022.

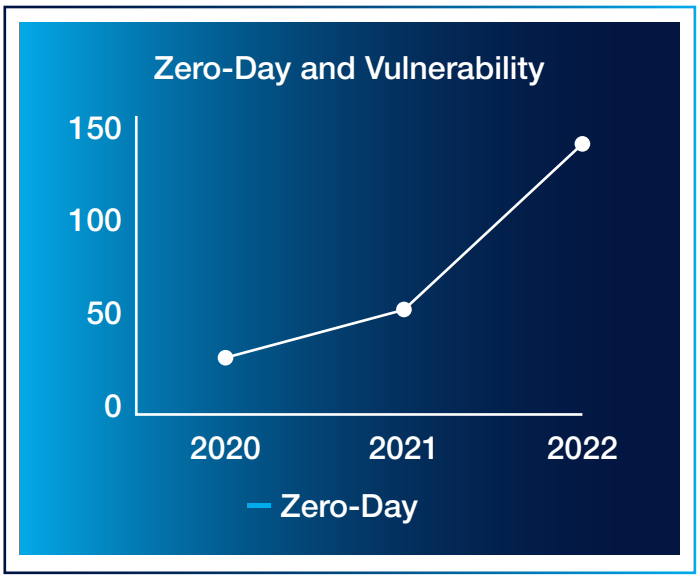


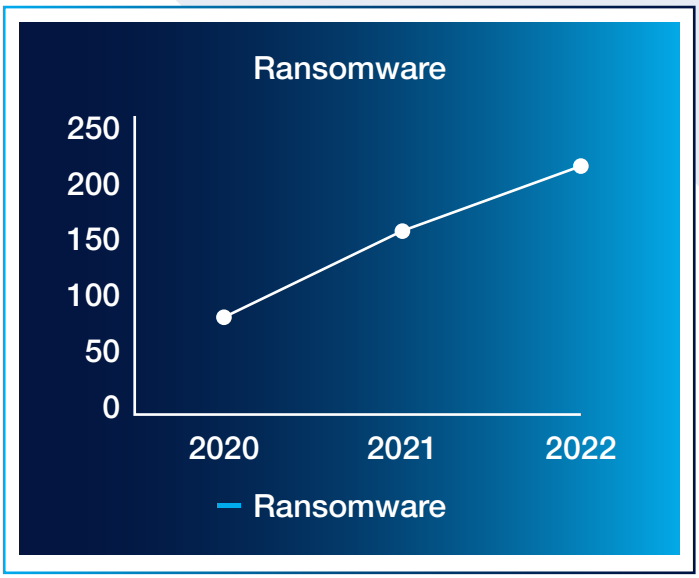
TIP User Registration Over Time

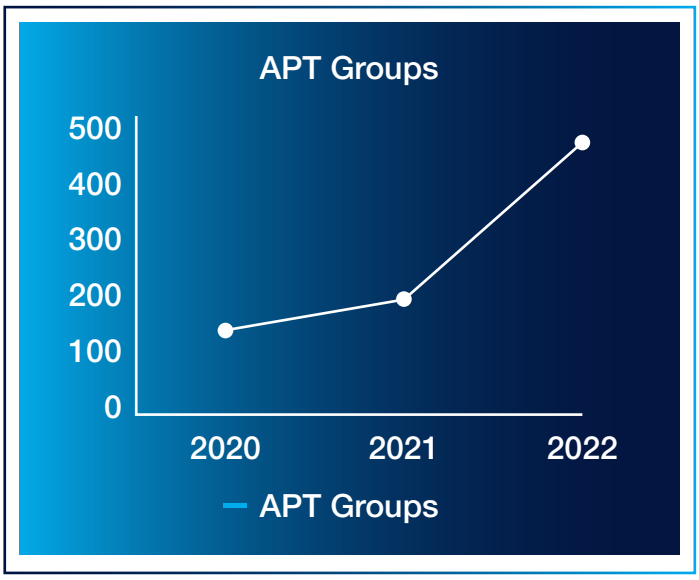


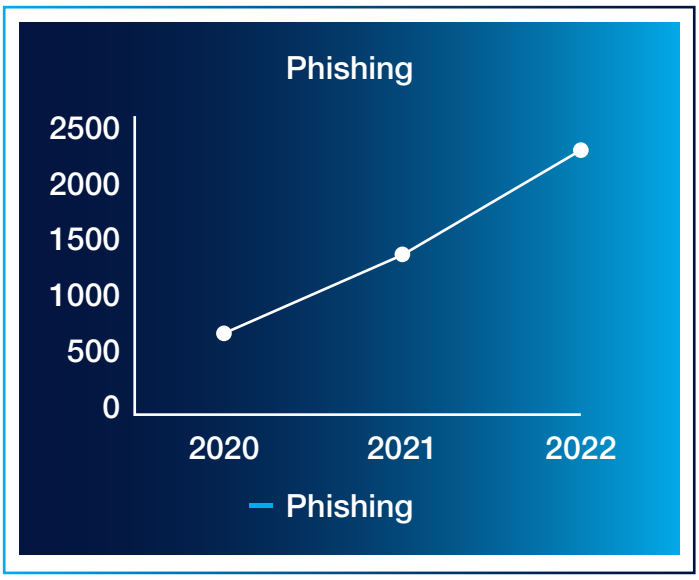


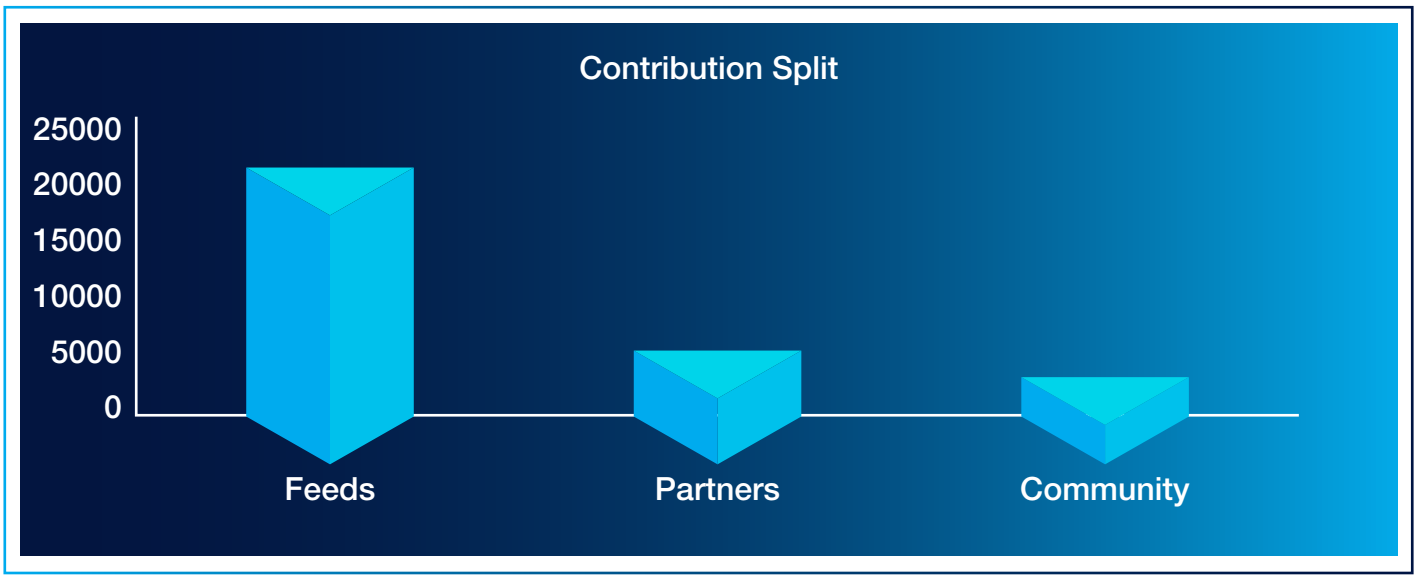



Zero-Day and Vulnerability
150
100
50
0
2020
2021
2022
Zero-Day


Ransomware
250
200
150
100
50
0
2020
2021
2022
Ransomware

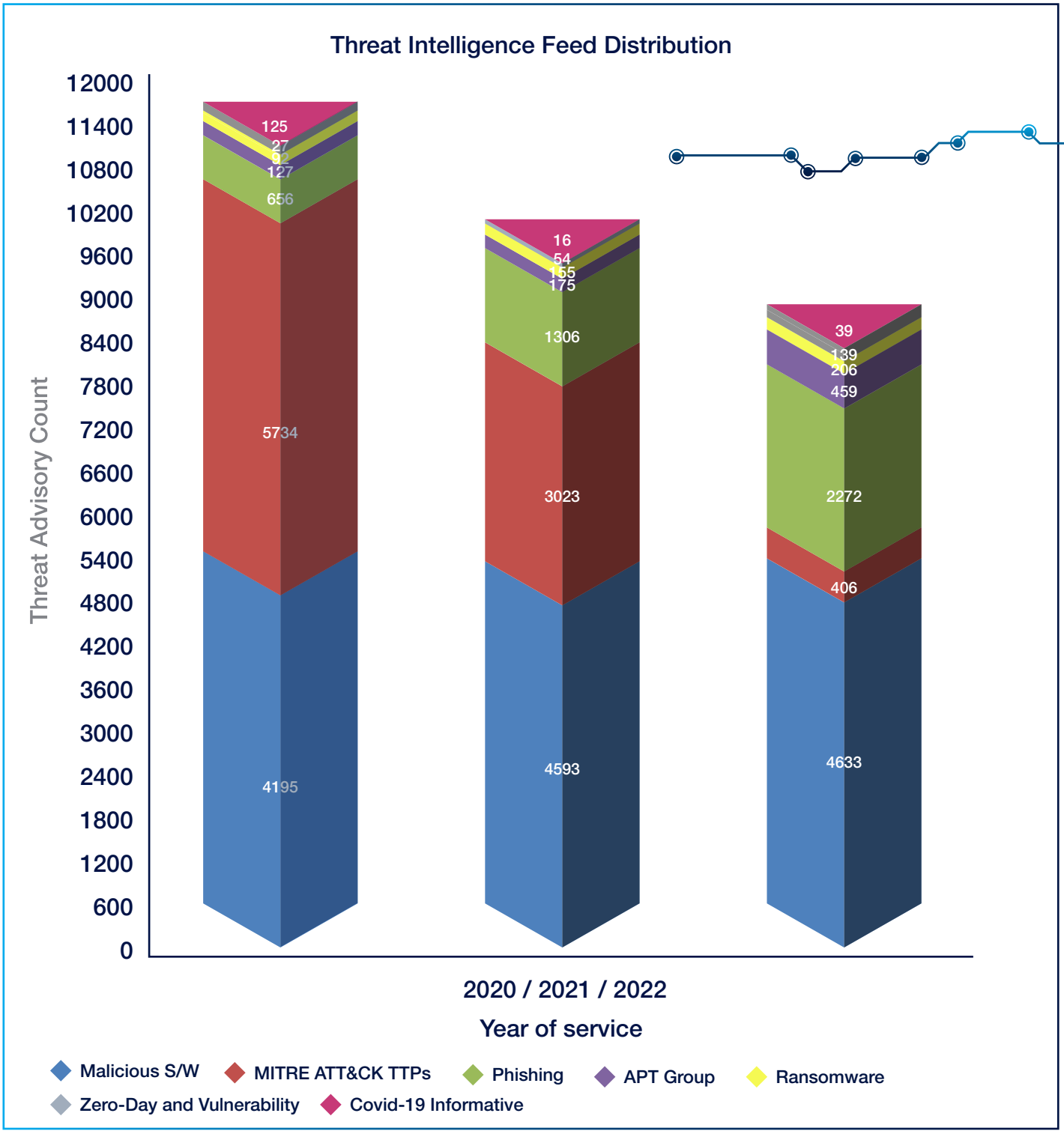

APT Groups
500
400
300
200
100
0
2020
2021
2022
APT Groups


Phishing
2500
2000
1500
1000
500
0
2020
2021
2022
Phishing


Contribution Split
25000
20000
15000
10000
5000
0
Feeds
Partners
Community

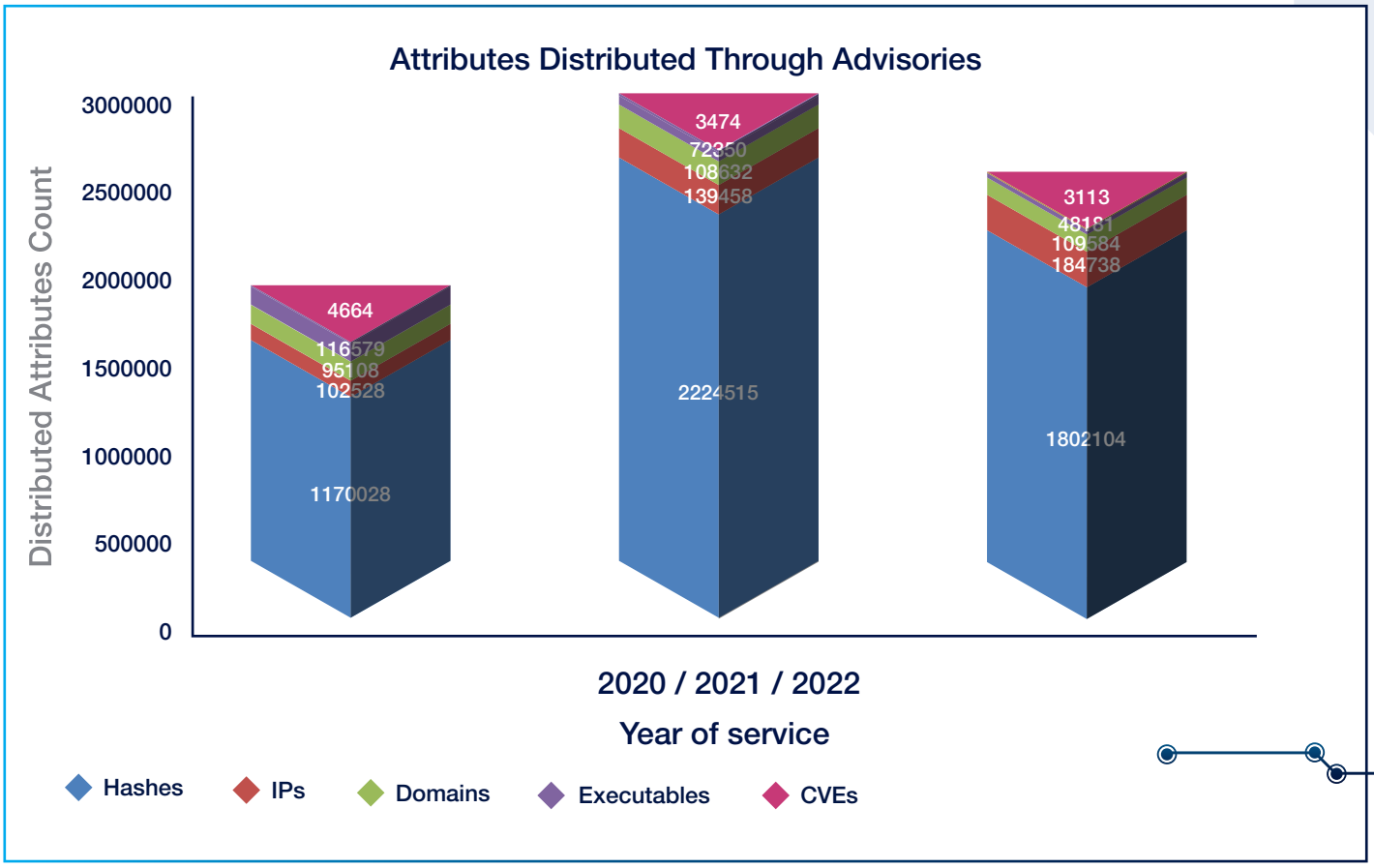
Threat Intelligence Distribution

Over three years of engagement, a total of 28,432 Threat Intelligence feeds and related advice were circulated via the DFSA Threat Intelligence Platform. The threat intelligence has been gathered from various organisations that include, but are not limited to, designated Threat Intelligence Service Providers, designated TIP platforms, various MISP platforms, globally known CERT and CSIRTs, OSINT (Open-Source Intelligence) platforms and applications, financial communities and regional MISP and CERT authorities.

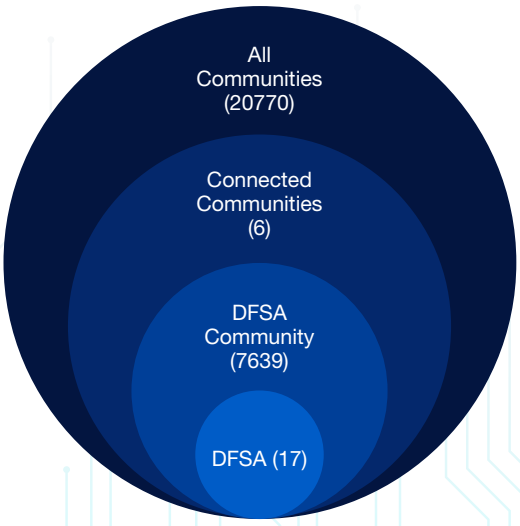


Attributes (IoCs) Through Threat Advisories

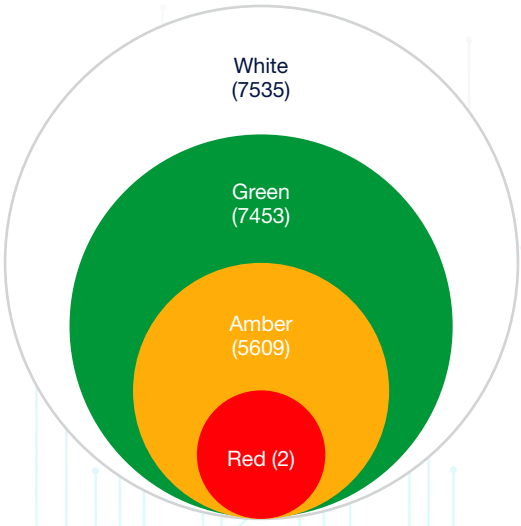
Since TIP was launched, nearly 6.2 million Attributes (IoCs) have been issued.



Threat Intelligence feeds have been shared with the DFSA, the DFSA TIP Community, and connected communities.



Community-wide TI Distribution



TI Classification

Threat Intelligence Categories

Over the three years TIP has been in service, threat intelligence feeds based on various types of risks and attacks have been shared as below:





www.dfsa.ae